Auditoria Especial no Sistema Eleitoral 2014

Partido da Social Democracia Brasileira - PSDB

RELATÓRIO DE AUDITORIA

PSDB – Comissão Executiva Nacional

SGAS Qd. 607, Ed. Metrópolis, Mód. B, Cob. 02, CEP 70.200-670, Brasília-DF.

Telefone: (61) 3424-0500; Fax: (61) 3424-0515; www.psdb.org.br; tucano@psdb.org.br

PARTICIPANTES

Especialistas:

Professor Clovis Torres Fernandes
Instituto Tecnológico da Aeronáutica – ITA
Comitê Multidisciplinar Independente - CMInd

Professor Marco Antônio Simplício Junior
Universidade de São Paulo - USP

Professor Edson Satoshi Gomi
Universidade de São Paulo - USP

Peritos:

Amilcar Brunazo Filho
Comitê Multidisciplinar Independente - CMInd

Marco Antônio Machado de Carvalho
Comitê Multidisciplinar Independente - CMInd

Márcio Coelho Teixeira
Comitê Multidisciplinar Independente - CMInd

Giuliano Giova
Instituto Brasileiro de Peritos - IBP

Felipe Rinaldi de Campos
Instituto Brasileiro de Peritos – IBP

Gustavo Batistuzzo
Instituto Brasileiro de Peritos – IBP

Wanderley José de Abreu Júnior
Auditor Independente

Ney Costa Doria Júnior
Auditor Independente

Assessoria Jurídica:

Flávio Henrique Costa Pereira
Partido da Social Democracia Brasileira – PSDB

Gustavo Guilherme Bezerra Kanffer
Partido da Social Democracia Brasileira – PSDB

Juliana Abrusio Florêncio
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados

Renato Opice Blum
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados

Emelyn Bárbara Zamperlin Nascimento
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados

Paula Lima Zanona
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados

Coordenação

Carlos Henrique Focesi Sampaio
Deputado Federal e Vice-Presidente Jurídico do PSDB

Flávio Henrique Costa Pereira
Partido da Social Democracia Brasileira – PSDB

SUMÁRIO

1. APRESENTAÇÃO

No Brasil, o processo eleitoral, o sistema eleitoral e os direitos políticos tiveram incontáveis transformações, sendo que o voto percorreu caminho laborioso até que fosse contemplado como direito de todos os cidadãos brasileiros.

Com efeito, a Constituição de 1824, outorgada pelo Imperador Dom Pedro I, determinava a realização de eleições para a escolha de representantes dos poderes legislativo e executivo. Naquela época, o eleitor apto deveria pertencer ao sexo masculino e ter no mínimo 25 anos. Além disso, havia o emprego do voto censitário, sendo que o cidadão só estaria apto a votar caso comprovasse renda mínima anual, tornando o voto um instrumento de ação política exclusivo das elites.

Após, com a Proclamação da República do Brasil, em 1889, foi instaurada a forma Republicana Federativa Presidencialista do Governo no Brasil, findando a soberania do imperador D. Pedro II e a Monarquia Constitucional do Império.

Na Constituição de 1891 foi determinado que o primeiro Presidente da República deveria ser eleito pelo Congresso Constituinte e, os subsequentemente, diretamente pelo povo.

Com a Constituição de 1934, o voto tornou-se obrigatório para as mulheres, bem como se criou a Justiça Eleitoral, sendo que, pela primeira vez, se inseriu na Constituição capítulos sobre a ordem social, direitos trabalhistas e previdência social, direito civil e administrativo, educação, cultura e segurança nacional.

Já a Constituição Federal de 1937 possuía feição ditatorial, embora contemplasse em seu artigo 1º que “O Brasil é uma República. O poder político emana do povo e é exercido em nome dele e no interesse do seu bem-estar, da sua honra, da sua independência e da sua prosperidade”.

Depois de quase uma década, com a Constituição de 1946 e Lei Constitucional nº 9, liberdades democráticas foram reconquistadas, estabelecendo, inclusive, eleições diretas. A nova Constituição reestabeleceu o princípio da separação e harmonia dos poderes e proibiu a organização, registro e funcionamento de partidos políticos ou associações que contrariavam o regime democrático.

Após duas décadas, com o rompimento do Estado Democrático de Direito por meio do golpe militar de 1964, que depôs o Presidente da República em exercício, João Goulart, após renúncia de Jânio Quadros, viveu-se novo período ditatorial, culminando com a Constituição de 1967 e Emenda 1, de 1969, que estabeleceram, entre outras disposições, eleições indiretas para o cargo de Presidente da República e governador, extinção das imunidades parlamentares, suspensão de direitos e garantias fundamentais, notadamente o *habeas corpus* para crimes políticos e fechamento do Congresso Nacional.

Em 1985 se encerrou o longo período ditatorial e em 1988 foi promulgada a atual Constituição da República Federativa do Brasil, restabelecendo as eleições diretas e os direitos individuais fundamentais e sociais, redefinindo o Brasil como um país democrático.

Diante da história de luta pelo voto e pela democracia, é imperioso que se adotem todas as medidas necessárias para tornar o processo eleitoral absolutamente transparente ao povo brasileiro, bem como que se busque o aperfeiçoamento do sistema democrático do país para se obter dos eleitores a inteireza de sua vontade, sem qualquer mácula ou engano. Este fim, para ser alcançado, exige a garantia de que o sistema eleitoral esteja protegido de abusos, fraudes e erros, conforme se deflui do art. 14, § 10 da Constituição Federal, que explicita o princípio de proteção à legitimidade e normalidade das eleições contra os atos de abuso, corrupção e fraude.

Não se pode perder de vista que a eleição é um processo que necessita evoluir no tempo, justamente para garantir a lisura de seu resultado contra as tentativas de manipulação do sistema eleitoral por aqueles que buscam o poder sem qualquer escrúpulo ou consciência democrática.

Foi justamente a busca por este aperfeiçoamento que levou a Justiça Eleitoral brasileira a iniciar o processo de informatização das eleições, em 1986, com o recadastramento de milhões de eleitores. Em 1994 ocorreu, pela primeira vez, a totalização das eleições gerais pelo computador central, no Tribunal Superior Eleitoral. Em 1995, iniciaram-se os trabalhos de informatização do voto, com a apresentação de um protótipo da urna eletrônica, sendo que durante as eleições municipais de 1996 o projeto foi concluído e, com isso, iniciada a primeira votação eletrônica no Brasil, com a implantação do voto eletrônico para todo eleitorado brasileiro no ano de 2000.

A informatização do voto, conforme dispõe o Egrégio Tribunal Superior Eleitoral:

> *"Surgiu para agregar mais qualidade, agilidade, transparência, segurança e robustez ao processo eleitoral. Tem sido uma ferramenta efetiva para o combate às fraudes. É um produto genuinamente brasileiro, único no mundo, concebido e construído sob a orientação do TSE, tanto o hardware das urnas eletrônicas como os milhares de programas computacionais que integram o sistema eletrônico de votação".*

Ainda nas palavras deste E. Tribunal Superior Eleitoral, dentre as principais premissas estabelecidas para o processo eletrônico de voto, estão:

- *Solução universal - registro do voto pelo número do candidato ou partido;*
- *Aderência à legislação vigente, com possibilidade de evolução para garantir que mudanças na legislação eleitoral não obriguem alterações na urna eletrônica;*
- *Processo amigável, de fácil utilização pelo eleitor, com a visualização na tela dos dados do candidato antes da confirmação do voto;*
- *Custo reduzido – o projeto deveria ser economicamente viável, em função do elevado número de seções eleitorais;*
- *Perenidade – possibilidade de uso em várias eleições, diminuindo o custo do voto;*
- *Segurança - eliminação da possibilidade de fraude no registro do voto e apuração do resultado;*
- *Facilidade na logística - pequena, rústica, peso reduzido, de fácil armazenamento e transporte;*
- *Autonomia - uso de bateria onde não há energia elétrica.*

Estas características, que são universais, é que levaram diversas democracias a aderir ao sistema eletrônico de votação.

Assim é que, além do Brasil, há diversos países, em diferentes continentes, que atualmente fazem uso das urnas eletrônicas, com especificações e procedimentos diferentes, tais como Argentina, Bélgica, Canadá, Equador, Estados Unidos, Índia, México, Peru, Rússia, Vaticano e Venezuela[1].

1 http://www.brunazo.eng.br/voto-e/textos/modelosUE.htm

Por outro lado, o mecanismo eletrônico não é utilizado em diversos países, como Holanda, Alemanha, Irlanda, Inglaterra e Paraguai[2], que testaram a utilização de urnas eletrônicas e desistiram por compreenderem que o sistema não seria seguro.

Se, por um lado, a votação eletrônica trouxe agilidade ao processo eleitoral e apresentou-se como caminho para evitar inúmeras fraudes, como, por exemplo, o "mapismo"[3], é possível que abriu as portas para outros tipos de fraudes, mais sofisticadas e de difícil constatação. Ressalte-se que, independentemente de qualquer manipulação de dados, o sistema eletrônico de votação, por suas próprias características técnicas, é obscurantista, pois aos leigos é impossível compreender como se dá o processo eletrônico de votação, o que enseja inúmeras especulações.

A partir desta realidade, os atores do processo eleitoral - candidatos, juízes eleitorais, Ministério Público, partidos políticos, Ordem dos Advogados do Brasil - necessitam não só garantir a normalidade e legitimidade das eleições, mas também agirem de forma a ampliar a transparência, evitando-se que a legitimidade do exercício do poder seja maculada perante o titular da soberania nacional.

As últimas eleições revelaram, de forma ímpar, a verdade desta afirmação, o que, inclusive, serviu de fundamento para se deferir esta Auditoria. Como será demonstrado neste trabalho, é inquestionável que ainda há muito a se caminhar para garantir a esperada transparência das eleições, principalmente uma atuação mais profícua de partidos e candidatos em seu dever de fiscalizar e uma maior amplitude de procedimentos de auditagem para efetivo controle do resultado eleitoral.

2 http://www.brunazo.eng.br/voto-e/textos/modelosUE.htm

3 Mapismo é um conhecido processo de fraude eleitoral que se aplicava quando a totalização dos votos ainda se dava por processo manual de votos. As somas dos votos eram anotadas em mapas e entre a passagem da totalização de um mapa para outro a fraude era aplicada anotando-se um número maior de votos que o efetivamente atribuído a determinado candidato.

2. INTRODUÇÃO

Os trabalhos da Auditoria Especial começaram com a coleta e organização dos principais tipos de denúncias que foram publicadas na Internet por eleitores no Brasil e no exterior. Em síntese, as denúncias faziam referência a falhas nos equipamentos, a erros em processo e a procedimentos indevidos no TSE, TRE´s, zonas e seções eleitorais.

Essa coleção de denúncias foi a base para se montar um plano inicial de trabalho que deveria ser reformulado e ajustado *pari passu* às novas e pouco previsíveis descobertas e necessidades que poderiam aflorar durante sua evolução, cenário típico em investigações exploratórias onde apenas o ponto de partida é bem conhecido.

Esse método investigativo, essencial para a efetiva apuração das denúncias, encontrou inúmeros limites, notadamente pelos diversos obstáculos que surgiram para sua efetiva aplicação. Hoje, como está claro para todas as partes envolvidas com a auditoria, os procedimentos de perícia previstos em leis e regulamentos da Justiça Eleitoral são insuficientes para garantia da transparência do processo de eleições, necessitando não só de um aperfeiçoamento de métodos como, também, de uma mudança de concepção por parte de todos aqueles que participam diretamente do processo eleitoral.

De um lado, candidatos, partidos e coligações precisam participar efetivamente de todas as etapas do processo eleitoral, fazendo-se representar por pessoas com capacidade real para acompanhar os procedimentos jurídicos e técnicos inerentes a todos os procedimentos de coleta, apuração e totalização dos votos.

De outro, a Justiça Eleitoral necessita alterar sua concepção de fiscalização do processo eleitoral, de forma a permitir a mais ampla e irrestrita auditagem do processo, único caminho para se atestar a regularidade das eleições.

Hoje, o TSE tem o poder de comandar os rumos da investigação mesmo sendo o próprio investigado em questões técnicas, porque acumula papéis tão diversos como regulamentar, ser Tribunal julgador, definir normas técnicas, desenvolver os sistemas eletrônicos e operar esse sistema para coletar e totalizar votos.

Esses múltiplos papéis impõem ao Tribunal o dever de apoiar e mandar aprofundar quaisquer investigações sobre si mesmo, de forma livre e ampla, sem opor obstáculos que impeçam qualquer resultado conclusivo da fiscalização operada.

O certo é que o Tribunal se afastou das melhores práticas e normas mundiais de auditoria sob a concepção de que exames independentes e profundos colocariam em risco a segurança do sistema eleitoral, afastando-se da consagrada prática de que a transparência aumenta a segurança e reduz riscos.

Como será visto adiante, essa postura viola tanto os princípios e determinações da Administração Pública sobre transparência e prestação de contas ao cidadão, como também as diretrizes do próprio Poder Judiciário sobre resolução de questões onde há conflito de interesses e as diretrizes sobre imparcialidade, contraditório, produção de provas técnicas e exames periciais, a exigir uma efetiva mudança de paradigmas da fiscalização das eleições.

3. SUMÁRIO DOS TRABALHOS

Os exames realizados pela Auditoria Especial a respeito das denúncias referentes aos sistemas eleitorais e aos procedimentos realizados pela infraestrutura do TSE estão sumarizados na tabela a seguir e detalhados nos próximos capítulos.

Em síntese, em função do grande volume, as denúncias foram organizadas segundo seus principais atributos e, em seguida, buscou-se identificar sua veracidade junto à área, processo ou componente do sistema eleitoral que é responsável pela prevenção, correção e guarda da trilha de auditoria correspondente.

Dessa maneira buscou-se avaliar tanto a procedência, ou não, das denúncias sobre supostas falhas ou procedimentos indevidos internos ou externos, como também o cumprimento pela infraestrutura do TSE dos requisitos relacionados à prevenção e correção dessas falhas ou procedimentos indevidos. Em função das limitações impostas aos trabalhos da Auditoria Especial, muitas avaliações podem apresentar resultados genéricos ou parciais, a serem aprofundadas ou complementadas oportunamente. A tabela a seguir apresenta os atributos avaliados e resultados alcançados conforme a seguinte legenda:

TSE demonstrou conformidade com o requisito

Insuficiente para comprovar conformidade

TSE demonstrou não conformidade

Os atributos e resultados da Auditoria Especial estão indicados a seguir:

	REQUISITOS	AVALIAÇÃO	PRINCIPAIS REFERÊNCIAS
1.	**GOVERNANÇA DO SISTEMA ELEITORAL**		
1.1	Instituição de governança do sistema eleitoral	C	TSE instituiu planejamento estratégico que o obriga, a partir da eleição de 2014, a assegurar transparência e segurança e manter alinhamento entre discurso e prática nas questões pertinentes ao sistema eleitoral. (Item 3.2, p.24)
1.3	Conformidade do TSE no atendimento de solicitações necessárias ao desempenho dos trabalhos de auditoria	NC	TSE comprovou transparência quanto à página na Internet sobre execução financeira, divulgação do repositório de dados e estatísticas eleitorais, processuais e de julgamentos. Contudo, deixou de atender aos pedidos de informações técnicas de interesse desta Auditoria e determinações da Lei 12.527 sobre Acesso às Informações de Interesse da Sociedade (item 3.4. p.32)
1.4	Conformidade do TSE da prestação de contas eleitorais e partidárias	C	Adequado no âmbito da presente auditoria (item 3.2, p.24)
1.5	Conformidade do TSE sobre relatórios de gestão	C	Adequado no âmbito da presente auditoria (item 3.2, p.24)
1.6	Conformidade do TSE quanto à qualidade da informação pública sobre o sistema eleitoral	I	O TSE foca responsabilidade social como um Tribunal aberto à comunidade e responsabilidade ambiental no combate ao desperdício e manutenção de Ouvidoria com canais para orientar o eleitor. Contudo, para efeito desta Auditoria Especial, não demonstrou atender princípios que o próprio Tribunal estabeleceu quanto a dar respostas efetivas e concretas aos questionamentos (item 3.5, p. 33)
1.7	CONFORMIDADE DE COMITÊS: Comprovar conformidade do TSE nas questões de estrutura relacionadas a Comitês e Conselhos	C	A presente Auditoria Especial pôde verificar a operação dos Comitês e Conselhos nas questões relacionadas ao sistema eleitoral

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
1.8	Conformidade da gestão de riscos pelo TSE	NC	Abrange a metodologia para gerenciamento de projetos, programas e portfólios. Considerando a sociedade como cliente preferencial do Escritório de Projetos, o TSE não conseguiu demonstrar cumprimento das demandas de informações claras, técnicas e objetivas sobre redução de riscos operacionais, melhor distribuição de informações sobre projetos e compartilhamento das lições apreendidas sobre projetos anteriores (item 3.6, p. 34)
1.9	Conformidade do Controle Interno e Auditoria no TSE	NC	Essa dimensão de análise endereça diversos indicadores, como estar vinculado à Presidência, fiscalizar contratos e gerir riscos. No âmbito deste trabalho cumpre notar que não foram constatados retornos efetivos da Auditoria Interna com relação às denúncias em questão, para os apontamentos das auditorias anteriores e para os pontos reiterados na presente Auditoria Especial, especialmente quanto à possível falta de liberdade de ação da Auditoria nas denúncias envolvendo alta tecnologia e fornecedores externos, efetiva fiscalização na entrega, desenvolvimento e utilização de componentes de alta tecnologia e omissões ou deficiências na gestão de riscos frente à grande quantidade de denúncias.(item 3.6, p. 34)

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
1.10	Conformidade do TSE sobre segurança da informação	NC	Essa dimensão de análise endereça indicadores como a Comissão de Segurança da Informação do Tribunal, instituição de políticas e avaliação do seu gerenciamento. No âmbito da presente Auditoria Especial não foram localizadas ações efetivas de segurança da informação no que concerne apurar e responder concretamente e objetivamente às denúncias, às críticas relacionadas a vulnerabilidades do sistema eleitoral e às demandas por investigações, auditorias e perícias mais profundas e transparentes (item 3.6, p. 34)
1.11	Conformidade do TSE na melhoria de processos	NC	TSE declara compromisso com diversas melhorias de gerenciamento. Contudo, no âmbito da presente Auditoria Especial demonstrou não ter atendido pontos específicos deste trabalho relacionados ao compromisso de satisfação do público alvo, deixando de tratar os resultados indesejados de forma a aumentar a satisfação do cidadão. Nessa mesma linha, não ficou claro se o TSE fiscalizou e aplicou sanções ao receber produtos tecnológicos em desacordo com as melhores práticas mundiais. Na avaliação de competências e modelos gerenciais não ficou claro se o TSE considerou as questões de transparência e apoio às auditorias de questões tecnológicas de forma independente da estrutura hierárquica (item 3.7, p. 35)

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
1.12	Conformidade do TSE na Governança de TI	NC	A atuação da presente Auditoria Especial confirmou o alinhamento da gestão de TI às diretrizes do Tribunal e à preocupação de não gerar prejuízos à imagem da instituição. Contudo, se apurou descumprimento da governança de TI com relação à análise transparente das denúncias e riscos apontados pela sociedade e reiteradas auditorias. Em lugar de aprofundar avaliações abertas e apresentar resultados de forma transparente, a governança de TI se mostrou voltada à proteção da própria estrutura e não de um claro e aberto aprofundamento conjunto das investigações (Item 3.7, p. 35)
1.13	Governança de TI no licenciamento do sistema operacional da Urna	NC	Não se constatou que o TSE cumpra os termos do licenciamento do sistema operacional utilizado na Urna Eletrônica (item 3.8, p. 37)
1.14	Governança do TSE quanto aos sistemas aplicativos	NC	Não se constatou que o TSE cumpra os termos do licenciamento do sistema operacional utilizado na Urna Eletrônica (item 3.8, p. 37)
1.15	Governança do TSE sobre criptografia e assinatura digital	NC	O TSE aceita no sistema eleitoral a existência de código e serviços de autenticação providos pelo CEPESC, constituindo em ponto crítico de falha e eventual procedimento indevido que pode influenciar quase todas as rotinas do sistema eleitoral, além de haver subordinação do CEPESC a órgão comando por parte possivelmente interessada na eleição, contrariando princípios de governança. Apurou-se que código-fonte do CEPESC não seguiu os trâmites previstos na lacração de *software*. (Item 3.10, p. 46)

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
1.16	Governança do TSE e a atuação dos Juízes Eleitorais	NC	Constatou-se que os Juízes abdicam dos procedimentos de investigação e produção de provas que usualmente utilizam em suas Varas de origem nas esferas Cível ou Criminal, pois na esfera Eleitoral limitam-se a cumprir as instruções sobre auditoria emitidas genericamente pelo TSE, perdendo eficácia no acatamento, apuração e comprovação de erros e fraudes. (Item 3.11, p. 47)
1.17	Governança do TSE sobre testes públicos de urnas	NC	Constatou-se ter o TSE encerrado ou postergado o teste previsto para 2014 justamente quando o teste público anterior descobriu falha grave no sistema. Coincidentemente, criou Grupo de Trabalho em Segurança voltado ao corpo técnico interno, procedimento inadequado frente às melhores práticas de governança. (Item 3.12, p. 48)
2	**GESTÃO DE ELEITORES**		
2.1	Cadastro nacional de eleitores e sistema de informações eleitorais	I	Gerido pelo TSE, com acesso por Autoridades Judiciárias e Ministério Público, seus dados são utilizados para inseminar urnas. Sistema, em tese, transparente. Porém, o TSE não comprovou a segurança do processo frente às denúncias de eleitores que tiveram problemas com sua identificação para votar. (Itens 4.4.5.4, 4.4.5.5, 4.3.4)
2.2	Combate a eleitores fantasmas	NC	Existência de eleitores que votaram e justificaram simultaneamente. Não foi permitido acesso a dados desses eleitores. (Itens 4.4.5.4, 4.4.5.5, 4.3.4)
2.3	Confiabilidade e eficácia do cadastro biométrico	I	Alto índice de falsos negativos e falsos-positivos. (item 4.4.5.3)
3	**GESTÃO DE CANDIDATURAS**		

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
3.1	Controle de partidos e candidatos.	C	Partidos, candidatos e situações geridos de forma transparente por TSE e TRE's.
3.2	Inseminar urnas com dados de seção, partidos e candidatos	I	TSE não demonstrou para a Auditoria Especial funcionamento adequado do sistema eleitoral frente às muitas denúncias sobre vícios em teclado ao tentar digitar número de um candidato e fotos de determinado candidato que não aparecem no momento da votação. TSE não permitiu utilizar programas e dados reais para apurar as supostas falhas. (Item 4.4.2.5.2, p. 92, item 4.4.5.3, p. 143)
4	**URNA – HARDWARE E FIRMWARE**		
4.1	Prover hardware e firmware/bios - terminal do eleitor e microterminal do mesário, impressora para boletim de urna, relatórios de carga e testes, slots para flash interna (com lacre) e externa, conectores, sensores internos de estado. Firmware BIOS e Extensão BIOS (funções de segurança), memórias não voláteis (EEPROM, número de série)	I	TSE demonstrou que realiza os procedimentos previstos pela Lei 8666/1993. Contudo, não comprovou haver controles efetivos e transparentes dos processos de desenho e manufatura do *hardware* da urna, cabendo considerar ainda os severos questionamentos relacionados ao *firmware*.
4.2	Transparência na aquisição e conferência no recebimento dos produtos e serviços contratados	NC	O TSE não permitiu o exame de *hardware* e não incluiu parte do *firmware* e *drives* nos testes permitidos.
5	**URNA - *SOFTWARE***		
4.3	Atividade de pré-compilação pelo TSE com inserção no código-fonte recebido de fornecedores ou próprios mediante inserção de rotinas e chaves criptográficas CEPESC, antes da compilação a ser realizada em audiência pública.	I	TSE não demonstrou ou possibilitou o exame pela Auditoria Especial. (item 4)

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
4.4	Apresentar códigos-fonte aos partidos, esclarecer dúvidas e compilar. Gravar em mídia, lacrar com assinaturas e guardar em cofre do TSE. Guardar log de compilação.	NC	Constatou-se que a prática é insuficiente para assegurar ausência de erros ou fraudes. A Auditoria Especial apurou que parte do código-fonte crítico do CEPESC não integra a mídia preservada no cofre do TSE. (item 4)
4.5	Providenciar dados sobre município, zona e seção eleitoral, tabela de eleitores, fotos de candidatos.	I	TSE não demonstrou ou autorizou averiguar posteriormente a qualidade e integridade do procedimento e cadastros. (item 4)
4.6	Empacotar *software* e dados e transmitir o conjunto. Gerar pacotes do sistema operacional, programas aplicativos, programas utilitários e dados para votação. Gerado e cifrado em ambiente SIS, transmitido com cadastro de eleitores, desempacotado para preparação das memórias flash de carga para inseminação das urnas mediante Gerador de Mídia	I	TSE não demonstrou ou autorizou averiguar posteriormente a qualidade e integridade do procedimento e cadastros. (item 4)
4.7	Prover Gerador de Mídia: Organizar e gravar em flash de carga os programas e dados (partidos, candidatos, eleitores, controles). Fazer inseminação e coleta da tabela de correspondência que associa EEPROM de número de série da urna com seção eleitoral a transferir para totalizador	I	TSE não demonstrou ou autorizou averiguar posteriormente a qualidade e integridade do procedimento e cadastros. (item 4)
4.8	Prover Subsistema de Instalação e Segurança (SIS): Nos computadores TSE, TREs e Polos de Inseminação de Urnas. Controlar programas, permissões e perfis de usuários e gerar logs de auditoria. Controlar processo de inseminação	I	TSE não demonstrou ou autorizou averiguar posteriormente a qualidade e integridade do procedimento e cadastros (item 4).

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
4.9	Prover Transportador de Dados: Leitura do flash (arquivos e BU) e transmissão para o centro de totalização, em computador da Justiça	I	TSE não demonstrou ou autorizou averiguar posteriormente a qualidade e integridade do procedimento e cadastros (item 4).
4.10	Prover Totalizador de Dados: Recepção nos TRE´s dos dados enviados pelo transportador, deciframento dos BUs extração dos dados e totalização, acumulação de votos, atualização do banco de dados, divulgação do resultado. Totalização nas zonas, TREs ou TSE conforme eleição.	I	TSE não demonstrou ou autorizou averiguar posteriormente a qualidade e integridade do procedimento e cadastros (item 4).
5	**URNA – PREPARAÇÃO E OPERAÇÃO**		
5.1	Prover serviços técnicos para manutenção das urnas.	I	TSE não demonstrou terem sido seguidos procedimentos considerados entre as melhores práticas (item 4).
5.2	Preparação: Prover serviços técnicos para preparação e instalação das urnas. Preparar para votação. Inserir flash de carga em slot externo e ligar urna, programa transfere sistema operacional e controles. Inserir flash de votação, programa verifica integridade, preparação final para votação.	I	TSE não demonstrou fundamentação para contratações, por exemplo da empresa Smartmatic, sendo que tais empresas têm acesso à gravação dos programas das urnas eletrônicas. A Auditoria Especial não teve acesso profundo (perícia) às mídias gravadas por essas empresas (item 4.4.5.2).
5.2	Preparação: Controle de armazenamento, distribuição e acompanhamento das urnas	I	TSE não demonstrou terem sido seguidos procedimentos considerados entre as melhores práticas (item 4).
6	**AVALIAÇÃO DO SISTEMA ELEITORAL**		
6.1	Dar publicidade aos procedimentos oficiais e aos resultados da eleição	C	TSE demonstra publicidade e transparência de normas e registros oficiais (item 4.4.4.1).

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
6.2	Comprovar transparências na execução dos contratos conforme Art. 39.da Lei 8666, determinações CNJ e princípios da Administração Pública	I	A Auditoria Especial solicitou, mas não teve acesso aos registros administrativos sobre os serviços prestados ao TSE. A Auditoria Especial identificou situações onde o código-fonte recebido de fornecedores não foi devidamente conferido (item 4).
6.3	Preservar sistemas e dados eleitorais para auditoria	NC	Auditoria comprovou que não foram preservados códigos-fonte do CEPESC/ABIN, da BIOS das urnas e do *firmware* do componente de segurança MSD (itens 4.3.4, 4.4.2.5.1).
6.4	Comprovar Inexistência de *software*, funções ou dados ocultos na urna	I	TSE não conseguiu demonstrar inexistência de *software* secreto ou indevido na urna.
6.5	Comprovar inexistência de *software*, funções ou dados ocultos nos módulos de CEPESC/ABIN	I	TSE não conseguiu demonstrar inexistência de funções ou códigos ocultos nos programas executáveis utilizados ou integrados ao longo de todo o sistema eleitoral (item 4).
6.6	Comprovar integridade e ausência de inserção de funções, *software* ou dados ocultos via rotinas de compilação	NC	TSE não preservou programas e procedimentos de compilação (itens 4.4.2.6, 4.3.4).
6.7	Comprovar inexistência de procedimentos indevidos nos programas e dados das urnas eletrônicas	I	TSE não conseguiu comprovar inexistência e também não forneceu os registros pertinentes à Auditoria Especial (item 4.4.5.1).
6.8	Comprovar integridade e não violação de lacres físicos das urnas	NC	A Auditoria Especial constatou haver alto índice de urnas com lacres violados (item 4.4.2.10).
6.9	Comprovar qualidade e integridade do código-fonte desenvolvido por TSE ou por terceiros	NC	A Auditoria Especial constatou haver baixa qualidade no código-fonte, claramente desorganizado e sujeito a falhas (item 4.4.2.4).

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
6.10	Comprovar correção, segurança e ausência de vulnerabilidades no código-fonte	NC	O TSE não conseguiu comprovar para a Auditoria Especial a inexistência de erros ou fraudes no código-fonte; também não demonstrou adotar métodos e mecanismos para identificar erros e fraudes. Além disso, o TSE não forneceu todos os códigos para análise (BIOS, *firmware*), nem preservou os códigos da CEPESC/ABIN. TSE impôs à Auditoria Especial métodos, ferramentas, local e tempo incompatíveis com o volume de código a ser verificado. Mesmo com essas limitações, a Auditoria Especial encontrou vulnerabilidades diversas nos pequenos trechos que foi possível avaliar (4.4.2.5).
6.11	Comprovar gerenciamento de programas de terceiros	NC	Não há controle sobre o compilador utilizado (item 4.4.2.6).
6.12	Comprovar que compilação posterior do código-fonte preservado gera executável aderente ao utilizado na votação.	I	TSE não conseguiu comprovar (itens 4.4.2.6, 4.4.2.7).
6.13	Comprovar correta geração de programas para as urnas eletrônicas	I	TSE não conseguiu comprovar e não forneceu à Auditoria Especial acesso às mídias das urnas eletrônicas (itens 4.4.5.1, 4.3.4)
6.14	Comprovar integridade dos programas gravados nas urnas eletrônicas	NC	TSE não conseguiu comprovar e foram identificadas fragilidades na certificação do *software*, ausência de rastreabilidade do programa VPP, ausência de verificação de memória de modo independente, alto índice de lacres violados (4.4.2.8, 4.4.2.3, 4.3.4).
6.15	Comprovar integridade da totalização dos Boletins de Urna	C	Não foram localizadas evidências de graves problemas nesse ponto (item 4.4.4.2).
6.16	Comprovar sigilo do Voto	C	Não foram localizadas evidências de graves problemas nesse ponto.

	REQUISITOS	AVALI-AÇÃO	PRINCIPAIS REFERÊNCIAS
6.17	Comprovar origem e integridade do código-fonte e rotinas executáveis do CEPESC utilizadas na eleição	NC	Não há rastreabilidade do código da CEPESC utilizado, um requisito imprescindível (item 4.3.4).
6.18	Comprovar que a votação paralela atinge o objetivo de demonstrar segurança e integridade do sistema eleitoral	NC	Demonstrado que, ao monitorar o ecossistema (isto é, diversos e distintos tipos de dados que o equipamento recebe durante o ciclo de vida das eleições), a urna pode identificar o estado de votação paralela e ocultar funções ou códigos fraudulentos. Portanto, a votação paralela não atinge seu objetivo principal (item 4.4.2.11).
6.19	Comprovar efetividade da Auditoria e Controle Interno do TSE	I	O TSE não demonstrou que sua Área de Auditoria e Controle Interno tenha efetiva atuação na análise e averiguação das muitas denúncias e que empreenda investigações independentes quando há possibilidade de fraude mediante alta tecnologia (item 4.4.2.11.3).
6.20	Comprovar independência das funcionalidades do sistema eleitoral com relação aos fornecedores de componentes do sistema	NC	TSE não apresentou funções eficazes que assegurem de forma transparente a independência do sistema eleitoral com relação às rotinas e processos indevidos eventualmente embutidos nos componentes entregues por fornecedores. Este requisito torna-se grave diante da ausência de outros controles, como voto impresso, obscurantismo e ocultação do código-fonte e compilação dos programas, dependência de assinaturas digitais e outras questões similares (item 4).

Esses resultados estão fundamentados no corpo do relatório.

3.1. Avaliação sobre Governança

Há diversos anos o TSE faz investimentos relevantes no sentido de aprimorar a governança do sistema eleitoral brasileiro, de tal maneira que esse esforço deveria ter trazido, entre outros benefícios obrigatórios, a criação de mecanismos eficazes para apurar e responder com transparência as denúncias e insatisfações da população brasileira, afastando omissões em trilhas de auditoria ou eventuais enfoques incorretos que impeçam ou dificultem apurações exemplares.

As avaliações realizadas ao longo da presente Auditoria Especial, no entanto, indicam que o TSE não atingiu os objetivos que estabeleceu a respeito da sua Governança Corporativa para o período de 2011 a 2014.

Como consequência dessas deficiências em governança, o próprio TSE, os Juízes, a Auditoria Interna e a Ouvidora do TSE, o Ministério Público, a OAB e as empresas externas de auditoria contratadas pelo TSE para a votação paralela deixaram de responder de forma transparente às denúncias em questão. Além disso, obstáculos existentes, cujas remoções eram necessárias para a conclusão da presente Auditoria Especial, não foram superados.

Ao impedir parte relevante dos procedimentos de auditoria e ao deixar de responder os questionamentos apresentados, a infraestrutura do TSE demonstrou inadimplemento quanto ao seu próprio Planejamento Estratégico, portanto à sua missão, visão e valores, além de violar as regras de governança em prejuízo da transparência e da credibilidade do sistema eleitoral brasileiro, conforme exposto nos próximos itens.

3.2. Governança do Sistema Eleitoral

O TSE produziu em 2010 um documento intitulado “Planejamento Estratégico do TSE 2011/2014” que estabelece Missão, Visão e Valores transcritos a seguir[4], onde grifamos os atributos de interesse para a presente Auditoria Especial:

> *Missão: Garantir a legitimidade do processo eleitoral e o livre exercício do direito de votar e ser votado, a fim de fortalecer a democracia.*
> *Visão em 2014: Consolidar a **credibilidade** da justiça eleitoral, especialmente quanto à efetividade, à **transparência** e à **segurança**.*

4 Planejamento Estratégico do TSE disponível em http://www.tse.jus.br/arquivos/tse-planejamento-estrategico-do-tse-2012-2014/view

> *Valores:*
> *COERÊNCIA: **alinhamento entre discurso e prática**;*
> *COMPROMETIMENTO: atuação com dedicação, empenho e envolvimento em suas atividades;*
> *ÉTICA: atuação sob os princípios da honestidade, lealdade e dignidade;*
> *FLEXIBILIDADE: atitude de abertura permanente para compreender a necessidade de mudanças, adotando medidas para promovê-las;*
> *INOVAÇÃO: estímulo à criatividade e à busca de soluções diferenciadas;*
> *INTEGRAÇÃO: compartilhamento de experiências, conhecimentos e ações que conduzam à formação de equipes orientadas para resultados comuns;*
> *RECONHECIMENTO: adoção de práticas de estímulo e valorização das contribuições individuais e de grupos que conduzam ao cumprimento da missão do TSE.*

O Planejamento Estratégico do TSE é claro ao estabelecer Missão, Visão e Valores e caracterizar a subordinação do Tribunal ao eleitor, fim último do sistema eleitoral. Logo, o Planejamento Estratégico configura a obrigação do Tribunal quanto à credibilidade, transparência, segurança e alinhamento entre discurso e prática naquilo que interessa ao eleitor, configurando a obrigação não só de apurar quaisquer denúncias, mas também de divulgar para o eleitor com a máxima transparência os exames e os resultados obtidos, mesmo se de intricada natureza tecnológica.

Ocorre que a Auditoria Especial não conseguiu comprovar respostas transparentes, espontâneas, técnicas e profundas do TSE frente às denúncias propagadas pelos eleitores na Internet. Entende-se que esses eleitores são os demandantes efetivos e reais do Planejamento Estratégico do TSE para o período 2011/2014, logo, seus objetivos deveriam ter sido alcançados e estar implantados e disponíveis em tempo para a eleição de 2014.

Em vez de encontrar as portas abertas ao apoiar o TSE na consecução do seu Planejamento Estratégico, no que se refere à apuração transparente para o eleitor, a Auditoria Especial foi fortemente limitada em suas ações e impelida de fato a se afastar da sua missão de conduzir verificação técnica profunda sobre credibilidade, transparência, segurança e alinhamento entre discurso e prática no sistema eletrônico eleitoral.

3.3. Conformidade Frente às Regras Gerais de Governança

A Resolução 99/2009[5] estabelece que cabe ao Conselho Nacional de Justiça (CNJ) prover soluções tecnológicas efetivas para o Poder Judiciário e agir para que ele seja reconhecido por transparência, imparcialidade, comunicação com públicos externos, documentação adequada dos sistemas e aderente às melhores práticas de segurança da informação.

A análise dessa resolução do CNJ é importante para que se compreenda a extensão do Plano Estratégico e os compromissos de Governança do TSE e seus reflexos na eficácia e transparência da apuração de denúncias.

Há cerca de 15 anos têm sido feitos registros que atribuem ao TSE problemas típicos de Governança nos quesitos, falta de transparência, falta de empenho e parcialidade na apuração de denúncias dos eleitores que são tecnicamente materializadas por meio de artigos científicos ou técnicos, auditorias independentes ou notícias na imprensa, como nos exemplos a seguir.

- Em 2001, artigo "Voto Eletrônico – Processo Eleitoral Brasileiro"[6], de Evandro Luiz de Oliveira, afirma que: (i) não é dado o direito aos representantes partidários de verificarem todos os programas que fazem parte do processo eleitoral; (ii) o prazo dado legalmente para verificação é exíguo; (iii) não existe nenhum mecanismo que garanta que o que está sendo verificado é o mesmo que será colocado nas urnas algumas semanas depois; e (iv) o processo eleitoral é um sistema baseado em premissas obscurantistas;
- Em 2002, relatório COPPETEC[7] relata sobre o sistema eleitoral: (i) as especificações são inadequadas, incompletas e inconsistentes; (ii) a documentação dos testes é incompleta e não foi possível examinar sua adequação e cobertura; (iii) não se pode fazer afirmativas sobre a confiabilidade do produto; (iv) nos testes, o produto não estava pronto e nada se pode garantir sobre ele; e (v) o TSE não permitiu a utilização de ferramentas de extração de métricas nos testes;

5 CNJ - Resolução número 99/2009 – Disponível em http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/rescnj_99.pdf

6 Artigo "Voto Eletrônico – Processo Eleitoral Brasileiro", publicado em revista IP, da Prodabel, Belo Horizonte, 2001, ISBN 1516-697X,

7 "Relatório de Avaliação do *Software* do TSE realizada pela Fundação COPPETEC", agosto de 2002, Fundação COPPE, UFRJ

- Em 2002, relatório da Unicamp[8] informa que: (i) o TSE não formaliza o ciclo de desenvolvimento do *software* da urna e de outros programas em procedimentos e marcos; (ii) deve ser aprimorado o exame dos programas-fonte pelos partidos; (iii) a configuração do ambiente de compilação deve ser completamente documentada; (iv) deve ser possível a reprodução do mesmo ambiente de compilação; (v) devem ser disponibilizados recursos para que a compilação dos programas e cálculos possam ser feitos em paralelo por representantes dos partidos, em ambientes gerados por eles mesmos;
- Em 2007/2008, a Subcomissão Especial de Segurança do Voto Eletrônico da Câmara dos Deputados[9] recomenda a criação de auditoria independente do *software* das urnas eletrônicas;
- Em 2009, o relatório CMind[10] afirma que: (i) não se pode perder a vigilância quanto ao aspecto da confiabilidade do processo; (ii) pode-se inferir que a falta de interesse na fiscalização significa a aceitação tácita dos procedimentos executados nas eleições; (iii) não é escusa aceitável a alta complexidade técnica dos procedimentos envolvidos na votação eletrônica para que os partidos deixem de fiscalizar e aferir a confiabilidade do processo eleitoral;
- Em 2010, o relatório Cmind[11] afirma: (i) há comprometimento do princípio da publicidade e soberania do eleitor em conhecer o destino do voto; (ii) é impossível conferir e auditar o resultado da apuração eletrônica dos votos; (iii) é necessário separar tarefas de normatizar, administrar e auditar o processo eleitoral; (ii) devem ser totalmente separadas a estrutura administrativa eleitoral, as funções de projeto, de operação e de auditoria interna; (iii) é necessário possibilitar auditoria externa totalmente independente das pessoas envolvidas na administração; (iv) não podem ser estabelecidas pelos próprios administradores e operadores as regras de fiscalização e auditoria;
- Em 2013, artigo de Diego Aranha[12] afirma: (i) um período de 3 dias é absolutamente insuficiente para se analisar uma porção significativa do código-fonte da

8 Relatório “Avaliação do Sistema Informatizado de Eleições”, Unicamp, maio 2002

9 Câmara dos Deputados, Subcomissão Especial de Segurança do Voto Eletrônico. Dois relatórios aprovados na CCJC – CCJC 2007 e CCJC 2008

10 “Relatório sobre o Sistema Brasileiro de Votação Eletrônica”, março 2009, Comitê Multidisciplinar Independente

11 “Relatório sobre o Sistema Brasileiro de Votação Eletrônica”, Brasília, 2010, Comitê Multidisciplinar Inde-pendente – CMind, Sérgio Sérvulo da Cunha et al..

12 “Vulnerabilidades no *software* da urna eletrônica brasileira”, Diego F. Aranha et al. Março 2013

> urna eletrônica, que em seu total possui milhões de linhas de código; (ii) avaliação completa e cuidadosa do *software* da urna requer enorme esforço e muito tempo de dedicação; (iii) sem a possibilidade de se efetuar testes extensos e sem qualquer tipo de restrição, segundo metodologia científica, não é possível afirmar que o formato atual do evento [teste] colabora significativamente para o incremento da segurança da urna eletrônica.

Verifica-se como alvo comum a todas essas críticas a imposição de métodos que de uma forma ou de outra cheguem sempre à conclusão de que o sistema eleitoral é seguro. Em outras palavras, são banidos quaisquer métodos que possam identificar e comprovar falhas da infraestrutura tecnológica do TSE. A justificativa para cercear os trabalhos de investigação também se mantém constante, sempre focada na pretensa proteção do próprio sistema eleitoral contra a cópia ou divulgação das suas informações técnicas que poderiam ser utilizadas para perpetrar fraudes contra o sistema.

Ocorre que, como demonstrado neste relatório, essa postura mundialmente não é mais considerada consistente, ao contrário, indica, como regra, a vontade de pessoas ou órgãos de ocultar suas falhas em vez de efetivamente proteger o sistema. A segurança dos sistemas há muito tempo não está no obscurantismo[13] que apenas oculta erros e fraudes, mas sim na adoção de melhores práticas e técnicas.

Essa postura de ofuscação e limitação imposta judicialmente ou administrativamente pelo Tribunal às auditorias se baseia em pareceres técnicos, requerimentos e pedidos que partem das próprias áreas técnicas que precisam ser alvo de auditoria para apurar as denúncias, tendo como resultado efetivo criar um manto de “inauditabilidade” incompatível com as determinações do Poder Judiciário e com a Administração Pública sobre transparência dos atos e apuração das denúncias.

Como já foi visto, o Artigo 11 da Resolução CNJ 90/2009 determina que o Planejamento Estratégico de Tecnologia da Informação e Comunicações (PETI) de cada Tribunal deve se manter alinhado com as diretrizes estratégicas institucionais e nacionais e determina, ainda, que cada Tribunal deve elaborar um plano diretor de Tecnologia da Informação e Comunicação (PDTI).

Verifica-se que o TSE buscou atender essa Resolução do CNJ quanto ao seu aspecto formal, primeiramente elaborando uma versão denominada “Planejamento Es-

13 O Princípio de Kerckhoffs, que discute a falácia da “segurança do obscurantismo”, foi originalmente enunciado em 1883. : "Kerckhoffs, A. La cryptographie militaire. Journal des sciences militaires, IX:5–83 (Jan), 161–191 (Feb), 1883"

tratégico de TI para 2010/2014”[14] e depois a aperfeiçoando. Esse documento registra que em 2010 o TSE detectou na sua infraestrutura as seguintes “fraquezas” que são de interesse para esta Auditoria Especial:

- *Deficiência na gestão de contratos de mão de obra terceirizada;*
- *Ausência de gestão de demandas, tais como: níveis de serviço, capacidade de atendimento e priorização;*
- *Ausência de gestão eficaz do conhecimento;*
- *Conhecimento e planejamento deficientes em relação ao processo de aquisição;*
- *Ausência de critérios vinculados a fornecimento de informações;*
- *Transitoriedade da alta gestão do TSE, ocasionando uma possível quebra de continuidade nos trabalhos da Secretaria;*
- *Mudanças intempestivas na legislação eleitoral;*
- *Monopólios e cartelização de fornecedores;*
- *Baixa integração entre as unidades de TI da Justiça Eleitoral;*
- *Ausência de critérios objetivos acerca do compartilhamento das boas práticas da Justiça Eleitoral.*

Em seguida o TSE criou seu Planejamento Estratégico para o período 2011 a 2014 de forma tal que essas e outras “fraquezas” estivessem resolvidas até as eleições de 2014.

Contudo, não se confirmou o alcance dessas metas, dado que a Auditoria Especial encontrou na eleição de 2014 problemas muito similares ou decorrentes das chamadas “fraquezas” de 2010, como demonstrado no capítulo 3.8 deste documento (p. 37), em síntese:

a) Utilização de interpretação excessivamente restritiva da legislação e das normas com o objetivo de limitar ou mesmo anular a eficácia das auditorias externas e perícias técnicas;
b) Aparente inoperância da auditoria interna, do Poder Judiciário, do Ministério Público e da OAB no que se refere às investigações e apuração de denúncias envolvendo a alta tecnologia utilizada no sistema eleitoral;

14 Planejamento Estratégico de TI 201/2014 do TSE- Disponível em https://groups.google.com/forum/#!topic/tse-ti2012/PKDtYlOxYls

c) Obscurantismo via não fornecimento à Auditoria de informações e documentos técnicos efetivos e originais de projeto, sendo fornecidos apenas material ilustrativo e construído propositalmente para demonstração em auditorias ou divulgação pública;
d) Proibição de utilizar métodos e técnicas investigativas efetivamente livres e apropriadas aos exames, limitando tempo, local, métodos e objetos àqueles previamente autorizados, configurando o controle da auditoria pelo próprio auditado;
e) Não fornecimento de arquivos digitais do sistema e do seu ambiente real de especificação, projeto, desenvolvimento, manutenção, teste, homologação e operação/produção, frustrando a efetiva e real averiguação das denúncias;
f) Não fornecimento de cópias de programas-fonte, mesmo sendo livres, e demais arquivos para exame efetivo no laboratório dos auditores, sendo autorizadas apenas análises parciais notoriamente insuficientes e inadequadas para auditoria verdadeira do sistema;
g) Proibição do exame de diversos componentes do sistema eleitoral;
h) Respostas vagas para os questionamentos apresentados.

Esse bloqueio ao trabalho da Auditoria Especial ocorreu de modo uniforme tanto junto aos diversos órgãos técnicos que integram o TSE em Brasília, quanto nos TRE's e cartórios visitados pelos auditores, demonstrando intensa coesão administrativa entre esses diversos órgãos e unidades da corporação no sentido de se cumprir com forte alinhamento as diretrizes centrais da organização. Todavia, essa linha de ação foi utilizada em desfavor da transparência e da governança voltada ao eleitor, fim último da existência da Justiça Eleitoral e da Administração Pública.

Paradoxalmente, o TSE tem instituído diversos projetos relacionados à implementação da Governança Corporativa visando à transparência junto ao eleitor. A Portaria nº 606/2011 do TSE criou uma comissão de estudos sobre governança e em 2012 instituiu o Sistema Gerencial de Governança Corporativa (SGGC)[15].

Ainda em 2012, o TSE avaliou sua própria governança e publicou o resultado no documento denominado "Avaliação do Sistema Gerencial de Governança Corporativa do TSE – 04/2012", reproduzido a seguir[16] e mais detalhadamente nas seções seguintes para melhor visualização:

15 Disponível em http://www.justicaeleitoral.jus.br/arquivos/governanca-corporativa-v1

16 Disponível em http://www.justicaeleitoral.jus.br/arquivos/tse-avaliacao-sggc-04-12

Avaliação do Sistema Gerencial de Governança Corporativa do TSE - 04/2012

Dimensão	Categoria	Elemento	Assessment
Alinhamentos	A.1 Alinhamento estratégico	A.1.1 Definição da Missão e Visão	5
		A.1.3 Elaboração do Planejamento Estratégico	5
		A.1.3 Acompanhamento e monitoramento dos indicadores estratégicos	4
	A.2 Alinhamento de conduta	A.2.1 Valores	5
		A.2.2 Código de Conduta e Ética	2
	A.3 Alinhamento organizacional	A.3.1 Regimento interno	3
		A.3.2 Regulamento da Secretaria	3
		A.3.3 Organograma da Secretaria	2
	A.4 Processo de transição	A.4.1. Grupo de transição	1
Conformidades	C.1 Transparência	C.1.1 Página de transparência	5
		C.1.2 Página de estatísticas eleitorais	5
		C.1.3 Página de estatísticas processuais e de julgamentos	3
		C.1.4 Publicação online de projetos básicos e termos de referência	3
	C.2 Prestação de contas eleitorais e partidárias	C.2.1 Prestação de contas e relação de processos partidários	5
		C.2.2 Prestação de contas e relação de processos eleitorais	5
	C.3 Relatórios de gestão	C.3.1 Processo de contas	5
		C.3.2 Relatórios da LRF	5
	C.4 Conformidade normativa	C.4.1 Conformidade com leis, resoluções do CNJ e outras normas	1
Sustentabilidade	S.1 Responsabilidade social	S.1.1. Tribunal Aberto à Comunidade	2
	S.2 Responsabilidade ambiental	S.2.1 Combate ao Desperdício e Apoio à Sustentabilidade	3
	S.3. Ouvidoria	S.3.1 Central do Eleitor	5
Estruturas	E.1 Comitês	E.1.1 Comitê executivo	5
		E.1.2 Comitê Gestor de Tecnologia da Informação	3
	E.2 Escritório de Projetos	E.2.1 Metodologia de Gerenciamento de Projetos	5
	E.3 Auditoria	E.3.1 Vinculação do Controle Interno e Auditoria à Presidência	1
		E.3.2 Fiscalização de contratos	4
		E.3.3 Núcleo de Gestão de Risco	1
	E.4 Segurança da Informação	E.4.1 Comissão de Segurança da Informação no Tribunal	2
Processos	P.1 Análise e melhoria de processos	P.1.1 Escritório de Processos Organizacionais	5
		P.1.2 Escritório de Gestão de Qualidade	4
	P.2 Gestão de contratos	P.2.1 Manual de gestão de Contratos Administrativos na JE	4
		P.2.2 Manual de aplicação de sanções em licitações e contratos	2
	P.3 Avaliações	P.3.1 Avaliação de competências	5
		P.3.2 Avaliação gerencial	5
		P.3.3 Programa de formação de lideranças	5
		P.3.4 Escola de gestão	5
	P.4. Governança em Tecnologia da Informação	P.4.1 Governança em Tecnologia de Informação	1
		P.4.2 Processo judicial e administrativo eletrônico	2

Esse documento registra que em 2012 o TSE tinha diversos problemas de governança relacionados ao não atendimento dos preceitos que devem cercar a auditoria e transparência do sistema eleitoral. Ocorre que em 2015 a Auditoria Especial constatou a respeito da eleição majoritária de 2014 que os mesmos tipos de problemas continuam prejudicando a realização de auditorias, a apuração eficaz de denúncias técnicas e a transparência na comunicação com o eleitor denunciante.

Portanto, os problemas apontados neste relatório pela Auditoria Especial são conhecidos há anos pelo TSE, constavam em seus registros como não resolvidos pela Administração, a despeito de haver críticas formalizadas, e continuam não resolvidos.

3.4. Conformidade com Leis, Resoluções e Normas

Os trabalhos da Auditoria Especial foram dificultados ou impedidos por interpretações das normas que se mostraram, sob o aspecto técnico**,** distantes dos princípios sobre o dever de transparência da Administração Pública. Esse entendimento é aderente à autoavaliação sobre governança no TSE na dimensão intitulada "Alinhamentos".

A categoria denominada pelo TSE como "C.1 Transparência" se refere explicitamente à publicação de dados oficiais na Internet e apresenta avaliações máximas, com nota 5, para "Página de transparência" e "Página de estatísticas eleitorais". Como se sabe, essas páginas são essenciais para a transparência do processo eleitoral, mas não são elas próprias objeto das denúncias.

As denúncias referem-se, principalmente, a supostas manipulações no próprio sistema eletrônico eleitoral. Porém, a Auditoria Especial foi impedida de acessar livremente e realizar os exames periciais adequados para avaliar esse sistema, configurando, portanto, descumprimento dos órgãos técnicos do TSE quanto ao requisito de transparência.

Esta realidade está em consonância com a própria autoavaliação do TSE que, em "C.4 Conformidade normativa" e em seu único elemento "C.4.1 Conformidade com leis, resoluções do CNJ e outras normas", se atribui avaliação negativa, com a nota mínima 1.

Conformidades	C.1 Transparência	C.1.1 Página de transparência	5
		C.1.2 Página de estatísticas eleitorais	5
		C.1.3 Página de estatísticas processuais e de julgamentos	3
		C.1.4 Publicação online de projetos básicos e termos de referência	3
	C.2 Prestação de contas eleitorais e partidárias	C.2.1 Prestação de contas e relação de processos partidários	5
		C.2.2 Prestação de contas e relação de processos eleitorais	5
	C.3 Relatórios de gestão	C.3.1 Processo de contas	5
		C.3.2 Relatórios da LRF	5
	C.4 Conformidade normativa	C.4.1 Conformidade com leis, resoluções do CNJ e outras normas	1

3.5. Qualidade da Informação Pública sobre o Sistema Eleitoral

Os trabalhos realizados pela presente Auditoria Especial refletem os anseios dos eleitores que se manifestaram amplamente a respeito de denúncias sobre o sistema eleitoral.

Tratando-se de interesse público criado, mantido e operado pelo TSE, cumpre recordar que a Lei de Acesso à Informação Pública (Lei n.º 12.527/2011) determina que:

> *É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.*

Entende esta Auditoria Especial que essa norma impõe a obrigação de divulgar, independentemente de requerimentos, os exames técnicos e demais providências relacionadas à apuração das denúncias e a fundamentação técnica sobre sua confirmação ou desmentido.

Entretanto, ao contrário do que determina essa norma, houve grande dificuldade para se obter do agente público as permissões para examinar informações efetivamente esclarecedoras. As informações apresentadas aos auditores, muitas vezes, foram vagas e superficiais, insuficientes para embasar apurações efetivas e esclarecer de fato os eleitores.

Esse entendimento da Auditoria Especial é consistente com a autoavaliação do TSE realizada em 2012, que reconhece como muito baixa (nota 2) - categoria “S.1

Responsabilidade social/S.1.1 Tribunal Aberto à Comunidade” – a transparência do Tribunal:

Sustentabilidade	S.1 Responsabilidade social	S.1.1. Tribunal Aberto à Comunidade	2
	S.2 Responsabilidade ambiental	S.2.1 Combate ao Desperdício e Apoio à Sustentabilidade	3
	S.3. Ouvidoria	S.3.1 Central do Eleitor	5

3.6. Gestão de Riscos na Estrutura do TSE

Na dimensão intitulada “Estruturas”, o TSE apresenta indicadores de grande relevância para a presente Auditoria Especial, confirmando as evidências apontadas nos demais capítulos deste documento.

Primeiramente, cabe notar a avaliação máxima (nota 5) atribuída ao Comitê Executivo do TSE, instância deliberativa interdisciplinar responsável por sanar questões críticas que possam impactar o sucesso de projetos e programas, estabelecendo critérios de priorização e definindo alternativas frente a riscos e problemas em projetos[17]. Confrontando-se a elevada avaliação em governança obtida pelo COMEX com a ausência de respostas efetivas para os problemas apontados neste e nos anteriores relatórios de auditora, se verifica nas normas que cabe a esse organismo responder questões afeitas ao Escritório Corporativo de Projetos (ECP), ao Escritório de Processos Organizacionais (EPO) e ao Escritório de Gestão da Qualidade (EGQ), sugerindo haver foco apenas nas questões eminentemente internas e não em respostas às denúncias externas envolvendo os próprios sistemas e procedimentos internos.

Essas questões contraditórias surgem dentro da mesma categoria “E.1 Comitês”, pois o Comitê Gestor de Tecnologia da Informação, diretamente relacionado à presente Auditoria Especial, apresentou avaliação de governança bem abaixo (nota 3).

As demais avaliações apresentam quadros bem mais graves, exatamente nos aspectos que demandam decisões e ações dos Comitê Executivo e Comitê Gestor de Tecnologia da Informação.

O TSE obteve avaliação extremamente baixa (nota 1) no quesito “Vinculação do Controle Interno e Auditoria à Presidência”, fator que poderia ser entendido, em tese,

17 Comitê Executivo COMEX – vide http://www.tse.jus.br/institucional/planejamento-e-gestao/governanca-corporativa/elementos/estrutura

como benéfico se ele indicar independência da auditoria interna em relação à própria estrutura administrativa (Presidência); contudo, as notas ruins nos demais indicadores de governança e a falta de solução para os problemas identificados nesta Auditoria Especial e nas auditorias externas anteriores não permitem entendimento distinto, remanescendo que a nota 1 atribuída para Controle Interno e Auditoria de fato representa deficiência de governança nessa função.

Além da nota mediana (nota 3) obtida pelo Comitê de TI, responsável por monitorar e acompanhar os projetos de tecnologia da informação, considera-se marcante a avaliação extremamente baixa (nota 1) para o Núcleo de Gestão de Riscos, isto é, a avaliação de governança do TSE confirma a existência de deficiências exatamente nos pontos críticos salientados na presente Auditoria Especial, pontos que comprometem a credibilidade e não permitem atestar a integridade da Urna Eletrônica e dos sistemas de votação, apuração e totalização.

Estruturas	E.1 Comitês	E.1.1 Comitê executivo	5
		E.1.2 Comitê Gestor de Tecnologia da Informação	3
	E.2 Escritório de Projetos	E.2.1 Metodologia de Gerenciamento de Projetos	5
	E.3 Auditoria	E.3.1 Vinculação do Controle Interno e Auditoria à Presidência	1
		E.3.2 Fiscalização de contratos	4
		E.3.3 Núcleo de Gestão de Risco	1
	E.4 Segurança da Informação	E.4.1 Comissão de Segurança da Informação no Tribunal	2

Figura 1 - Avaliação de governança - Estruturas - fonte TSE

Não se pode deixar de constatar que as baixas notas sobre governança apontadas pelo próprio TSE, inclusive sobre riscos, deficiências em segurança da informação e insuficiência de controles internos (Figura 1, p. 35), e as frequentes críticas em relatórios de auditoria de terceiros, apontam para a necessidade de averiguação e providências específicas dos órgãos competentes do Tribunal[18].

3.7. A Governança de TI no Sistema Eleitoral

Especificamente quanto à tecnologia da informação, o Conselho Nacional de Justiça (CNJ) estabeleceu na Resolução 90/2009[19] os requisitos de nivelamento de tecnologia da informação no âmbito de todo o Poder Judiciário e, entre outras providências,

18 Vide http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-no-23-416-de-20-de-novembro-de-2014-brasilia-df

19 CNJ Resolução 90/2009 – Disponível em http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_90_29092009_02012013134629.pdf

determinou que cada Tribunal deve elaborar e manter um Planejamento Estratégico de TIC – PETI devidamente alinhado às diretrizes estratégicas institucionais e nacionais, sendo que essa mesma Resolução (Art. 15) concede ao TSE propor normas específicas sobre Tecnologias da Informação e das Comunicações (TIC) para o respectivo segmento, podendo também recomendar uso de estruturas e serviços de tecnologia disponíveis. Consta na norma que, nesse caso, cabe ao CNJ manter banco das melhores práticas e que definirá requisitos para atestar a conformidade de sistemas de automação judicial, conferindo selo a esse respeito.

Não restou claro para a presente Auditoria Especial o alcance das normas do CNJ com relação ao próprio sistema eletrônico eleitoral. A Auditoria Especial também não teve acesso a um possível "Selo" que o CNJ teria concedido ao TSE sobre as melhores práticas para o sistema eleitoral e urna eletrônica, uma vez que esse "Selo" constituiria um requisito obrigatório caso o TSE pretendesse se submeter apenas às suas normas particulares sobre Tecnologia da Informação.

Como poderá ser verificado no corpo do presente relatório, a Auditoria Especial foi impedida de realizar exames, recebeu esclarecimentos técnicos muitas vezes superficiais e vagos e não teve acesso a documentos técnicos supostamente existentes em função de normas específicas do TSE que não seguem integralmente as diretrizes de transparência do Poder Judiciário. Considera-se que o problema está relacionado ao papel múltiplo do TSE enquanto elaborador e aplicador de normas, fiscalizador do seu cumprimento e operador do sistema eleitoral.

A autoavaliação sobre governança no TSE realizada em 2012 mostra avaliações máximas (nota 5) para o Escritório de Processos Organizacionais, para a Escola de Gestão e para as questões gerenciais e de competências, o que se mostra coerente com o forte espírito de equipe demonstrados pelos técnicos do TSE e TRE's que atenderam os auditores desta Auditoria Especial.

Contudo, o estudo do TSE sobre sua própria governança confirma a existência de problemas graves nas questões que podem ser críticas para a integridade do sistema eleitoral. Foi atribuída ainda em 2012 nota péssima (nota 1) exatamente para a "Governança em Tecnologia da Informação", o que, em tese, permanece e atualmente se mostra coerente com as deficiências na Governança em TI identificadas na presente Auditoria Especial com respeito à transparência com o eleitor e cerceamento na averiguação das denúncias.

A falta de conformidade nas questões de Governança de TI remete a problemas graves como aqueles relacionados à não comprovação pelo TSE de efetivos controles

sobre os módulos e componentes de *software* que são fornecidos por terceiros para compor o sistema eleitoral, comprometendo a credibilidade e integridade de todo o sistema. Constatações desse tipo pela atual Auditoria Especial são coerentes com a má avaliação (nota 2) apurada em 2012 no que se refere à falta de aplicação de sanções em licitações e contratos. A carência de controles efetivos, por exemplo, no código-fonte de programas criados e mantidos por terceiros e que integram a Urna Eletrônica pode perpetuar fragilidades e dar abertura para fraudes por ausência de sanções que deveriam ser aplicadas a cada falha, além de sugerir possíveis conivências:

Processos	P.1 Análise e melhoria de processos	P.1.1 Escritório de Processos Organizacionais	5
		P.1.2 Escritório de Gestão de Qualidade	4
	P.2 Gestão de contratos	P.2.1 Manual de gestão de Contratos Administrativos na JE	4
		P.2.2 Manual de aplicação de sanções em licitações e contratos	2
	P.3 Avaliações	P.3.1 Avaliação de competências	5
		P.3.2 Avaliação gerencial	5
		P.3.3 Programa de formação de lideranças	5
		P.3.4 Escola de gestão	5
	P.4. Governança em Tecnologia da Informação	P.4.1 Governança em Tecnologia de Informação	1
		P.4.2 Processo judicial e administrativo eletrônico	2

Figura 2 - Avaliação de governança - Processo - fonte TSE

A esse respeito, mais recentemente a Portaria número 490, de 08 de outubro de 2013, instituiu mais um grupo de trabalho incumbido de realizar estudos e propor orientações para fomentar a implantação de Governança de TI nos tribunais eleitorais [20].

3.8. Governança de TI e o Sistema Operacional da Urna

Sistema operacional é um programa vital responsável pelas funções básicas de um computador. Basicamente, ele estabelece o início das operações, controla teclado e vídeo, comanda o funcionamento dos demais programas e cuida da integridade do equipamento.

A importância das funções executadas pelo sistema operacional torna imprescindível seu exame detalhado para assegurar a correta averiguação das denúncias. Porém, esse exame não pode ser realizado efetivamente nas condições extremamente restritivas impostas pelo TSE.

20 Disponível em http://sintse.tse.jus.br/documentos/2013/Out/14/portaria-no-490-de-8-de-outubro-de-2013-constitui

Se por um lado o TSE autoriza vislumbrar rapidamente o código-fonte do sistema operacional da urna, denominado atualmente UENUX, por outro lado é impossível sua avaliação real dentro da curta janela de tempo permitida pelo Tribunal e nas condições técnicas extremamente limitadas.

Nessa questão cabe analisar a origem do sistema operacional UENUX, sua titularidade e as permissões pertinentes.

O UENUX não é um *software* original desenvolvido pelo TSE ou pelos seus fornecedores, mas sim um programa na sua origem adaptado (derivado) a partir de um núcleo (*kernel*) conhecido pelo nome Linux, desenvolvido e mantido orginalmente pelo programador finlandês Linus Torvalds.

O autor Linus Torvalds coloca seu código-fonte livremente disponível no mundo especializado, mas para isso é necessário que as condições de licenciamento se propaguem obrigatoriamente para as novas derivações[21].

Ponto relevante com relação à Auditoria Especial é que o contrato de licenciamento do sistema operacional em questão impõe ao desenvolvedor a obrigação de permitir a qualquer pessoa copiar o código-fonte, realizar quaisquer estudos, testes e avalições e produzir novas derivações a partir da cópia do código-fonte. Vejamos:

O UENUX utiliza o GNU/Linux[22]:

> *O Projeto GNU tem duas licenças principais a serem usadas para bibliotecas. Um deles é o GNU Lesser GPL; o outro é o GNU GPL. A escolha de uma licença faz uma grande diferença: usando a Lesser GPL permite o uso da biblioteca em programas proprietários; usando a GPL para uma biblioteca torna disponível apenas para programas livres[23].*

A Licença Pública Geral GNU (GPL)[24]:

> *"é uma licença de copyleft livre para softwares e outros tipos de trabalhos (...) A Licença Pública Geral GNU pretende garantir sua liberdade de compartilhar e modificar todas as*

21 Vide GNU, General Public License (GPL) e Free *Software* Foundation (FSF)

22 Disponível em: http://www.tse.gov.br/internet/eleicoes/arquivos/Linux_nas_urnas.pdf

23 Tradução livre: http://www.gnu.org/philosophy/why-not-lgpl.html

24 http://www.gnu.org/licenses/gpl-howto.html

> *versões de um programa – para se certificar que o software continue livre para todos os seus usuários (...)*[25].

Copyleft é:

> *um método legal de tornar um programa em software livre e exigir que todas as versões modificadas e estendidas do programa também sejam software livre*[26].

Auditar esse código é tarefa essencial porque o funcionamento efetivo dos programas aplicativos da Urna Eletrônica pode ser indevidamente e silenciosamente modificados ou influenciados a partir de alterações indevidas no sistema operacional ou em seus *drivers*. Tais procedimentos escusos poderiam, por exemplo, modificar a identificação das teclas digitadas pelo eleitor com o código do candidato, as informações mostradas na tela com sua fotografia ou mesmo os votos gravados em uma memória de resultado.

Cabe notar que a imprensa especializada frequentemente divulga notícias sobre modificações secretas realizadas em outras partes do mundo no núcleo do sistema operacional Linux com finalidades escusas ou não autorizadas. Por isso, é essencial o exame contínuo do código-fonte do sistema operacional e *drivers* utilizados na Urna Eletrônica e suas cópias devem ser posta à disposição dos partidos em conformidade com sua licença.

As normas do TSE não preveem o atendimento das normas relativas à *copyleft*, pois não consta que haja livre acesso e possibilidade de cópia do código-fonte do sistema operacional e seus *drivers* para análise nos laboratórios dos auditores.

Essas normas do TSE permitem apenas rápidas e limitadas vistorias realizadas dentro das instalações do TSE, havendo também restrições quanto às ferramentas e os métodos que podem ser utilizados.

Lesser GPL, por sua vez, permite o desenvolvimento de programas proprietários[27], o que significa que, em determinado grau, sua cópia, reprodução ou redistribuição é limitada pelo autor do programa proprietário.

---

25 Tradução livre – Fonte: http://www.gnu.org/licenses/gpl-3.0.en.html

26 http://www.gnu.org/licenses

27 http://www.gnu.org/philosophy/why-not-lgpl.html

Quando há programa proprietário, é uma faculdade do autor do código deixar o programa em domínio público, deixando-o, por exemplo, sob a licença de *copyleft*.

Pelas regras do GNU, o autor do UENUX não estaria obrigado a disponibilizar o código-fonte de seu programa aos eleitores, sendo obrigada a, no máximo, fornecer o código-fonte e manual de instalação a quem possuir cópia do código-objeto[28]:

> *O GPLv3 exige que eleitores sejam capazes de modificar o software sendo executado em uma urna eletrônica (#v3VotingMachine)?*
> *Não. Empresas distribuidoras de dispositivos que incluam software coberto pela GPLv3 são obrigadas no máximo a prover o código fonte e informações sobre instalação do software para pessoas que possuam uma cópia do código objeto. O eleitor que usa a urna eletrônica (como qualquer outro "kiosque") não ganha a posse sobre o equipamento, nem mesmo temporária, de modo que o eleitor também não recebe a posse do programa binário nele contido.*
> *Perceba, entretanto, que a votação é um caso muito especial. O simples fato do software em um computador ser gratuito não significa que você pode confiar no computador para a eleição. Nós acreditamos que computadores não podem ser considerados confiáveis para fins eleitorais. Votações deveriam ser feitas em papel.*

Assim, embora a utilização do GNU não obrigue seu usuário a disponibilizar o código fonte de programas modificados quando não disponibilizados a terceiros, como é o caso do UENUX, é fato que o autor do código modificado tem a faculdade de promover o *software* livre, disponibilizando seu código, por licença *copyleft*, a fim de contribuir com o Projeto GNU:

> *Fazer do programa um software GNU significa contribuir explicitamente para o Projeto GNU. Isso acontece quando os desenvolvedores do programa e o Projeto GNU concordam em fazê-lo[29].*

28 Fonte Free *Software* Foundation's Licensing and Compliance Lab, disponível em: http://www.gnu.org/licenses/gpl-faq.en.html#v3VotingMachine

29 http://www.gnu.org/licenses/gpl-faq.pt-br.html

> *A GPL não obriga você a distribuir sua versão modificada. Você é livre para fazer as suas modificações e utiliza-las de forma privada, sem nunca disponibilizá-las.*
> *Mas se você disponibilizar a versão modificada para o público de qualquer forma, a GPL requer que você torne o código fonte disponível para os usuários, sob os termos da GPL.*
> *Portanto, a GPL dá permissão para se disponibilizar o programa modificado de algumas formas, mas não de outras formas; mas a decisão disponibilizar ou não o programa depende de você*[30]*.*

Com efeito, esta pareceu ser a ideologia do TSE quando do desenvolvimento e aplicação do UENUX, pois, conforme publicou o próprio TSE em 2007, a ideia do código aberto foi uma das motivações que o levaram a escolher o GNU/LINUX, uma vez que o *software* livre ensejaria a disponibilização do código fonte ao público em geral, permitindo sua auditoria:

> *Segundo a Secretaria, as vantagens da utilização do Linux na urna eletrônica são: padronização, pois é possível utilizar o sistema operacional Linux em todos os modelos de urna; transparência, por se tratar de um sistema operacional aberto,* ***todo código-fonte está disponível ao público em geral e pode ser auditado livremente****; independência, já que o desenvolvimento será realizado pela própria equipe técnica do TSE, não haverá dependência de fabricante ou fornecedor, muito menos haverá pressões mercadológicas para atualização de versão, nem dependência de políticas de licenciamento e suporte, como ocorre hoje.*
> *Outros aspectos positivos são: a confiabilidade; o custo zero, pois não há pagamento de propriedade intelectual e de direitos autorais, pois não requer qualquer licença; e sua adaptação às necessidades da Justiça Eleitoral, uma vez que conterá somente o necessário para o funcionamento da urna. A manutenção ou qualquer alteração poderá ser feita interna-*

30 http://www.gnu.org/licenses/gpl-faq.pt-br.html

> *mente e com muita rapidez, sem a necessidade de intervenção do fabricante ou fornecedor.*
> *Essa substituição, por fim, aumentará a credibilidade das eleições, pois a substituição dos atuais sistemas operacionais utilizados por Linux é um fator facilitador para apresentação do sistema na íntegra, incluindo o núcleo, sem as dificuldades impostas pela propriedade intelectual dos criadores*[31]*.*

A ideia de código aberto foi reforçada em outras publicações. Vejamos notícia publicada pela Agência TSE em 2008:

> *Os novos modelos de urna possuem um scanner para identificação dos eleitores pelas digitais e custa aproximadamente 800 dólares. A partir deste ano, todas as urnas vêm com o sistema operacional Linux, que é de código aberto. Até a última eleição, o TSE utilizava sistemas proprietários, que são pagos. Para a alteração, são apontadas três vantagens: a gratuidade do Linux, a transparência do código aberto, que facilita auditorias, e, por fim, a robustez do sistema, que garante segurança dos dados das eleições*[32]*.*

Também em 2008, o TSE publicou notícia a respeito da votação paralela e sobre a abertura dos códigos dos sistemas eleitorais aos partidos, destacando que, em determinado dia daquele ano, haveria uma sala de apresentação do sistema aos partidos e especialistas previamente credenciados:

> *TSE abre códigos dos sistemas eleitorais aos partidos e descarta possibilidade de invasão (...)Um dos recursos que se-*

31 http://agencia.tse.jus.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=966324

32 Fonte:http://agencia.tse.jus.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1029372&toAction=NOTI_AGENCIA_PAGE_PRINT&print=true

> *rão colocados à disposição dos partidos será o dispositivo de assinatura digital, que servirá para validar os programas que serão desenvolvidos para as eleições, os quais serão todos desenvolvidos na plataforma Linux, de código aberto e softwares livres. A assinatura digital servirá para confirmar a integridade da votação, já que as urnas só vão funcionar se reconhecê-la.*

Em 2009, no II Congresso Internacional sobre *Software* Livre e Governo Eletrônico - CONSEGI, realizado pela Secretaria de Logística e Tecnologia da Informação (SLTI/MPOG), Comitê Técnico de Implementação de *Software* Livre – CISL e pela Escola de Administração Fazendária – ESAF[33], foi ministrada palestra sobre o UENUX, sendo, mais uma vez, frisada a transparência e confiabilidade do programa:

> *O software livre foi adotado nas eleições municipais do ano passado no Brasil. As 430 mil urnas eletrônicas utilizadas foram adaptadas para usar sistema operacional GNU-Linux, desenvolvida pela equipe técnica do TSE (Tribunal Superior Eleitoral).*
> *A mudança no sistema operacional das urnas tornou o processo eleitoral mais transparente e confiável, permitindo auditoria do sistema operacional por qualquer interessado em se certificar de sua segurança, além de diminuir o custo da aquisição de novas urnas eletrônicas, dada a gratuidade do Linux, segundo o TSE[34].*

Assim, é bastante claro que o TSE utilizou como importante motivo à implementação do GNU/Linux no sistema eleitoral o fato de ser *software* livre, com código aberto, auditável por todos, o que não corrobora com sua negativa de fornecimento de dados solicitados pela equipe técnica da Auditoria Especial das Eleições de 2014.

No mesmo sentido, não coaduna com a ideia de transparência, *software* livre e código aberto, a limitação imposta pela Resolução 23.397[35] do TSE, quando determina que, nas cerimônias de análises de códigos – que não poderá ser realizada por qual-

33 http://www2.consegi.gov.br/2009/comites-e-organizacao

34http://www2.consegi.gov.br/2009/assessoria-de-imprensa/clipping-consegi-2009/palestra-uenux-*software*-livre-nas-urnas-eletronicas/

35 http://www.tse.jus.br/eleicoes/eleicoes-2014/normas-e-documentacoes/resolucao-no-23-397-consolidada-com-alteracoes

quer pessoa – somente poderão ser utilizados os programas previamente aprovados pela Secretaria de Tecnologia da Informação do TSE.

Por fim, cabe a reflexão sobre o código-objeto[36], também não fornecido aos Auditores, que, conforme visto alhures, ensejaria o fornecimento do código-fonte, especialmente no caso de urnas eletrônicas, segundo as regras do GNU.

3.9. Governança do TSE Quanto aos Sistemas Aplicativos

Em essência, o sistema eleitoral como um todo é composto por cerca de 27 sistemas aplicativos que cumprem as funções inerentes aos processos de gestão de eleitores, candidatos e unidades eleitorais, votação e totalização. O elevado índice de automatização do processo e a ausência de controles paralelos efetivos faz com que o sistema eleitoral como um todo imponha à nação a necessidade de acreditar na própria governança do TSE como fiador da licitude do processo, o que contradiz todas as normas técnicas sobre segurança de sistemas eletrônicos.

Os aplicativos que compõem o sistema eleitoral são desenvolvidos principalmente pelo TSE, por outros órgãos públicos e por empresas fornecedoras privadas. As fases de especificação e desenvolvimento dos sistemas eleitorais não podem ser acompanhadas por representantes da sociedade, mas há determinadas janelas nas quais partidos, coligações, OAB e o Ministério Público podem realizar algum acompanhamento, basicamente limitado à visualização dos códigos-fonte em Sala de Apresentação do TSE, sendo os procedimentos sujeitos a normas limitadoras[37] que dispõem sobre a cerimônia de assinatura digital e fiscalização do sistema eletrônico de votação, do registro digital do voto, da votação paralela e dos procedimentos de segurança dos dados dos sistemas eleitorais.

Em seguida, os programas são compilados e assinados digitalmente por representantes do TSE, partidos, OAB e Ministério Público. Códigos *hash* são gerados, entregues aos participantes e publicados no site do TSE. Após, os sistemas são gravados em mídia não regravável, lacrados fisicamente, depositados em sala-cofre do TSE e as correspondentes chaves eletrônicas privadas e senhas de acesso guardadas pela Justiça Eleitoral.

36 “(...) criado pela conversão do código-fonte em linguagem de máquina. É gerado pelo compilador. Só é criado quando não há erros no código-fonte”. https://www.inf.pucrs.br/~pinho/LaproI/ConceitosBasicos/ConceitosBasicos.htm

37 Lei nº 9.504/1997, artigo 66, parágrafo 1º, e Resolução do TSE 23.397/2013

Os dados e programas eleitorais assinados e lacrados são enviados por rede privada aos TRE's, os quais conferem códigos *hash* em audiências públicas e via programa GEDAI-UE geram a *flash* de carga sobre candidatos e eleitores, a *flash* de votação e memória de resultado. A *flash* de carga gera número único de correspondência SCUE a partir do número de série da urna, da seção e de outros dados. São inseridas então *flash* de votação e a memória de resultado, sendo que o programa ATUE verifica a urna e seus componentes com acompanhamento dos partidos, OAB e MP. O programa VOTA obtém os votos, grava o resultado em memória e os dados são transmitidos para totalização[38]. Os partidos podem novamente verificar códigos-fonte e executáveis, porém, sempre sob limitações que impedem exames conclusivos.

Conforme descrito neste documento, a Auditoria Especial comprovou que: (i) a área de tecnologia não conseguiu apresentar documentação técnica original e consistente sobre a especificação, desenvolvimento e manutenção dos sistemas aplicativos; (ii) parte da documentação de programas está inserida diretamente no código-fonte. Contudo, sua utilização é irregular e confusa (por exemplo, ora há maior detalhamento de funções, ora não há qualquer detalhamento), de tal maneira que a alegação dos técnicos de que isso resultaria da complexidade ou importância da rotina se mostrou inconsistente, pois foram encontradas rotinas críticas não documentadas e rotinas acessórias e simples fartamente documentadas, demonstrando tratar-se mais de estilos individuais de cada técnico do que uma metodologia consistente e uniforme; (iii) ao longo da vistoria, a Auditoria Especial constatou frequentes dúvidas e confusões das equipes técnicas do Tribunal ao não conseguir localizar e explicar tecnicamente determinados programas ou componentes, notando-se que nesse momento, aparentemente, não procuram apoio em documentação, possivelmente por não existir, não estar atualizada ou ser inadequada aos objetivos; (iv) verificou-se existir comentários e anotações inapropriadas e comentários sobre a existência de erros em rotinas, sem que tivessem sido claramente corrigidas, ocorrência frequente em programas de teste, sendo que os técnicos explicaram que tais trechos de código foram gerados por fornecedores externos e tais comentários seriam removidos, demonstrando-se com isso que os técnicos do TSE falham ao receber produtos adquiridos via licitação pública e permitem a existência de erros ao longo da vida útil dos programas, mesmo que sejam de teste.

Cabe novamente reiterar que a auditoria eficaz dos sistemas aplicativos deveria ser realizada em laboratórios autônomos e independentes, sem restrições quanto aos

38 Vide http://www.tse.jus.br/noticias-tse/2014/Julho/sistemas-da-urna-eletronica-brasileira-sao-totalmente-desenvolvidos-pelo-tse

objetivos, métodos e ferramentas, além de serem realizados sem qualquer supervisão com prazo mínimo de 60 dias. A cada alteração de qualquer componente deve ser assegurada a possibilidade de nova auditoria do componente e do sistema como um todo.

3.10. Governança TSE na Criptografia e Assinatura Digital

A integridade do sistema eleitoral depende essencialmente do sistema de criptografia desenvolvido, mantido e fornecido pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC).

Esse Centro está subordinado ao Departamento de Pesquisa e Desenvolvimento Tecnológico (DPDT), da Secretaria de Planejamento, Orçamento e Administração (SPOA), todos na Agência Brasileira de Inteligência (ABIN). Por sua vez, a ABIN responde ao Gabinete de Segurança Institucional (GSI) da Presidência da República (PR).

Como é mostrado neste documento, o código desenvolvido pelo CEPESC está presente em praticamente todos os pontos centrais do sistema eleitoral, configurando um ponto crítico de falha uma vez que erros ou procedimentos indevidos inseridos nessa rotina são capazes de se propagar ou dominar os demais componentes do sistema.

Nesse mesmo sentido, considera-se violação dos princípios que norteiam a segurança de sistema o fato do projetista e mantenedor do sistema estar funcionalmente subordinado diretamente a uma das partes que participam do próprio pleito eleitoral processado pelo sistema, no caso, a Presidência da República.

Considera-se que os procedimentos formais estabelecidos pela legislação eleitoral sobre pontos de controle do código-fonte são insuficientes e não asseguram a inexistência de erros ou rotinas inadvertidas ou indevidas no processo eleitoral.

A Auditoria Especial considera como crítica e não confiável a função de criptografia empregada no sistema eleitoral: os códigos, procedimentos e chaves não são de fato auditáveis e prevalecem pontos de risco e enfraquecimento na segurança. Mesmo se for considerado que, pelo menos em tese, as rotinas são públicas e apenas as chaves precisam ser mantidas em sigilo, considera-se o sistema não confiável por princípio porque as chaves são geradas pela própria ABIN.

O CEPESC cria algoritmos criptográficos e soluções proprietárias de uso exclusivo do Governo e desenvolveu para o TSE a biblioteca criptográfica com assinatura digital. Parte do seu código-fonte fica à disposição para análise por uma semana antes da la-

criação dos programas da Urna Eletrônica[39], cabendo notar que ele é um elemento comum às diversas fases do processo eleitoral, como ilustra o diagrama a seguir:

Logo, considera-se crítica qualquer falha na gestão desse ambiente, ante a sua relevância para o sistema e operação em diversas fases de execução do processo eleitoral.

3.11. Governança do TSE na Atuação dos Juízes Eleitorais

A Auditoria Especial verificou que a conduta dos Juízes Eleitorais segue estritamente a rotina estabelecida pelo TSE durante as chamadas auditorias de urnas em atendimento a reclamações dos partidos em determinada zona eleitoral. Uma vez que tais normas determinam procedimentos inócuos frente a falhas ou procedimentos indevidos mais sofisticados, a rotina oficial proporciona meios para torná-las indetectáveis. Afinal, falhas ou fraudes serão indetectáveis nos procedimentos de auditoria se houver comprometimento dos programas empregados na própria auditoria.

Cumpre notar que os Juízes abdicam de adotar nos seus processos em Varas Eleitorais os mesmos critérios que usualmente utilizam nas suas Varas de origem nas esferas Cível ou Criminal, onde determinam e dirigem perícias técnicas imparciais e realizadas com a profundidade necessária para apurar a verdade dos fatos. Na Justiça Eleitoral, eles deixam de realizar exames periciais e se submetem a determinar única

39 Memorando CSELE/STI 152, de 20/11/2013, em atendimento ao Ofício 58/2013 CPIDAESP. Disponível em www.senado.gov.br.

e exclusivamente os procedimentos estabelecidos pelo TSE, insuficientes e ineficazes para a real verificação dos fatos técnicos e para o efetivo convencimento judicial, podendo levar o decisor a erro.

3.12. Governança do TSE nos Testes Públicos das Urnas

O TSE instituiu em 2010 a prática de realizar testes públicos como parte dos procedimentos para avaliar a segurança da urna eletrônica e apoiar a melhoria continua do projeto.

Tais testes não cumprem o objetivo pretendido pelo TSE sobre comprovar a segurança da Urna porque são fortemente limitados por normas e decisões do próprio Tribunal que levam à não exposição efetiva dos equipamentos e sistemas à avaliação de técnicos independentes. Assim, os testes públicos são inservíveis ao propósito de comprovar a segurança do sistema porque os testadores não estão livres para escolher métodos e ferramentas segundo o método investigativo, exploratório e típico da cultura *hacker,* que em todo o mundo identifica e demonstra graves falhas de segurança.

Além disso, é impossível para qualquer técnico avaliar mais de uma dezena de milhões de linhas de complexa programação durante as poucas horas concedidas pelo TSE, condição que mais uma vez demonstra a falha de governança do TSE no que se refere à segurança do sistema eleitoral, frustrando sua obrigação para com o eleitor, quem é, de fato, o proprietário do sistema eleitoral.

Por outro lado, os testes públicos realizados conforme formato adotado inicialmente pelo TSE são úteis na busca de falhas. Nesse sentido, foram significativos os resultados obtidos por avaliadores independentes no teste público realizado em 2012.

Esta Auditoria Especial considera uma falha grave de governança do TSE, contrária às diretrizes sobre transparência do Poder Judiciário e da Administração Pública já mencionadas, a supressão do teste público previsto para 2014, logo após o último teste público, realizado em 2012, ter descoberto e demonstrado grave falha de segurança que permitia a quebra do sigilo dos votos de qualquer urna, feito realizado por equipe coordenada pelo Prof. Diego Aranha, com equipe independente de investigadores da Universidade de Brasília.

Não restou transparente ao eleitor, como deveria, a real motivação do TSE e quais práticas de governança adotou diante da sua própria infraestrutura tecnológica

quando suprimiu ou postergou os testes públicos razoavelmente independentes logo após a descoberta da grave falha de desenvolvimento no programa aplicativo da Urna.

Ocorre que na sequência o TSE editou a Portaria nº 215, de 10 de abril de 2015[40], que institui um Grupo e Trabalho sobre a segurança do sistema automatizado de votação brasileira, um formato ainda mais restrito para se avaliar a segurança do sistema, concentrado em funcionários internos do próprio TSE, incluindo representantes dos grupos de trabalho sobre inovação tecnológica das urnas eletrônicas[41], representantes do grupo responsável pelo ecossistema da urna eletrônica[42] e de representantes de TRE's.

O Grupo de Trabalho de Segurança da Urna será conduzido pelo Coordenador de Sistemas Eleitorais e terá participação externa limitada a um ou dois participantes que não podem ser considerados independentes em função dos critérios para admissão dos interessados. Por exemplo, não consta que tenha sido incluído no grupo o pesquisador que descobriu nos testes de 2012 a já mencionada grave falha no sistema da Urna - mais um indicador que sugere estar a governança TSE voltada para a causa corporativa interna ligada à área tecnológica com possível detrimento na transparência e prestação de contas ao Poder Judiciário como um todo, à Administração Pública, ao eleitor e à sociedade, especialmente se for confirmada a substituição dos testes públicos pelas ações do grupo de trabalho recentemente criado.

Consta que esse grupo terá como objetivos:

> *I – mapear os requisitos de segurança das diversas fases do processo eleitoral; II – atuar como interlocutor nos tribunais regionais nas demandas decorrentes de denúncias de fraudes no sistema eletrônico de votação; III – elaborar um plano nacional de segurança do voto informatizado, para ser amplamente divulgado junto das Secretarias de Tecnologia da Informação (STIs) dos tribunais regionais (TREs); IV – propor um modelo ágil de auditoria da votação e totalização dos votos, tal como auditoria interna, que possa ser aplicada pelos tribunais regionais durante e após as eleições; V – elaborar material institucional que divulgue à sociedade os meca-*

40 Portaria TSE nº 125 disponível em http://sintse.tse.jus.br/documentos/2014/Abr/11/portaria-no-215-de-10-de-abril-de-2014-ica

41 Portaria TSE nº 123, de 12 de março de 2015

42 Portaria TSE nº 33, de 27 de janeiro de 2015

nismos de segurança do processo eleitoral; VI – estudar, propor e validar modelos de execução de testes de segurança.

Como se pode verificar, os objetivos do grupo de trabalho sobre segurança da urna eletrônica indicam mais uma vez a existência de severas falhas de governança no TSE naquilo que se refere à sua própria área de tecnologia da informação e ao sistema eleitoral como um todo.

Se por um lado estão corretos os objetivos estipulados pelo TSE sobre: (*i) mapear os requisitos de segurança do processo eleitoral*; (*ii) atuar como interlocutor nos TRE's nas demandas decorrentes de denúncias de fraudes no sistema eletrônico de votação*; e *(iii) elaborar um plano nacional de segurança do voto informatizado";* por outro lado, configura erro de governança que tais responsabilidades sejam atribuídas a um "grupo de trabalho". Bem ao contrário disso, tais atribuições deveriam ser tarefa essencial e rotineira da sua infraestrutura fixa do TSE, isso é, das responsabilidades e objetivos permanentes e prioritários da Secretaria de Tecnologia da Informação e dos órgãos que lhe são subordinados (Coordenadoria de Sistemas Eleitorais, Coordenadoria de Soluções Corporativas, Coordenadoria de Logística e Coordenadoria de Infraestrutura).

Sob a óptica das melhores práticas de governança, não parecer coerente que tais atribuições, por serem contínuas e essenciais para quem produz e mantém um sistema eletrônico eleitoral, passem a ser de responsabilidade de um "grupo de trabalho" *ad hoc;* ao contrário, elas devem ser atribuídas a órgãos permanentes, atuais ou novos, internos ou externos ao TSE.

Ademais, o objetivo do TSE de *(ii) atuar como interlocutor nos TRE's nas demandas decorrentes de denúncias de fraudes no sistema eletrônico de votação* não pode ser considerado afeito a um "*grupo de trabalho*", pois fraudes no sistema eletrônico constituem crimes a serem averiguados por Controles Internos e Auditoria do Tribunal, pelo Ministério Público Eleitoral e pela Autoridade Policial, não parecendo ser razoável que um grupo de trabalho constituído por funcionários que, em tese, poderiam ser alvo da própria investigação por fraude eleitoral sejam o "*interlocutor nos TRE's nas demandas decorrentes de denúncias de fraudes*".

Cabe notar ainda que funcionários do Tribunal se revestem de fé pública (exceto quando suas próprias atividades são alvo de averiguação) e que informações sigilosas sobre possíveis terceiros investigados não podem ser entregues a pessoas estranhas ao Tribunal, que eventualmente participem do grupo de trabalho.

Outras falhas de governança estão relacionadas aos objetivos: *(iv) propor um modelo ágil de auditoria da votação e totalização dos votos, tal como auditoria interna, que possa ser aplicada pelos tribunais regionais durante e após as eleições*; e *(vi) estudar, propor e validar modelos de execução de testes de segurança*. Primeiramente, não se pode deixar de notar a expressão "*tal como auditoria interna*", confirmando o entendimento desta Auditoria Especial sobre não ter encontrado indicadores de atuação efetiva da área de Controles Internos e Auditoria nas questões que envolvem tecnologia. Além disso, não se mostra razoável que um grupo de trabalho heterogêneo e subordinado a uma coordenação de tecnologia atue "*tal como auditoria interna*".

Ainda com relação a esse objetivo, a Auditoria Especial estranha a expressão "*propor um modelo ágil de auditoria da votação e totalização dos votos*", uma vez que as denúncias ora em apuração e os diversos relatórios de auditoria externa fazem referência exatamente à falta de respostas reais, profundas e convincentes aos questionamentos que envolvem a auditoria da infraestrutura do Tribunal, dos seus fornecedores e dos sistemas de votação e de totalização de votos.

Grande parte das críticas se refere ao fato dos Juízes Eleitorais abdicarem das práticas que utilizam costumeiramente nas suas Varas Cíveis ou Criminais de origem para a apuração de fatos e produção de provas técnicas, pois, em seu lugar, se limitam a seguir as instruções para auditoria de urnas impostas como normas pelo TSE, sendo notório que tais auditorias são superficiais e totalmente insuficientes para verificar a segurança do sistema eleitoral e para apurar fraudes de alta tecnologia.

Uma vez que as normas do TSE permitem apenas verificações limitadas e a utilização de programas produzidos ou aprovados pelo mesmo grupo que desenvolve os próprios sistemas de votação, não é possível considerar esses procedimentos como sendo pertinentes a verdadeiras auditorias. Para que assim fosse, seria necessário pelo menos a execução de programas independentes e que buscassem dados diretamente nos dispositivos de armazenamento, sem qualquer filtro ou seleção programada internamente pelo TSE. Portanto, o modelo adotado há anos pelos TRE's já é um "*um modelo ágil de auditoria da votação e totalização dos votos*" e por isso é imprestável para assegurar a identificação e apuração de fraudes, especialmente aquelas mais sofisticadas tecnologicamente ou cuja origem eventualmente seja interna ao próprio TSE ou em seus fornecedores.

Como demonstra a presente Auditoria Especial, para cumprir suas responsabilidades para com a transparência e segurança do sistema eletrônico eleitoral o TSE precisa determinar, não modelos mais "*ágeis de auditoria*", mas sim modelos de auditoria

mais profundos, independentes e transparentes, isto é, modelos mais próximos da perícia técnica forense largamente utilizada em outras instâncias do Poder Judiciário.

Com relação ao objetivo *(vi) estudar, propor e validar modelos de execução de testes de segurança*, inexorável observar que, de forma similar aos objetivos anteriores, como modelos de fato não garantem a segurança de qualquer sistema, eles não podem ser utilizados para limitar a atuação de auditores, investigadores ou Juízes, como já ocorre atualmente.

Finalmente, cabe reiterar diversos aspectos de governança que podem comprometer a segurança do sistema eleitoral:

(i) o sistema de criptografia e assinatura digital é desenvolvido por órgão subordinado a uma das partes na eleição, tem falhas de implementação e seu uso em vez de trazer mais segurança de fato impede verificações e auditorias transparentes sobre fraudes;
(ii) a metodologia de verificação do código-fonte adotada pelo STI não assegura ausência de erros ou fraudes;
(iii) o TSE impede verificações verdadeiramente profundas e independentes sobre o sistema eleitoral;
(iv) não se vislumbra auditoria interna eficaz nas questões que envolvem tecnologias complexas como aquelas do sistema eleitoral;
(v) o próprio Tribunal reconhece muitas falhas de governança, especialmente no que se refere às suas áreas de tecnologia;
(vi) a votação paralela não pode ser considerada garantidora de integridade e fidelidade da votação porque os programas desenvolvidos internamente no Tribunal valem-se dos sensores da urna para monitorar seu ecossistema e assim podem perfeitamente detectar a condição de votação paralela e com isso ofuscar quaisquer rotinas fraudulentas;
(vii) a falta de independência real entre as diversas áreas envolvidas (geradora de normas, desenvolvedora do sistema, testadora do sistema, homologadora do sistema, colocação do sistema em produção e operação do sistema); e
(viii) a falta de transparência quanto aos processos e procedimentos técnicos internos.

Dessa maneira, em termos de governança voltada ao eleitor, cabe propor aprofundamento e maior transparência do modelo por meio de auditorias independentes e

não o desperdício de recursos públicos em ações de mera divulgação sobre uma segurança não comprovada, o que pode levar o eleitor a engano.

4. AVALIAÇÃO SOBRE SISTEMAS E PROCEDIMENTOS

Este capítulo foi desenvolvido pelos auditores Amílcar Brunazo Filho, Clovis Torres Fernandes, Márcio Coelho Teixeira, Marco Antônio Carvalho, Marcos Antonio Simplicio Junior para a Coordenação Geral da Comissão da Auditoria Especial do PSDB e contém o parecer dos auditores após os trabalhos de coleta de dados no TSE e nos TRE's e de análise desses dados e do *software* eleitoral desenvolvido no TSE e usado no 2º turno da eleição presidencial de 2014.

O pedido inicial de Auditoria do processo eleitoral de 2014[43] foi apresentado pelo PSDB ao TSE na data de 30 de outubro de 2014. A petição inicial continha a justificativa do pedido e uma lista inicial dos documentos gerados no processo eleitoral, aos quais se pretendia ter acesso para Auditoria.

43 Protocolo TSE n. 32.860/2014, dentro do processo de APURAÇÃO DE ELEIÇÃO No 1578-04.2014.6.00.000 – CLASSE 7 – DISTRITO FEDERAL (Brasília)

O pedido foi submetido à Procuradoria Geral Eleitoral, que se manifestou pelo indeferimento, e também foi submetido à Secretaria de Tecnologia de Informação (STI) do TSE, que emitiu parecer no sentido de atender o pedido dentro de limitações e restrições contidas nas Resoluções TSE 23.397/2013 e 23.399/2013.

No dia 04 de novembro de 2014[44], o plenário do TSE aprovou o pedido do PSDB com as limitações inscritas na Resolução 23.397/13, como sugerido pela STI.

Outros desdobramentos de natureza burocrática adiaram o início efetivo dos trabalhos da Auditoria para o final do mês de janeiro de 2015. Durante seu desenvolvimento, a Auditoria encontrou restrições impostas pela autoridade eleitoral, que comprometeram o alcance e a profundidade dos trabalhos.

O resumo das conclusões desse relatório é o seguinte:

a) O Sistema Eleitoral Informatizado Brasileiro não foi projetado, desenvolvido e implantado para permitir uma auditoria independente efetiva do resultado que produz;
b) O sistema adotado e o processo desenvolvido pela autoridade eleitoral, com suas severas restrições, não permitiram a conferência e a determinação do nível de confiabilidade da etapa de votação e apuração dos votos que ocorrem nas urnas eletrônicas;
c) Na etapa de transmissão e de totalização dos votos, não foram encontrados problemas graves que indicassem comprometimento da sua confiabilidade.

Neste relatório se descreve, na seção 4.1, a coleção das dúvidas que levaram o partido à iniciativa de solicitar a auditoria e que compõem os objetivos a serem esclarecidos. Em seguida, na seção 4.2, é apresentado o plano de trabalho idealizado para o início e andamento da auditoria. Na seção 4.3 são descritas as condições restritivas que os auditores enfrentaram no desenvolvimento de seus trabalhos. Segue-se, na seção 4.4, a análise conjunta de todas as informações coletadas. Ao final, nas seções 5 e 7, se apresentam as conclusões e as recomendações dos auditores.

4.1. Dúvidas Iniciais e Objetivos da Auditoria

Nos dias seguintes ao 2º turno da eleição presidencial de 2014, chegaram à coordenação da campanha do PSDB um conjunto de várias questões (denúncias e des-

44 Julgamento AE Nº 1578-04.2014.6.00.0000

confianças) que haviam sido enviadas por milhares de eleitores, as quais envolviam desde descrição de vulnerabilidades e hipóteses de fraudes até denúncias documentadas sobre ocorrências indevidas.

As denúncias de caráter geral com alguma consistência ou evidência aparente (antes de uma auditoria específica), eram:

4.1.1. Desvio de Votos nas Urnas Eletrônicas

Vulnerabilidades nos procedimentos e nas urnas eletrônicas permitiriam a inserção de software malicioso para desviar votos durante seu registro ou apuração.

Denúncia baseada no fato das urnas eletrônicas brasileiras serem de modelo "*dependente do software*" e de que há vários momentos em que elementos terceirizados têm acesso à produção, transporte e instalação do *software* nas urnas.

Esta denúncia é agravada pelo fato do administrador eleitoral não permitir qualquer forma de verificação da integridade do *software* carregado nas urnas que seja feita de modo independente do próprio *software* sob avaliação. Ela também é agravada por testes de penetração bem sucedidos[45, 46], no exterior, em modelos de urnas do mesmo fabricante das urnas brasileiras.

4.1.2. Desvio de Votos na Transmissão e na Totalização dos Votos

Possibilidade de trocas dos resultados transmitidos para as centrais de totalização ou a troca dos resultados dentro dessas centrais.

Baseada no fato que os TRE's contrataram empresas para, entre outras tarefas, participar da coleta e transmissão os resultados das urnas para os computadores de totalização.

A percepção pública de fraude nesse momento também foi agravada pela divulgação do resultado da totalização para o cargo de presidente já quase completa e so-

45 Testes da Black Box Voting, em: http://www.blackboxvoting.org/BBVtsxstudy.pdf

46 Testes da Universidade de Princeton, em: http://www.youtube.com/watch?v=0AKR-Lo-700

mente às 20h, depois do final da votação no Acre, e por ter se tornado público que um grupo pequeno de pessoas sob coordenação da STI/TSE, para consulta, teve acesso aos dados parciais da totalização, com oportunidade de eventual modificação.

4.1.3. Outras Denúncias

As denúncias mais específicas (antes da avaliação de sua procedência) abordavam o seguinte:

Geração de Mídias *- computadores que geravam as mídias de carga das urnas tinham conexão ativa com a Internet;*
Smartmatic[47] *– a empresa, estrangeira, teria fraudado a contagem dos votos – muitas denúncias com documentação diversa, mas inespecífica;*
Eleitor "já votou" *– eleitor não pôde votar porque alguém já tinha votado em seu nome – muitas denúncias, algumas documentadas, inclusive em seções com urnas biométricas;*
Eleitor fantasma *– eleitor que viajou ao exterior constatou que alguém votou em seu lugar, tendo apresentado documentação da viagem e do certificado de votação dado pelo TSE;*
Fraude do Mesário *– mesários inseriam votos nas urnas no final do dia – muitas denúncias, pouco documentadas;*
Urna fantasma *- urna votava "sozinha" - com vídeo ilustrando;*
Documentos oficiais descartados *- documentos da seção eleitoral jogados no lixo – com vídeo ilustrando;*
Fraude na zerésima *- uma zerésima constava com 400 votos para a candidata Dilma Roussef;*
Teclado adulterado *- urna registrava 44 quando se tentava digitar 45 – com vídeo ilustrando;*
Dispositivo suspeito *- inseriram pen-drive na urna antes do início da votação – sem documentação.*

Diante dessas denúncias e do quadro de incertezas sobre o resultado eleitoral, os auditores tomaram como objetivo verificar a procedência de tais denúncias com a pro-

47 A empresa Smartmatic teria sido contratada pelo TSE e, posteriormente, por 11 TRE's para, entre outras tarefas, carregar o *software* nas urnas e transmitir os resultados.

fundidade necessária em cada caso, inclusive procurando fazer recontagens e conferências da apuração e da totalização onde possível.

4.2. Plano de Trabalho

Além do objetivo de verificar as denúncias e conferir a apuração e a totalização dos votos, a elaboração de um plano de trabalho dos auditores teve que levar em conta o modelo tecnológico do sistema eleitoral eletrônico brasileiro sob avaliação.

As características técnicas do sistema de voto eletrônico brasileiro, de interesse para auditoria, são descritas a seguir.

4.2.1. Descrição do Sistema Eleitoral Eletrônico

O sistema eleitoral eletrônico adotado pelo TSE baseia-se no uso de urnas eletrônicas de modelo conhecido na literatura acadêmica internacional como DRE sem VVPAT, descrito da seguinte maneira:

- **DRE** - *Direct Recording Electronic voting machine* - equipamento com gravação eletrônica direta do voto, depois de confirmado na tela pelo eleitor, em um arquivo chamado de *Registro Digital do Voto* (RDV).
- **sem VVPAT** – *Voter Veriable Paper Audit Trail*[48] – não se produz uma trilha material (em papel) para auditoria que permita comparar o voto como visto pelo eleitor com o voto que foi registrado no RDV. Essa trilha material para auditoria do processamento do voto também é chamada de *Independent Voter-Verifiable Record* (IVVR)[49] ou ainda, em português, como *Voto Impresso Conferível pelo Eleitor* (VICE).

A ausência do VVPAT cria um ponto cego de auditoria na apuração dos votos, pois nem os fiscais de partido ou auditores independentes, nem o próprio eleitor, têm como conferir se o voto visto na tela da urna foi gravado corretamente no RDV.

48 **Mercuri R.** - "*Electronic Vote Tabulation, Checks & Balances*". USA: University of Pennsylvania, 27/10/2000 - http://www.notables*oftware*.com/Papers/thesdefabs.html

49 **NIST, US-EAC** – "*Voluntary Voting System Guidelines*". USA: U.S. Election Assistance Commission, maio/2009 - IV Systems ou IVVR é especificado na Seção 7.8 do Volume 1 - http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf

Por este motivo, na literatura acadêmica internacional, se diz que este modelo DRE sem VVPAT é *"dependente do software"*[50] ou que não atende ao *Princípio de Independência do Software em Sistemas Eleitorais*[51], pois um erro não detectado no *software* (da urna) pode causar erros no resultado que não serão detectados por uma auditoria contábil da apuração.

O sistema desenvolvido pelo TSE, contudo, produz documentação digital e em papel que possibilitam uma auditoria contábil da transmissão e da totalização dos votos.

Os documentos de auditoria gerados no andamento do processo eleitoral são:

a) **Arquivos de LOG do Sistema Gerador de Mídias** – contendo as informações de data, hora, identificação e abrangência dos cartões de memória "*Flash de Carga*" gerados para a carga das urnas;
b) **Arquivos de Eleitores Aptos** de cada seção/urna;
c) **Tabela de Correspondências Esperadas** - com a relação dos números das urnas e das respectivas seções eleitorais para a qual foram preparadas e contêm, ainda, a hora em que foi feita a carga da urna e outras informações;
d) **Arquivos de LOG das Urnas** – com registros de data e hora dos eventos principais ocorridos durante o funcionamento de uma urna. Permite, entre outras análises, contar o total de votos computados no dia da eleição, confirmar a quantidade de justificativas apresentadas, avaliar o desempenho do sistema de identificação biométrica e tabular o tempo de votação de cada voto confirmado;
e) **Zerésima** – lista impressa com os nomes dos candidatos ladeados pelo número Zero que, supostamente, indicaria ausência de votos;
f) **RDV** - *Registro Digital do Voto* – com os votos supostamente confirmados pelo eleitor, gravados em posições aleatórias para impedir a reconstituição da lista dos votos ordenados no tempo;
g) **Justificativas** – com os nomes e seções eleitorais de eleitores que se apresentaram para justificar sua ausência da seção eleitoral de origem. Permite, junto com os arquivos de eleitores aptos, determinar a quantidade de casos de eleitores que teriam votado em uma cidade e apresentado justificativa em outra;

50 **Rivest R.R. , Wack, J.P. -** "On the notion of "*software* independence in voting systems". USA: NIST, 28/07/2006 - *http://people.csail.mit.edu/rivest/pubs/RW06.pdf*

51 O Princípio da Independência do *Software* em Sistemas Eleitorais estabelece o seguinte: "*Um sistema eleitoral é independente do software se uma modificação ou erro não-detectado no seu software não pode causar uma modificação ou erro indetectável no resultado da apuração ou na inviolabilidade do voto*"
http://pt.wikipedia.org/wiki/Independ%C3%AAncia_do_*Software*_em_Sistemas_Eleitorais

h) **Faltosos** – com os nomes dos eleitores que não compareceram para votar. Permite conferir, junto com o arquivo de eleitores aptos, o total de votos colhidos;
i) **BU digitais** – os Boletins de Urna são calculados ao final da votação, pela soma dos votos gravados no RDV. São gerados em duas formas digitais: a binária para processamento da totalização e o Espelho de BU (em texto aberto legível);
j) **BU impresso** - trilha material (em papel) de auditoria, para entrega aos fiscais dos partidos, que permite a auditoria contábil da transmissão e da totalização;
k) **LOG do sistema de totalização** – para se reconstruir e auditar a sequência de totalização;
l) **Tabela de Correspondências Efetivadas** - com a relação dos números das urnas e das respectivas seções eleitorais de onde vieram os resultados para totalização.

4.2.2. Definição do Plano de Trabalho Inicial (PTI)

Essas características do sistema eleitoral eletrônico brasileiro (DRE, dependente do *software*) condicionaram a elaboração do plano de trabalho de auditoria, já que não há eficácia em uma eventual "*recontagem dos votos*" feita pela impressão dos *Registros Digitais dos Votos* (RDV), método este sugerido pelo Ministro Henrique Neves em seu voto na inicial desse processo.

Devido ao ponto cego de auditoria da apuração, acima descrito, ao final de tal "*recontagem dos RDV impressos*" os auditores continuariam sem ter determinado se o resultado da apuração em cada urna estava correto ou se teria sido distorcido anteriormente à gravação de cada RDV pelo próprio *software* da urna.

Por ser um sistema eminentemente dependente do *software*, a auditoria da primeira etapa do processo eleitoral, a apuração (contagem dos votos de cada seção eleitoral) tem que ser feita indiretamente, por meio de um processo de validação e certificação do *software* usado nas mais de 420 mil urnas utilizadas no dia da eleição.

A validação do *software*, neste caso, consiste numa auditoria completa do código-fonte do *software* das urnas e de todas as etapas do processo de compilação desse código-fonte e, ainda, na realização de testes exaustivos do funcionamento do *software* sob situações diversas de risco.

A certificação do *software* consiste numa auditoria por amostragem nos códigos executáveis (binários) do *software* embarcado nas urnas.

Por outro lado, a existência de BU impresso que poderia ser coletado pelos Partidos no dia da eleição, permite uma auditoria contábil direta da segunda etapa do processo eleitoral, que é a transmissão e a totalização dos resultados.

Essa auditoria da totalização tem, no entanto, de ser feita por amostragem, confrontando os BU impressos com os respectivos valores digitais recebidos pelo sistema totalizador do TSE, pois não seria possível, por limitações econômicas e práticas, coletar a totalidade dos BU impressos.

A partir dos objetivos e da análise das características do sistema se estabeleceu o seguinte plano de trabalho inicial (PTI):

4.2.2.1. Coleta Inicial de Dados

Solicitação de cópias de todos os 12 tipos de dados acima listados para análise, cruzamento de informações e verificação da coerência interna entre eles.

4.2.2.2. Auditoria da Apuração nas Urnas

Em um sistema dependente do *software*:

a) verificar as consistência entre a quantidade de votos gravados nos diversos arquivos de controle de cada urna (RDV, BU, LOG, Eleitores Aptos-Faltosos);
b) avaliar toda a implementação do sistema (*hardware* e *software*), para verificar se os requisitos de segurança do projeto, as salvaguardas anunciadas e as normas técnicas adotadas foram atendidas;
c) avaliar o sistema de certificação digital usado na assinatura digital dos sistemas eleitorais, quanto a sua conformidade com o padrão ICP-Brasil;
d) avaliar a documentação descritiva do desenvolvimento do *software* das urnas para determinar o seu grau de maturidade e de adequação às técnicas e boas práticas de engenharia de *software*;
e) analisar o código-fonte completo de todo o *software* carregado nas urnas eletrônicas[52], obtendo o *software* fonte no DVD lacrado no dia 04 de setembro de 2014

52 No entender dos auditores, na expressão "*todo o software embarcado*" se inclui, ao menos: o *Firmware* gravado em circuitos internos, o BIOS (*Basic Input e Output System*), o *Loader* gravado nas mídias de inicialização, o Sistema Operacional e todos Aplicativos com suas respectivas bibliotecas internas e externas.

no TSE, para avaliar sua completude e a eventual existência de vulnerabilidades que pudessem ser exploradas em ataques internos e externos[53];

f) analisar os programas compiladores utilizados quanto a sua autenticidade e integridade;
g) recompilar o *software* para fazer uma auditoria da compilação, comparando com os códigos executáveis gravados no mesmo DVD;
h) ter acesso a uma amostra de urnas realmente usadas na eleição para comparação dos códigos executáveis encontrados com os esperados e também para efetuar testes emulando uma votação real, para verificar seu correto funcionamento;
i) avaliar o resultado e a eficácia das auditorias internas posteriores às eleições de 2014, desenvolvidas sobre os equipamentos usados;
j) avaliar o sistema de lacres usados nas urnas eletrônicas como meio para revelar uma tentativa de adulteração do *software*;
k) avaliar os *Testes de Votação Paralela*, realizados nos TRE's, quanto a sua efetividade para verificar a integridade do *software* das urnas quando em uso sob condições normais de votação;
l) fazer um teste de penetração em urnas reais, carregadas com *software* oficial, para determinar se eventuais vulnerabilidades encontradas são viáveis para ataque.

4.2.2.3. Auditoria da Transmissão e da Totalização

a) comparar os dados gerais da eleição (2º turno, 2014 – presidente), como abstenção, votos válidos, brancos e nulos, com eleições anteriores similares em busca de discrepâncias;
b) verificar a consistência e coerência entre os resultados da apuração de cada seção/urna e o resultado final publicado;
c) obter o maior número possível de BU impressos recolhidos por fiscais no dia da eleição, inclusive pelo projeto *Você Fiscal*[54], e obter cópias dos BU extraídos de uma amostra de urnas usadas na eleição, para comparar com resultados oficiais por seção eleitoral;
d) analisar os arquivos de eventos (logs) dos sistemas de transmissão de resultados para procurar sinais de acessos impróprios e para refazer e conferir o gráfico da totalização no tempo, publicado pelo TSE.

53 Por falta de tempo e de recursos, optou-se por não se efetuar testes exaustivos com o *software* sob validação.

54 Projeto Você Fiscal – http://www.vocefiscal.org/

4.2.2.4. Demais denúncias específicas e localizadas

a) procurar evidências das demais denúncias nos TRE's, nos Cartórios e também na análise dos procedimentos de segurança do sistema.

4.2.2.5. Evolução

Este plano inicial poderia ser modificado ou complementado conforme o desenvolvimento das atividades previstas indicasse a eventual necessidade.

Ainda, diante da forte concentração das funções de desenvolvimento, implantação, operação e controle do sistema eleitoral eletrônico pela STI e também pela percepção de seu forte poder de influência na tramitação do processo de auditoria, decidiu-se, para segurança da eficácia da auditoria, que o PTI não deveria ser aberto por completo desde o início, sendo apresentadas apenas as partes necessárias a cada etapa do processo.

4.3. Restrições Encontradas aos Trabalhos de Auditoria

Desde o início, os auditores enfrentaram obstáculos de natureza administrativa que dificultaram seus trabalhos a ponto de comprometer o resultado obtido pela auditoria.

Muitas atividades do plano de trabalho inicial não puderam ser desenvolvidas regularmente por interferências externas e impedimentos impostos pelos administradores do processo sob auditoria que, direta ou indiretamente, estavam tendo auditados os seus próprios desempenhos durante a eleição.

Descreve-se a seguir uma coleção de impedimentos e dificuldades que acabaram por restringir o alcance e a profundidade da auditoria.

4.3.1. As Resoluções do TSE

As primeiras limitações aos trabalhos da auditoria especial surgiram com a decisão da Corte do TSE de acatar sugestão da STI e submeter todos os procedimentos da auditoria aos termos das Resoluções TSE 23.397 e 23.399, ambas de 2013.

Tais resoluções regulamentam o artigo 66 da Lei 9.504/1997[55] e tratam dos procedimentos de segurança praticados sobre o equipamento eleitoral. Foram aprovadas em dezembro de 2013, sob relatoria do Ministro Dias Toffoli, a partir de minutas apresentadas pela própria STI.

Cabe anotar que, durante os procedimentos de aprovação do texto final das Resoluções, os partidos podem apresentar sugestões, mas essas sugestões também são submetidas ao crivo da STI, para que opine sobre o que aceitar ou não.

Sem exceção, as recomendações da STI foram acatadas e nenhuma sugestão de Partidos foi aceita sem ter a aprovação prévia da STI[56].

---

55 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. § 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.
§ 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.
§ 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.
§ 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.
§ 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.
§ 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.
§ 7 º 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.

56 Um dos autores do presente relatório tem regularmente apresentado sugestões às resoluções do TSE. Teve, por exemplo, acatada a obrigação de se entregar aos partidos copias idênticas dos arquivos das urnas, sem qualquer tratamento prévio pela STI.Entre as sugestões rejeitadas pela STI/TSE, constam os pedidos de uma forma de auditoria real que permitisse aos partidos conferir diretamente se os arquivos executáveis carregados nas urnas eram os mesmos lacrados em cerimônia no TSE.
Tal pedido vem sendo apresentado regularmente desde o ano de 2004, depois que constou como recomendação na seção 5.5 do *Relatório da Unicamp* contratado pelo TSE em 2002 e que está disponível em: http://www.tse.jus.br/arquivos/relatorio-final-de-avaliacao-do-sistema-informatizado-das-eleicoes
Mas as propostas de adoção de uma forma de auditoria confiável para os Partidos verificarem a integridade do *software* carregado nas urnas por meio independente do próprio *software* têm sido, desde então, sistematicamente rejeitada pela Corte Eleitoral, sempre acatando recomendação da STI contrária a tal tipo de transparência.

De qualquer forma, tanto o artigo 66 da Lei 9.504/1997 quanto essas duas Resoluções do TSE abordam basicamente procedimentos de avaliação que ocorrem antes e durante a eleição, como a apresentação prévia dos códigos-fonte aos partidos, a compilação em cerimônia aberta, a assinatura digital, lacração e carga dos códigos compilados nas urnas, a entrega dos BU impressos e o Teste de Votação Paralela.

As únicas atividades de auditoria previstas e permitidas nos dias posteriores à eleição são o recebimento de cópias de parte dos arquivos de auditoria das urnas (LOG, RDV, BU e Tabelas de Correspondências Efetivadas) e a possibilidade de se solicitar a execução do programa VPP (Verificador Pré e Pós-eleição) que já fora previamente carregado na urna antes da eleição.

Essas resoluções não preveem, entretanto, qualquer atividade condizente com as técnicas comuns de uma auditoria forense sobre o desempenho das urnas eletrônicas como, por exemplo, recontagem dos votos realmente vistos pelo eleitor, verificação direta e sem restrições do conteúdo da memória dos equipamentos, testes de carga e de funcionamento em condições controladas, testes de penetração, análise dinâmica do *software* e recompilação dos códigos-fonte, etc.

Em resumo, tais resoluções não foram escritas com o objetivo de regulamentar uma auditoria forense, posterior, sobre o desempenho real de um equipamento eletrônico usado em uma eleição.

Porém, a Corte do TSE acatou a sugestão da STI de adotar a Resolução 23.397/2013 como regulamentadora dos procedimentos da Auditoria como se vê, a título de exemplo, neste trecho do voto do Ministro Relator:

> *c) a disponibilização de cópias dos arquivos eletrônicos que compõem a memória de resultados será feita nos termos do art. 42 da Res.-TSE nº 23.397/2013, devendo o requerente especificar os municípios, as zonas eleitorais ou seções do seu interesse, fornecendo as mídias necessárias para gravação; ...*
> *f2) o acesso aos programas de totalização de votos utilizados pelos tribunais regionais eleitorais e por este Tribunal Superior Eleitoral deverá ser feito de acordo com o procedimento previsto na Res.-TSE nº 23.397/2013, **conforme assinalado no parecer técnico**; e*
> *f3) o acesso aos programas e aos arquivos presentes nas urnas eletrônicas, a serem obtidos diretamente das urnas utili-*

> *zadas nas eleições de 2014, será feito mediante escolha aleatória em todos os Estados e em pelo menos 10 (dez) cidades de cada Estado, observando-se o disposto na Res.-TSE nº 23.397/2013.*

Com essa decisão, logo no início da Auditoria, de adotar norma que não regulamentava uma auditoria externa e independente, a Corte Eleitoral criou fortes obstáculos ao desenvolvimento salutar das atividades de uma auditoria de qualidade forense.

De fato, várias solicitações de dados e de procedimentos de auditoria necessários para a sua completa realização foram posteriormente recusadas pela autoridade eleitoral com o argumento simples de que não estavam previstos na normatização que eles próprios, os auditados, haviam previamente criado.

Porém, o mais surpreendente foi o argumento usado pela STI para não permitir acesso dos auditores aos códigos executáveis do *software* carregado nas urnas (para que se pudesse verificar a sua integridade), como previsto nos §1º e §2º do artigo 66 da Lei 9.504/1997 e no artigo 5º da Resolução TSE 23.397/2013, sendo dito que nesse caso não se aplicariam os termos da mencionada Resolução porque:

> *Resposta ao Pedido de Esclarecimento 33 – "... os artigos citados fazem menção a um período que se encerra com a assinatura digital e lacração dos sistemas eleitorais"* (que ocorreram em 04 de setembro de 2014, antes da eleição e da auditoria, portanto)

Enfim, de forma casuística e contrariando seu próprio parecer técnico, acatado no julgamento da inicial e por ela reafirmado em várias respostas a petições dos auditores, a STI negou permissão para os auditores verificarem a integridade dos programas executáveis que carregou nas memórias das urnas eletrônicas afirmando, de forma contraditória, que os termos da Resolução 23.397/2013 sobre auditoria dos programas pelos Partidos não se aplicariam a um ambiente de auditoria do *software* posterior a 4 de setembro de 2014.

4.3.2. A STI no Processo de Auditoria

A STI do TSE assume todas as tarefas ligadas ao uso de tecnologia da informação nas eleições. Sob seu amplo guarda-chuva estão incluídas: funções de projeto dos equipamentos; definição dos parâmetros de desempenho e de segurança do sistema eleitoral; desenvolvimento do *software*; especificação técnica das licitações; recebi-

mento e guarda dos equipamentos (urnas) comprados; manutenção e logística dos equipamentos; controle de toda base de dados e dos sistemas de assinaturas digitais, inclusive tendo posse de cópias das chaves privadas de assinatura do TSE e das urnas; preparação e operação de todo o sistema informatizado de eleições; controle e guarda de todos os dados digitais gerados nas eleições, etc.

Também compete à STI fazer a auditoria interna do desempenho do próprio sistema que desenvolve e opera (uma espécie de auto-auditoria) e, ainda, oferecer ao TSE assessoria e pareceres técnicos em processos judiciais e administrativos, atuando como um verdadeiro "*perito do Juízo*", inclusive quando é parte no processo.

Todas as decisões técnicas sobre informatização foram tomadas pela Corte sempre baseada e concordante com o parecer da STI, mesmo quando o caso sob análise seja o desempenho da própria STI, sendo que na seção anterior foi descrito como a STI afetou a decisão de se permitir a auditoria especial.

Basta ler o voto vencedor do ministro relator e verificar que TODAS as decisões parciais da Corte, inclusive a decisão de permitir a auditoria sob limitações, foram tomadas em consonância com o parecer técnico da STI, sendo válido repisar que as Resoluções TSE 23.397 e 23.399, impostas à auditoria por sugestão da STI, tiveram a própria STI como a responsável pela redação da sua minuta e da redação final sobre os procedimentos de segurança e de auditoria permitidos aos partidos.

Outro exemplo marcante da influência da STI sobre as decisões da Corte ocorreu no caso da definição dos termos da resolução sobre Testes de Segurança (PA TSE nº 188-62).

Como constava do plano de trabalho desenvolver testes de penetração, o PSDB peticionou para apresentar sugestões à resolução que estabeleceria as regras desse tipo de teste. Foi aberto prazo para o recebimento de sugestões que acabaram sendo apresentadas por 4 entidades.

O PSDB e o Comitê Multidisciplinar Independente (CMInd), entre outras sugestões, peticionaram para que a STI fosse excluída como membro das Comissões de Regulamentação e de Controle dos testes justificando que era a efetividade do próprio trabalho da STI que seria avaliado e, assim, ela não teria isenção administrativa necessária para evitar-se o direcionamento e controle de tais testes. A sugestão não pedia a exclusão de membros de outros setores do TSE e também não impedia que a STI, se chamada, prestasse assessoria às Comissões.

As sugestões recebidas pelo TSE foram então submetidas ao parecer da STI, inclusive a sugestão de excluir a própria STI do controle dos testes.

A STI deu parecer contrário à sua exclusão da comissão reguladora sem responder diretamente ao argumento dos proponentes, alegando genericamente que tal comissão *"requer o envolvimento direto de pessoas com disponibilidade e vínculo com a instituição"* (TSE).

Todas as sugestões da STI foram acatadas pela Corte, inclusive a de se manter a STI como regulamentadora e controladora dos testes de segurança.

Todo esse poder de influência da STI sobre as "*regras do jogo*", mesmo em situações que caracterizem conflito de interesses, como quando seu desempenho está sob avaliação, acabaram por interferir no livre andamento da Auditoria, uma vez que até simples solicitações de acesso a dados chegaram a ser recusadas por pareceres contrários da STI, como se detalha adiante.

4.3.3. Organização Administrativa do Processo Eleitoral

Toda a atividade administrativa que ocorre dentro da Justiça Eleitoral, inclusive a presente Auditoria, é tratada e desenvolvida internamente nos mesmos moldes formais e burocráticos característicos de um processo judicial, com uma petição inicial e condução do processo por um Ministro Relator, que apresentará relatórios e votos para orientar a votação dos demais ministros. Como a função judicante é a principal e é a especialidade dos Ministros da Corte, a função administrativa costuma ser em parte delegada aos escalões administrativos do Tribunal.

Com isso, no caso de assuntos de natureza tecnológica, os mesmos funcionários do TSE que assessoram tecnicamente o Ministro na sua função de administrador eleitoral, o assessoram também quando na função de juiz.

Esta ordenação por vezes causa conflito de interesses, por exemplo, em demandas de terceiros que abordem o trabalho ou contestem pareceres da STI, pois, comumente, o juiz toma o parecer da própria STI como a de um assessor seu e não como de uma parte na demanda. Exemplo desse conflito é descrito com mais detalhes adiante.

A submissão da presente Auditoria aos ritos e procedimentos administrativos comuns em processo judicial, levou a um forte formalismo burocrático que provocou efeitos negativos ao andamento da Auditoria, descritos a seguir:

a) **Lentidão na Auditoria -** afetando negativamente a própria eficácia da Auditoria, devido ao trâmite formal ineficiente – por. ex.: simples diferenças de nomenclatura usada entre as partes (auditores e auditados) geravam dúvidas e erros de interpretação de pedidos que, em vez de serem esclarecidos rapidamente em uma conversa ou reunião, demandavam uma longa e lenta sequência de atos formais, como a protocolização de nova petição, recebimento, avaliação e encaminhamento pelo Ministro Relator, elaboração de parecer pelo corpo técnico, volta do processo ao relator para voto e julgamento em seção administrativa pelo plenário do Tribunal - e nem sempre a dúvida ficava totalmente esclarecida, levando a repetição de procedimentos. Ilustra esse problema o caso em que os auditores constataram, no primeiro dos dez dias abertos para análise do *software*, que a STI não havia disponibilizado os programas executáveis; foi então necessário fazer uma nova petição ao Ministro Relator (que estava ausente em viagem). A petição foi negada no oitavo dia, quando, mesmo se aceita, não haveria tempo hábil para sua implementação;
b) **Quebra da isenção do julgador -** embora seja adotado um rito formal de característica de processo judicial, a relação triangular normal (um polo ativo, um polo passivo e um julgador independente), que é um princípio basilar nesse tipo de processo, não foi respeitada nesta Auditoria, pois o polo ativo é o Partido requisitante (PSDB), o polo passivo é o administrador eleitoral responsável pelo processo sob auditoria – tanto no nível operacional (STI) como no nível decisório (Pleno do TSE) – e o ente julgador é também o próprio corpo diretivo do TSE, que conta com assessoria direta da STI, quebrando sua isenção, uma vez que ocupa, a um só tempo, o polo passivo e o de julgador;
c) **Auditoria comandada, na prática, pelo auditados** – essa quebra da isenção no momento de decidir a sequência da auditoria resultou em um sistemático prevalecimento das posições e decisões do ente auditado (STI/TSE) sobre qualquer vontade de atuação dos auditores do PSDB, fazendo com que os caminhos da auditoria fossem escolhidos, dirigidos e limitados pelos auditados, usurpando função e prerrogativa nativa dos auditores.

Todas as sugestões e restrições da STI/TSE, contrárias às solicitações do PSDB, foram acatadas pelo corpo decisório do TSE, impedindo a livre atuação dos auditores.

Tal forma de "*auditoria comandada pelos auditados*" não se enquadra entre três tipos de auditoria de sistemas de informação reconhecidos e padronizados pela ISACA[57]: (a) avaliação simples (*Review*); (b) auditoria profunda (*Examination*); e (c) auditoria de procedimentos acordados (*Agreed-upon Procedures Engagement*)[58].

Como exemplo do controle exercido pelo auditados sobre como podem ou não podem atuar os auditores, tem-se:

a) **Termo de Confidencialidade e Plano de Trabalho** - Foi exigida a assinatura prévia de um Termo de Confidencialidade e a apresentação de um plano de trabalho. Esta imposição, somada ao rito burocrático adotado, resultou na demora de dois meses para a entrega dos dados solicitados inicialmente (a entrega ocorreu no dia 12/01/2015), embora a regulamentação criada pelo próprio TSE estabelece que dados digitais, como RDB, BU e LOG das urnas e de totalização sejam disponibilizados, sem restrições, em apenas três dias depois de solicitado pelos partidos (art. 209 da Res. TSE 23.999/2013) e os logs do Sistema de Geração de Mídias em apenas dois dias (art. 62, § 5º Res. TSE 23.999/2013);
b) **Rigor e Complacência Assimétricos** – enquanto o polo passivo (auditados) conta com a complacência na interpretação das regras e dos prazos legais quando deixa de cumprir os procedimentos regulares (como a entrega completa dos dados das urnas em 3 (três) dias ou a disponibilização dos códigos executáveis), ao polo ativo (auditores) é exigido todo o rigor e são impostos prazos legais e extralegais. Por ex.: o pedido de acesso aos arquivos de *log* do Sistema de Geração de Mídias, que é aberto aos Partidos quando solicitado até o dia 13/01/2015 (art. 62, § 5º Res. TSE 23.999), foi negado por alegada '*preclusão*' apenas porque não constava expressamente na petição inicial, mesmo tendo sido apresentada em uma petição complementar posterior, no dia 12/11/2014;
c) **Inversão da Ordem Natural de Auditoria** - os auditores queriam receber os dados digitais completos de todas as seções eleitorais para, naturalmente, avaliá-los antes de decidir quais passariam por uma análise mais minuciosa; entretanto, prevaleceu a sugestão da STI de que os auditores deveriam definir com ante-

57 **ISACA** - *Information Systems Audit and Control Association* (Associação de Auditoria e Controle de Sistemas de Informação): é uma organização sem fins lucrativos, independente e internacional que regulamenta os papéis de profissionais do mundo inteiro quanto aos aspectos de governança, segurança, auditoria de sistemas de informação - http://www.isaca.org

58 **ISACA**. *Information Systems Auditing: Tools and Techniques* – IS Audit Reporting. Professional Practices Report 2015, pp. 10-11. - http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/information-systems-auditing-tools-and-techniques.aspx

cedência as seções onde a auditoria teria continuidade, antes mesmo de terem recebidos os dados completos, sob o argumento que as urnas deveriam passar por procedimentos de manutenção.

A exigência de se apresentar previamente um '*plano de trabalho*' a ser cumprido também pode ser considerada descabida, visto que os caminhos a serem tomados em uma auditoria são, em muito, ditados pelo próprio andamento das investigações realizadas. Entretanto, a autoridade eleitoral revelou grande inflexibilidade quando exigiu cumprimento estrito de planos de trabalhos prévios, como no caso da recusa em fornecer os arquivos de *log* do Gerador de Mídias e na recusa de permitir a recompilação dos códigos-fonte, porque não constavam da petição ou do plano de trabalho inicial.

4.3.4. Petições Negadas e Justificativas

Lista-se, abaixo, a relação dos pedidos de acesso a dados ou a procedimentos de auditoria que foram rejeitados e as respectivas justificativas apresentadas:

Pedido de acesso ou de Procedimentos	Restrições e Justificativas da Negação
Acesso aos arquivos de eleitores aptos, de faltosos e de justificativas, para avaliar as denúncias de "eleitores fantasmas" - itens 2.(b) e 2.(c).	Negado sob o argumento de não haver previsão nas Resoluções 23.397/2013 e 23.399/2013, do próprio TSE.
Acesso aos arquivos de *LOG* do sistema Gerador de Mídias (GEDAI) como previsto no art. 62, § 5º Res. TSE 23.999/2013.	Negado "*por preclusão*", embora o pedido tenha sido apresentado em 13/11/2014 e o prazo de disponibilidade desses dados se esgotasse apenas em 13/01/2015 (art. 62, § 5º Res. TSE 23.999/2013[59]).
Acesso aos '*arquivos de log referentes ao sistema de totalização*' como previsto no art. 209 da Res. TSE 23.999/2013[60].	Negado porque tais arquivos não existiriam de fato com tal designação. Foi concedido prazo de 48h para o solicitante detalhar as informações pretendidas relativas aos Siste-

59 Resolução 23.399/2013, artigo 62, § 5º: Os arquivos log referentes ao Sistema Gerenciador de Dados, Aplicativos e Interface com a urna eletrônica somente poderão ser solicitados pelos partidos políticos, coligações, Ministério Público e Ordem dos Advogados do Brasil à autoridade responsável pela geração das mídias nos locais de sua utilização até 13 de janeiro de 2015.

60 Resolução 23.399/2013, artigo 209: Após a conclusão dos trabalhos de totalização e transmissão dos arquivos de log das urnas, os partidos políticos e coligações poderão solicitar aos Tribunais Eleitorais, até 13 de janeiro de 2015, cópias desses arquivos, dos espelhos de boletins de urna, dos arquivos de log referentes ao sistema de totalização e dos Registros Digitais dos Votos.§ 1º O pedido de que trata o caput deste artigo deverá ser atendido no prazo máximo de 3 dias. § 2º Os arquivos deverão ser fornecidos em sua forma original, mediante cópia, não submetida a tratamento.

Pedido de acesso ou de Procedimentos	Restrições e Justificativas da Negação
	ma de Autenticação de Usuários, Sistema de Preparação, Sistema de Gerenciamento e dos equipamentos servidores. O prazo é exíguo para uma tarefa que se desconhece a priori, já que nenhuma explicação de como se relacionam esses sistemas foi fornecida.
Instalação de mais ferramentas de auxílio à análise de códigos (Visual Studio e Editores Hexadecimais) nos computadores disponibilizados (ped.2 e 8).	Os Editores Hexadecimais foram instalados sem restrições, mas o Visual Studio foi negado porque "*não constava do pedido inicial*" e a STI não entende que ele seja necessário.
Acesso à documentação completa relativa ao projeto de desenvolvimento de *software* de cada sistema ou aplicativo utilizado nas urnas eletrônicas, conforme faculta os §1º do art. 66 da Lei 9.504/97[61] e o art. 3º da Res. 23.397/2013[62] (ped.3 e 9).	Negado, contrariando a própria resolução do TSE, porque a STI entende que a documentação do desenvolvimento do *software* faz parte do *software* mas não do código-fonte (!?).
Especificação dos requisitos previstos de segurança ou salvaguardas, bem como a relação das normas técnicas seguidas no desenvolvimento dos sistemas e *software* eleitoral (ped.4 e 10).	Negado pela Corte seguindo recomendação da STI, a qual alegou que *"por questões de sigilo, o pedido não deve ser deferido"*
Acesso à documentação e ao fonte do *software* embarcado (*firmware*[63]) na BIOS e no circuito de segurança MSD (ped.14, 15 e 27).	Negado porque a STI entende que *firmware* é parte do *hardware* e não do *software* (!?). Também foi negado por não constar expressamente na petição inicial.
Permissão para fazer uma recompilação dos códigos-fonte, para verificar se os binários presentes nas urnas usadas na eleição derivam desses fontes, sem adulteração (ped.20 e 41).	Negado em decisão do Ministro Dias Tófolli, por não constar explicitamente da petição inicial.

61 Lei 9.504/1997, artigo 66, § 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.

62 Resolução 23.397/2013, artigo 3º: Art. 3º Os partidos políticos, a Ordem dos Advogados do Brasil e o Ministério Público, a partir de 6 meses antes do primeiro turno das eleições, poderão acompanhar as fases de especificação e de desenvolvimento dos sistemas, por representantes formalmente indicados e qualificados perante a Secretaria de Tecnologia da Informação (STI) do Tribunal Superior Eleitoral.

63 Firmware - em tradução livre da definição da PC Magazine: "*firm software*", ou instruções de *software* residentes em chips de memória não volátil. Visto em: http://www.pcmag.com/encyclopedia/term/43223/firmware

Pedido de acesso ou de Procedimentos	Restrições e Justificativas da Negação
Acesso aos códigos executáveis (binários) das urnas, conforme facultam os §1º e §2º[64] do art. 66 da Lei 9.504/97 e o art. 5º da Res. TSE 23.397/2013[65], para verificar sua integridade e conformidade com os códigos-fonte (ped.33).	Negado porque, segundo a STI, a Res. 23.397/2013 não se aplicaria nesse caso pois "*os artigos citados fazem menção a um período que se encerra com a assinatura digital e lacração dos sistemas eleitorais*" e por decisão da Presidência do Tribunal (procedimentos que extrapolassem a simples análise de código-fonte deveriam ser precedidos de aprovação prévia).
Acesso ao código compilado (executável) desenvolvido pela ABIN/CEPESC para verificar sua conformidade com o respectivo código-fonte, uma vez que este não se encontrava no DVD lacrado na cerimônia de 04 de setembro de 2014.	Negado em decisão do Ministro Dias Tófolli por não constar expressamente no pedido inicial (que, obviamente, tinha sido feito antes de se poder verificar a ausência dos fontes da ABIN no DVD lacrado).

Pode-se ver que as justificativas do TSE e da STI para obstruir atividades da auditoria impedem o pleno exercício das atividades de auditagem.

É importante destacar que, embora tenham aceitado trabalhar sob tais restrições estabelecidas pelos auditados, os auditores entendem que, em uma auditoria forense normal, não competiria aos administradores eleitorais (i.e., os auditados) decidir que procedimentos de auditoria se deve ou se pode desenvolver.

4.4. Análise dos Dados Disponibilizados

A seguir são analisados os dados que foram possíveis de obter ao longo da auditoria e as consequências negativas sobre a Auditoria pelas restrições impostas.

A análise é apresentada na mesma ordem de itens do PTI: coleta de dados, auditoria da apuração, auditoria da totalização e denúncias específicas.

64 Lei 9.504/1997, artigo 66, § 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.

65 Resolução 23.397/2013, artigo 5º: Os programas utilizados nas eleições serão apresentados para análise na forma de programas-fonte e programas-executáveis, enquanto as chaves privadas e as senhas de acesso serão mantidas em sigilo pela Justiça Eleitoral.

4.4.1. Coleta de Dados – Item 1 do PTI

O pedido de auditoria foi aprovado, com restrições definidas nas Resoluções 23.397 e 23.999/2013 do TSE, no dia 04/11/2014. Nenhum procedimento de auditoria forense foi autorizado além dos que já constassem nas resoluções citadas, mesmo que os auditores entendessem necessário.

Outra restrição foi a falta de flexibilidade para o peticionário complementar e/ou especificar o contido na petição inicial. Nos dias 12 e 13/11/2014, o PSDB apresentou quatro requerimentos complementares à petição inicial, detalhando os dados que pretendia receber para auditoria. Porém, parte desses pedidos foi negada, e a negativa mantida até o final dos trabalhos, por não constarem da petição inicial, alegando-se '*preclusão*'.

Os dados solicitados na inicial (30/11/2014) foram entregues, incompletos, no dia 12/01/2015, somente depois de assinado o Termo de Confidencialidade, embora as resoluções do TSE que liberam o acesso desses dados aos Partidos estabeleçam prazo bem mais curtos e não façam qualquer menção à necessidade de confidencialidade.

Prolongou-se até 26/01/2015 o prazo para o Partido apresentar uma lista de cidades cujas urnas deveriam ser preservadas para análise futura.

O volume dos dados entregues era grande, totalizando:

- 27 *Gigabyte* em um arquivo compactado;
- 360 Gb depois de descompactados;
- mais de 2,1 milhões de arquivos de dados (BU, RDV, LOG, etc.);
- mais de 2 bilhões de registros de LOG a serem processados e analisados;
- 1 *Terabyte* de memória necessária durante o processamento.

Foram necessários mais de 7 (sete) dias de processamento computacional apenas para descompactar e preparar esses dados todos em Bancos de Dados (relacional e não-relacional) para, só então, poder se iniciar o estudo do seu conteúdo.

Nesse instante, verificou-se que nos dados fornecidos não constavam:

a) os arquivos de Justificativas, de Eleitores Aptos e de Faltosos;
b) os arquivos de LOG do Sistema Gerador de Mídias (GM);
c) os arquivos de LOG do Sistema de Totalização (no seu lugar foram fornecidas tabelas sem todos os eventos anotados);
d) 2279 arquivos de LOG de urna em formato .txt, e 2278 arquivos de LOG binários, a grande maioria deles do Estado de São Paulo.

Tais faltas levaram a nova petição do PSDB, apresentada no dia 21/01/2015, que foi julgada em 05/02/2015 e negada em sua maior parte após manifestação da STI. A nova decisão estabeleceu:

a) Os arquivos de Justificativas, Eleitores Aptos e Faltosos não seriam fornecidos porque não há previsão para tanto nas Resoluções do próprio TSE;
b) Os arquivos de LOG do GM não seriam fornecidos por preclusão, embora o pedido tenha sido apresentado em 13/11/2014 e o prazo de disponibilidade se esgotasse apenas em 13/01/2015 (art. 62, § 5º da Res. 23.999);
c) Embora previstos no art. 209 da Res. TSE 23.999/2013[66] (com a designação de: *'arquivos de log referentes ao sistema de totalização'*), os arquivos de LOG da Totalização não foram fornecidos porque, segundo a STI, tais arquivos não existiriam de fato com tal designação, devendo o solicitante detalhar em 48h que informações desejaria receber relativos aos Sistema de Autenticação de Usuários, Sistema de Preparação, Sistema de Gerenciamento e dos equipamentos servidores (Jboss). O prazo é exíguo para uma tarefa que se desconhece *a priori*, já que nenhuma explicação detalhada de como se relacionam esses sistemas com a totalização foi fornecida;
d) Os arquivos faltantes dos LOG de urnas deveriam ser obtidos diretamente nos Cartórios que, alegadamente, não os teriam transmitido à STI.

A explicação sobre o não envio dos "arquivos faltantes" carece de credibilidade uma vez que os demais arquivos que acompanham os LOG das urnas, como RDV e Espelhos de BU, foram transmitidos regularmente e entregues.

Diante do impasse sobre a dificuldade de se obter os dados completos foi realizada uma reunião no dia 23.02.2015, nas dependências do TSE, que teve uma pauta definida nos termos do Ofício 612 da STI/TSE.

Estiveram presentes nessa reunião dois Ministros representando a Corte do TSE (inclusive o Corregedor), um representante do MPF, um representante da OAB e um representante técnico do TRE-DF.

66 Resolução 23.999, artigo 209: Após a conclusão dos trabalhos de totalização e transmissão dos arquivos de log das urnas, os partidos políticos e coligações poderão solicitar aos Tribunais Eleitorais, até 13 de janeiro de 2015, cópias desses arquivos, dos espelhos de boletins de urna, dos arquivos de log referentes ao sistema de totalização e dos Registros Digitais dos Votos.
§ 1º O pedido de que trata o caput deste artigo deverá ser atendido no prazo máximo de 3 dias.
§ 2º Os arquivos deverão ser fornecidos em sua forma original, mediante cópia, não submetida a tratamento.

Ainda, pelo corpo administrativo e técnico do TSE, participaram a Diretora Geral do TSE, o Secretário de TI do TSE, um grande contingente de chefes de setores (como ASPLAN, SEVIN, CLOGI e outros) e de técnicos da STI, e, ainda, dois técnicos do CE-PESC (ABIN) e dois técnicos da empresa Módulo.

Pelo lado do PSDB estiveram presentes os advogados Flávio Pereira e Gustavo Kanffer e os técnicos Giuliano Giova, Amilcar Brunazo Filho e Marco Carvalho.

Nessa reunião foram estabelecidos os procedimentos de coleta, nos TRE's, de dados das urnas selecionadas e foram feitas cópias do conteúdo do DVD lacrado no dia 04.09.2014 em cerimônia oficial no TSE e que continha (ou deveria conter) todo o *software*, fonte e executáveis, do sistema eleitoral informatizado, para posterior análise pelos auditores.

Posteriormente, nos TRE's foram coletados os dados de urnas escolhidas pelo PSDB, os dados do Teste de Votação Paralela e os dados do Sistema Transportador.

A coleta de dados das urnas não foi permitida por cópia direta do conteúdo das mídias, mas sim de forma indireta, com a utilização dos programas RED e VPP das próprias urnas, que geraram novas mídias com os arquivos de LOG, BU e RDV e imprimiram cópias do BU, da lista de resumos criptográficos (*hash*) dos cartões de memória interno (FI) e externo (FE) e da lista de justificativas.

O impedimento, pelo TSE, de se obter os dados pela leitura direta das mídias de memória das urnas criou uma grave lacuna na auditoria, afastando-a em termos de qualidade e de confiabilidade de uma auditoria forense: afinal, como os dados fornecidos são gerados pelo próprio *software* que se deseja auditar, sua confiabilidade para tal fim fica totalmente comprometida.

Também foram tiradas fotos dos lacres das urnas e das Listas de Votação (com as assinaturas dos eleitores) e filmadas a tela das urnas durante o processo de inicialização (*boot*) dos programas RED e VPP.

Dos Testes de Votação Paralela foram copiados os arquivos de LOG, BU e RDV de cada urna testada e tiradas cópias das atas da cerimônia, do Relatório do Sistema de Conferência dos Resultados e do relatório de auditoria da empresa Maciel.

Os aparentemente equivalentes aos '*arquivos de log referentes ao sistema de totalização*' previstos no Art. 209 da Res. TSE 23.999/2013, seriam extraídos dos arquivos do Sistema Transportador ou JE-Connect.

Os trabalhos de coleta de dados nos TRE's se iniciaram no DF em 02.03.2015, onde se testaram os procedimentos definidos na reunião anterior, até o dia 22.05.2015, quando se encerraram as coletas nos TRE-PA e TRE-RJ.

Ao todo foram coletados dados de 684 urnas nos TRE's de 18 estados, a saber: Acre, Alagoas, Amazonas, Bahia, Ceará, Distrito Federal, Goiás, Maranhão, Minas Gerais, Paraíba, Pará, Paraná, Pernambuco, Piauí, Rio de Janeiro, Rio Grande do Norte, São Paulo.

Não foram coletados os dados nos estados seguintes: Amapá, Espírito Santo, Mato Grosso, Mato Grosso do Sul, Rondônia, Roraima, Rio Grande do Sul, Santa Catarina, Sergipe, Tocantins e das Embaixadas no exterior.

A quantidade de equipamentos passíveis de auditoria (universo de mais de 420 mil) e sua dispersão geográfica por todo o território brasileiro, criam, naturalmente, obstáculos de natureza econômica e logística à Auditoria. Porém, entende-se que o impedimento de acesso direto às mídias de memória, para se obter cópia de seus dados, foi um grave obstáculo adicional.

4.4.2. Auditoria da Apuração, via *Software* – Item 2 do PTI

Uma auditoria da apuração em sistema eleitoral eletrônico do tipo DRE sem VVPAT depende totalmente de uma profunda e completa análise de validação e de certificação do *software* embarcado nos equipamentos de votação e de apuração - as urnas eletrônicas - uma vez que não se produz uma trilha documental para auditoria contábil que permita a recontagem dos votos como vistos e confirmados pelo eleitor.

A sugestão do Ministro Henrique Neves, apresentada durante o julgamento do pedido inicial, para se fazer uma auditoria contábil da apuração pela impressão dos arquivos RDV de cada urna e contagem desses "*votos impressos*", carece de eficácia por sua redundância, pois os números gravados nos arquivos RDV não puderam ser vistos e confirmados pelo eleitor no momento da votação. Em termos simples, seria o mesmo que querer certificar a veracidade de um documento, meramente comparando-o com uma fotocópia do próprio documento.

Uma contagem desse tipo só acrescentaria custos e riscos de erros humanos à Auditoria, sem propiciar qualquer garantia de que os arquivos RDV estivessem íntegros.

Estabeleceu-se que a análise do *software* eleitoral seria feita ao longo de 10 dias úteis, nas dependências do TSE, sobre os arquivos extraídos do DVD lacrado antes da eleição[67].

A auditoria da apuração, o PTI previa doze tarefas. No entanto, a auditoria por validação do *software* eleitoral teve seu resultado totalmente prejudicado pelas restrições impostas ao trabalho dos auditores. Mais precisamente, dez das tarefas previstas no PTI não puderam ser concluídas a contento e as restantes (avaliação dos lacres e da Votação Paralela) revelaram impropriedades, como se descreve a seguir.

4.4.2.1. Quantidade de Votos Gravados

Atividade prevista no PTI: verificar as consistências internas entre a quantidade de votos gravados nos diversos arquivos de controle de cada urna (RDV, BU, LOG, Eleitores Aptos e Faltosos).

A verificação da consistência interna na quantidade de votos digitais gravados nos diversos arquivos de controle de cada urna tem por finalidade detectar eventual mau funcionamento do *software* ou, ainda, detectar fraudes grosseiras no *software* embarcado que alterem o resultado no arquivo de BU sem alterar os demais.

A cada vez que um eleitor confirma o seu voto final, três procedimentos são desenvolvidos pelo *software* da urna: inclui-se uma cópia do voto no arquivo RDV, marca-se o nome do eleitor como já tendo votado e registra-se o evento "*voto computado*" no arquivo de LOG. Ao final da votação os votos do RDV são contados e registrados no arquivo de BU.

Dessa forma, para se verificar o funcionamento coerente do *software* durante a votação e a apuração, deve-se analisar a coerência dos registros nos seguintes quatro arquivos disponíveis nas urnas, de onde se pode obter o total de votos confirmados (votos válidos + brancos + nulos = comparecimento):

a) RDV – contém o registro digital de cada voto confirmado;
b) LOG – registra a hora e data de cada voto confirmado;
c) BU – registra os totais de eleitores aptos, de comparecimento e de votos válidos, brancos e nulos;
d) Faltosos – indica a quantidade de eleitores que não votaram, permitindo determinar o comparecimento por diferença com os eleitores aptos.

67 Foram disponibilizados para análise quase 50 mil arquivos contendo mais de 17 milhões de linhas de código-fonte.

A autoridade eleitoral recusou-se a fornecer os arquivos de eleitores faltosos, alegando que isso não estava previsto na sua própria Resolução 23.397/2013, adotada como normativa dos trabalhos da auditoria, conforme anteriormente discutido.

A comparação dos totais de votos computados registrados nos demais arquivos não constatou incoerências significativas[68].

Considera-se incompleta essa etapa da auditoria do *software* das urnas, por não ter sido permitido comparar os dados de todos os arquivos disponíveis, mas apenas dos arquivos escolhidos pelos auditados.

4.4.2.2. Requisitos de Segurança, Salvaguardas e Normas Técnicas

Atividade prevista no PTI: avaliar toda a implementação do sistema (hardware e software), para verificar se os requisitos de segurança do projeto, as salvaguardas anunciadas e as normas técnicas adotadas foram atendidas

Esta tarefa de auditoria tem por objetivo verificar a conformidade do projeto completo das urnas (*hardware* e *software*) com as normas técnicas e boas práticas aplicáveis e com as próprias especificações de segurança, podendo servir como um forte indicativo da qualidade, da confiabilidade e da segurança do sistema para os interessados externos, como os eleitores e os candidatos.

Em toda a propaganda institucional do seu sistema eleitoral eletrônico, o TSE utiliza com frequência a expressão "*Salvaguardas do Sistema*" como garantia da confiabilidade; porém, na página oficial do TSE só se encontram referências informais e incompletas sobre quais seriam tais salvaguardas.

Para obter uma descrição oficial e completa das informações necessárias, os auditores solicitaram o seguinte:

> *(ped.4) Solicitamos o fornecimento de uma descrição completa e detalhada das Salvaguardas de Segurança aplicáveis ao uso do hardware e do software do Sistema Eleitoral Informatizado do TSE.*

68 Em apenas 60 urnas (12 biométricas e 48 comuns) foram detectadas pequenas divergências que podiam ser explicadas por virem de urnas de contingência nas quais os arquivos de log apresentavam diferente formatação.

> *Solicitamos, ainda, que tal descrição inclua uma relação das Normas Técnicas e padrões internacionais relacionados, utilizados no projeto do Sistema Eleitoral Informatizado, inclusive relativos à Segurança de Dados e ao Desenvolvimento de Software.*
> *(ped.10 – de reiteração do ped.4) ... Para que possamos verificar se o código-fonte apresentado atende os requisitos iniciais do projeto é necessário no mínimo saber quais são tais requisitos, como as salvaguardas de segurança pretendidas e as normas técnicas que regulamentam tais metas.*

Para surpresa dos auditores, a autoridade eleitoral recusou-se a fornecer uma descrição formal e completa de quais seriam os requisitos de segurança e as normas técnicas que segue no projeto do sistema eleitoral.

O motivo alegado pelo Presidente do TSE para essa negativa foi dado em sua decisão de 19 de março de 2015, quando alegou "*questões de sigilo*" conforme parecer técnico da STI que tem o seguinte teor:

> *Informação nº 51 – ASPLAN/STI de 17 de março de 2015 – pág. 7*
> *Considerando serem as salvaguardas os aspectos de prevenção e segurança dos sistemas eleitorais, esta STI entende que, por questões de sigilo, o pedido não deve ser atendido.*

Considera-se esta tarefa da Auditoria <u>100% prejudicada pela surpreendente recusa da autoridade eleitoral de fornecer uma relação dos requisitos de segurança e das normas técnicas que adotou no projeto e desenvolvimento do seu sistema eleitoral informatizado</u>.

Consequentemente, <u>não foi possível afastar</u> as hipóteses de que, de fato:

a) a autoridade eleitoral <u>não possui uma relação formal de requisitos de segurança</u> no projeto das urnas eletrônicas;
b) o sistema eleitoral eletrônico brasileiro <u>não está em conformidade com qualquer norma técnica reconhecida de projeto e de segurança</u>.

4.4.2.3. Certificação Digital

Atividade prevista no PTI: avaliar o sistema de certificação digital usado na assinatura digital dos sistemas eleitorais, quanto a sua conformidade com o padrão ICP-Brasil

Embora a autoridade eleitoral tenha recusado informar quais seriam as salvaguardas do sistema eleitoral informatizado, depreende-se do apresentado na página oficial do TSE que a assinatura digital do *software* e sua verificação são etapas cruciais na segurança das urnas eletrônicas.

Toda a validação de segurança passa pelo ato de assinatura e se completa na verificação das assinaturas digitais.

Para aplicar o conceito de assinatura e de certificados digital, o TSE optou por criar sua própria autoridade certificadora que não passa por qualquer auditoria externa e pela certificação oficial que o padrão legal e oficial *ICP-Brasil* exige, como confirma a resposta ao Pedido de Esclarecimento 29, nos seguintes termos:

> *O TSE é a primeira autoridade de certificação. Não há certificação externa dos certificados utilizados pelo TSE*

Sendo assim, o certificado raiz, bem como todos os demais certificados utilizados no processo eleitoral, são gerados pelo próprio TSE e resultam no seguinte:

a) Não existe algum certificado de um terceiro confiável que possa ser utilizado para validar os certificados da certificadora do TSE. Ou seja, ninguém, externo ao grupo dos executores das eleições, tem como certificar se houve alguma fraude ou problema com algum certificado utilizado pelo TSE nas eleições;
b) O certificado raiz não é público para ser conferido ou usado na conferência, das assinaturas digitais feitas;
c) As chaves públicas utilizadas não são realmente públicas e não podem ser conferidas;
d) As medidas de segurança para se evitar vários possíveis problemas ou fraudes não podem ser auditadas pelos partidos e ou fiscais;
e) Para ter alguma validade em uma perícia forense, o "carimbo de tempo" (*time stamp*[69]) tem que ser obtido de algum sistema servidor externamente certificado, o que não é viável de ser feito dentro do sistema do TSE, uma vez que

69 *Time stamp*: comprovação do horário em uma assinatura digital foi feita

não há como determinar que há um terceiro para garantir que o horário e o certificado estão corretos;

f) O CEPESC tem participação nesta certificadora, mas não ficou claro qual é esta participação.

É muito importante o uso de carimbo de tempo externamente certificado na assinatura digital dos componentes de *software* e de dados. É através dele que um auditor externo poderia verificar se a data e a hora reais da assinatura do *software* eleitoral ocorreram efetivamente durante a cerimônia oficial de compilação dos programas.

Existem vários tipos de quebra de segurança que podem ocorrer durante a geração e utilização de certificados e das chaves privadas associadas. Como, por exemplo:

a) Chaves fracas – passíveis de serem quebradas com pouco esforço computacional;
b) Vazamento de chaves privadas;
   Troca do certificado raiz – o que pode permitir que uma falsa assinatura seja avaliada como correta;
c) Cópia de uma chave privada em mais de uma mídia;
d) Clonagem da mídia com a chave privada;
e) Fraude no ambiente – quando se está utilizando uma chave privada para se fazer uma assinatura;
f) Mal-uso de uma chave privada pelo responsável por guardá-la.

Estes tipos de possíveis problemas não podem ser 100% evitados. A melhor maneira de minimizar a ocorrência de problemas é através da transparência, fiscalização e auditoria externas. Entretanto, a verificação desses três importantes aspectos não foi permitida pelo TSE, nas eleições 2014, em relação à certificação digital que desenvolve e utiliza.

Também é de vital importância que as assinaturas digitais possam ser verificadas em equipamentos que não sejam computadores ou urnas eletrônicas do TSE. Isto é, o fiscal ou auditor externo deve utilizar um equipamento seu e não deve ser obrigado a aceitar, como confiável, um equipamento sobre o qual ele não tem controle. Porém, a autoridade eleitoral não permite que qualquer verificação de assinaturas seja feita em um computador de confiança do auditor.

Conclui-se que a certificação digital, componente fundamental na segurança do processo eleitoral informatizado, não se apresenta em conformidade com o padrão oficial *ICP-Brasil*, restando apenas a palavra dos próprios operadores como garantia de confiabilidade do processo.

4.4.2.4. Metodologia e Documentação do *Software*

Atividade prevista no PTI: avaliar a documentação descritiva do desenvolvimento do software das urnas para determinar o seu grau de maturidade e de adequação às técnicas e boas práticas de engenharia de software

O objetivo da análise da documentação do *software* é determinar o seu grau de conformidade com as boas práticas de Engenharia de *Software*. A documentação do *software* disponibilizada para análise do código-fonte mostrou-se bastante incompleta, o que dificultou sua análise e compreensão.

Como consequência, foram apresentados dois pedidos de complementação dos dados nos seguintes termos:

> *(Petição 03) "Solicitamos que seja disponibilizada a documentação completa relativa ao projeto de desenvolvimento de software de cada sistema ou aplicativo utilizado nas urnas eletrônicas e nos demais computadores no processo eleitoral, incluindo a documentação descritiva das metodologias de desenvolvimento de software empregadas."*
>
> *(Petição 09) "... informamos que o que está disponível nos equipamentos está incompleto ao menos em relação à documentação dos sistemas da urna eletrônica, faltando a) toda a especificação de requisitos de software e b) os diagramas de classes, de atividade e de estados de vários sistemas, como, por exemplo, o HOTPLUGUE, INITJE, SAVD, SJE, VPP, SCAUE (Autenticador) e partes do GAP (020-carrega info Municipio e MunZona, 11_Monta_regras e 20_Verifica_Possibilidade) ... Além disso, ela é essencial, necessária e imprescindível para o pleno entendimento do código-fonte propriamente dito e para a verificação se tal código de fato implementa os requisitos e salvaguardas alegados pelos técnicos que nos tem prestado esclarecimentos verbais. Por exemplo, estamos com dúvida no funcionamento de partes do VPP e do GAP e a visualização da documentação de alto nível auxiliaria a esclarecer tais dúvidas com maior rapidez.*

No entanto, não houve sucesso em obter os complementos de documentação solicitados. Nas respostas da STI, alegou-se tão somente que o pedido da documentação extrapolava o pedido inicial de auditoria do *software*, nos seguintes termos:

> *(Resposta à Petição 03) ... Esta Secretaria de Tecnologia da Informação esclarece que a documentação dos sistemas encontra-se disponível nos equipamentos instalados e pode ser complementada por meio dos pedidos de esclarecimentos ... esta Secretaria não pode atender à solicitação por meio desse instrumento, sendo assim necessário que os pedidos que extrapolem o objeto dos trabalhos sejam feitos por meio de Petição protocolizada e direcionada à Presidência do Tribunal.*
> *(Resposta à Petição 09) ... Nesse sentido, como na petição de Protocolo TSE Nº 4.455/2015, juntado ao processo judicial Petição Nº 1855-20.2014.6.00.0000, o requerente expressamente solicitou análise de código-fonte, entende-se que não é objeto da análise qualquer documentação associada. Ainda assim, a STI/TSE tem fornecido documentação de apoio ao entendimento do código-fonte. Grande parte dessa documentação encontra-se junto ao código-fonte e outras foram entregues ao longo dos trabalhos.*
> *Por último, numa abordagem mais moderna da disciplina de Engenharia de Software, os principais autores reduzem a importância de uma documentação detalhada, em virtude do dinamismo na evolução dos requisitos do software. Na prática, a única verificação quanto à validade do comportamento de um software é a análise do seu código-fonte.*

Na auditoria de sistema de *software*, em busca de vulnerabilidades[70] (fraquezas que podem ser disparadas acidentalmente ou exploradas intencionalmente), tem-se dois propósitos[71]: i) auditar a aplicação de *software* em si; ii) auditar o desenvolvimento da aplicação, incluindo a metodologia usada no seu desenvolvimento.

70 **NIST-RA**. "*Guide for Conducting Risk Assessments*". USA: NIST Special Publication 800-30 Revision 1, 2012 - http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

71 **ISACA**, "*Information Systems Auditing: Tools and Techniques*". USA: IS Audit Reporting, 2015 - http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/information-systems-auditing-tools-and-techniques.aspx

Ao auditar a aplicação de *software*, deseja-se verificar e avaliar, entre outros potenciais, os seguintes aspectos: segurança no sentido de *security* (proteção contra agentes externos), segurança no sentido de *safety* (confiabilidade quanto à resposta a eventuais falhas), disponibilidade, integridade de dados e de código, armazenamento e recuperação de dados, transmissão de dados e disseminação de programas e dados nas urnas. Isso, embora com muitas restrições impostas pelo TSE, encontra-se apresentado nos outros itens deste relatório.

Ao auditar o desenvolvimento da aplicação, visou-se dois pontos: (i) a revisão do processo de desenvolvimento e das metodologias, políticas e procedimentos empregados no desenvolvimento dos sistemas de *software* do TSE; e (ii) o exame do desenvolvimento e implementação do aplicativo de *software*, para verificar a conformidade com o processo de desenvolvimento adotado e avaliar o sistema final.

No item (i), buscou-se analisar e avaliar o seguinte:

a) A adequação da mesma ao tipo de aplicação de *software* alvo;
b) O uso de padrões nacionais e internacionais que ajudam a garantir a qualidade durante o desenvolvimento do *software* desenvolvido;
   O uso de padrões nacionais e internacionais que ajudam a garantir aspectos de segurança durante o desenvolvimento do *software* desenvolvido;
c) O uso de padrões nacionais e internacionais na auditoria de *software* de terceiros antes de promover a integração desses *softwares* na aplicação de *software* desenvolvida.

As aplicações de *software* que constituem o sistema de votação eletrônica do TSE podem ser consideradas partes de um *software* de missão crítica[72].

Para ajudar a avaliar a adequação da documentação do *software* do TSE no contexto tratado aqui, desmembrou-se a análise das afirmações ou assertivas da STI, da seguinte forma:

4.4.2.4.1. Não é correto afirmar que a "única verificação quanto à validade do comportamento de um software é a análise do seu código-fonte".

A última frase da resposta à Petição 09 (*"Na prática, a única verificação quanto à validade do comportamento de um software é a análise do seu código-fonte"*), além de difícil de entender, não tem respaldo da literatura, muito provavelmente sendo esta

72 *Software* de missão crítica é um *software* em que uma falha é provável que resulte na perda de vida ou danos ambientais, conforme:**Sommerville, I**. "*Engenharia de Software - 9ª ed*". São Paulo: Pearson Education BR. 2011
No caso do *software* eleitoral, pode resultar em danos à democracia e à justa disputa pelos cargos eletivos.

a razão pela qual a afirmação é apresentada sem referência bibliográfica alguma. Essa afirmação parece estar associada ao princípio ágil de programação[73], em que todos os membros do time de desenvolvimento são donos do código[74].

Essa propriedade coletiva é promovida e reforçada pelo outro princípio ágil de programação em pares[75] (em especial da metodologia ágil Programação Extrema), fazendo com que todos, com a supervisão de um par, exercitem autonomamente a programação de novas funcionalidades e supostamente aumente a produtividade e conhecimento coletivo do código sendo produzido. Contudo, Meyer[23] mostra que não há evidências fidedignas de que esses dois princípios ofereçam melhorias para o processo de programação; tudo parece depender mais da qualidade dos membros do time envolvido, sendo esse tipo de abordagem voltada ao desenvolvimento de *softwares* de porte pequeno a médio.

Além disso, qualquer abordagem de desenvolvimento de *software*, incluindo métodos ágeis, devem ter claros os requisitos do *software*, para que os programadores saibam os objetivos do código que estão desenvolvendo e, portanto, tenham um direcionamento mínimo de suas tarefas. É comum que tais requisitos evoluam durante o processo de desenvolvimento, mas, ao final do processo, quando o *software* é finalmente concluído, eles devem estar claros o suficiente para serem documentados, permitindo (1) evoluções futuras e (2) verificação por pessoas que não participaram do processo de desenvolvimento.

Ambler[76] apresenta algumas ideias de documentação de projeto de *software* em geral com métodos ágeis; o objetivo não é evitar documentar, mas documentar apenas o que agregue valor e na quantidade e hora certas, o que: (1) em sistemas críticos sem dúvida incluem os objetivos de segurança de cada módulo e as salvaguardas utilizadas para garantir seu correto funcionamento, para evitar que alterações posteriores invalidem sua segurança; e (2) em sistemas auditáveis incluem descrições razoavelmente detalhadas de seus principais módulos, agregando valor para os auditores. Des-

73 **Meyer, B.** "Agile! The Good, the Hype and the Ugly". : Springer, 2014 -http://www.springer.com/978-3-319-05154-3

74 Propriedade coletiva do código: dado que todos do grupo de desenvolvimento supostamente têm conhecimento do código sendo desenvolvido, qualquer um deles poderia fazer modificações no código em desenvolvimento; portanto, eles supostamente conhecem o comportamento do *software* no nível do código-fonte

75 **Sommerville, I**. "*Engenharia de Software - 9ª ed*". São Paulo: Pearson Education BR. 2011

76 **Ambler, Scott**. "*Agile/Lean Documentation: Strategies for Agile Software Development*", 2012 - www.agilemodeling.com/essays/agileDocumentation.htm

se modo, ao final, haverá uma documentação mínima, mas completa, para atender as necessidades de certificação ou auditoria interna ou externa.

De qualquer forma, mesmo se fosse verdade que a programação ágil não resulta em qualquer tipo de documentação, também não há evidência na literatura de que um auditor que acabe de tomar contato com um *software* contido em cerca de 50 mil arquivos terá facilidade no entendimento do código-fonte disponibilizado para avaliação em apenas 2 semanas, em especial tendo em vista que a pouca documentação interna, como comentários no código-fonte, nem sempre estava adequada, completa ou sequer correta.

Essa frase da resposta do STI parece ter sido usada para depreciar a necessidade de documentação associada para facilitar o entendimento do código pelos auditores. De fato, parece que ela foi tirada de um contexto que não se reproduz no contexto da resposta, em especial por ela não se aplicar de forma alguma a sistemas de missão crítica.

4.4.2.4.2. A documentação colocada à disposição estava incompleta, muitas vezes inconsistente com a correspondente parte do código-fonte e prejudicou o entendimento mais rápido e ágil do código-fonte associado, no tempo de apenas 2 semanas da auditoria.

Quando se fez uso da documentação para entender e tirar dúvidas sobre o funcionamento de algumas partes críticas, notou-se o quão curto foi o prazo para essa tarefa dos auditores. Muitos pontos críticos não puderam ser estudados a contento por falta da documentação apropriada ou por haver inconsistências ou discrepâncias com o respectivo código-fonte, fazendo necessário recorrer à ajuda pessoal dos técnicos do TSE. Destaque-se que a ajuda dos técnicos sempre foi muito cooperativa, mas nem sempre efetiva em eliminar todas dúvidas surgidas.

Como o código-fonte é a palavra final, tais discrepâncias ocorreram por causa de documentação desatualizada, conforme relatado na Petição 42: *“Cabe notar ainda que os arquivos de documentação fornecidos em parte pelo STI se mostraram desatualizados, pois há divergências em relação aos códigos-fonte examinados”.*

Com base apenas na documentação do *software* da urna, explicitado na Petição 09, estima-se que faltou cerca de 25% da documentação. A resposta da petição 09 vem corroborar essa impressão: *“Grande parte dessa documentação encontra-se junto ao código-fonte e outras foram entregues ao longo dos trabalhos”*. Acrescentamos que “*outras*” corresponde a pouca documentação adicional.

Extrapolando essa estimativa para todo o código-fonte disponibilizado, pode-se estimar que cerca de 75% da documentação associada estava presente.

Considerando que toda documentação adicional tivesse sido fornecida como resposta às petições 03 e 09 (*"documentação completa relativa ao projeto de desenvolvimento de software de cada sistema ou aplicativo utilizado nas urnas eletrônicas e nos demais computadores no processo eleitoral, incluindo a documentação descritiva das metodologias de desenvolvimento de software empregadas"*), adicionada às documentações referentes aos padrões nacionais e internacionais supostamente usados pelo TSE mais a documentação das salvaguardas de segurança solicitadas nas petições 04 e 10 (também recusadas), estima-se que a parte entregue, numa estimativa grosseira para efeito comparativo, corresponderia a apenas 25% do total solicitado.

4.4.2.4.3. A qualidade dos comentários no código-fonte, de maneira geral, não era muito boa.

Isso ficou demonstrado em comparação com o código desenvolvido pelo CEPESC, cuja documentação por comentários era bem superior ao do código do TSE, fato que se explicitou na Petição 42. Numa escala de 1 a 5: pessimamente documentada, mal documentada, neutra, bem documentada e muito bem documentada – **estimamos 3 (neutra).** Ou seja, não ajuda muito nem prejudica muito; quando a dúvida, contudo, envolvia código comentado dessa maneira, porém, com ausência de documentação, a situação ficava crítica e dificultava muito o trabalho dos auditores. Embora um bom projeto e uso adequado de padrões de projeto, nomes apropriados de variáveis, métodos e classes possa reduzir a necessidade de comentários no próprio código, não se pode considerar uma boa prática a ausência de documentação mais abrangente e externa ao código-fonte para o entendimento por pessoas externas que desejam verificar a qualidade do *software*.

4.4.2.4.4. A metodologia empregada não é apropriada para o desenvolvimento do software do sistema de eleição eletrônica do TSE.

Embora não se tenha obtido uma resposta por escrito à petição 03, pode-se considerar que a metodologia usada seja uma metodologia ágil. Ao menos isso foi informado em conversa com técnicos do TSE, que não especificaram qual metodologia ágil era a adotada. Adicionalmente, o último parágrafo da Resposta à Petição 09 é um indício do uso de metodologia ágil, tanto pelo texto (*"Por último, numa abordagem mais moderna da disciplina de Engenharia de Software, ..."*), quanto pela referência bibliográfica citada (embora um tanto antiga, mas representativa: BECK, Kent. *Embracing Change with Extreme Programming*. IEEE Computer, v. 32, n. 10, 1999, p 70-78.).

Segundo Sommerville[77], métodos ágeis são bastante adequados a equipes pequenas, para desenvolver *softwares* de pequeno porte e que não sejam críticos. Desse ponto de vista, o *software* da eleição eletrônica do TSE não parece apropriado para ser desenvolvido e evoluído por meio de método ágil, pois é *software* de missão crítica e de grande porte.

Embora exista um trabalho muito grande na indústria de *software* para escalar métodos ágeis para *software* de grande porte[78], o fato de ser de missão crítica coloca uma barreira muito forte para se utilizar método ágil plenamente no seu desenvolvimento.

Cabe notar que alguns autores mostram que é possível aplicar alguns princípios de métodos ágeis em sistemas críticos, mas outros princípios não[79]. Por exemplo, há uma necessidade de uma fase bem intensiva de análise e projeto, bem como desenvolver uma documentação um tanto extensa, em geral em atendimento a regulamentos externos ou pela adoção de padrões ou normas internacionais que precisem ser, inclusive, certificadas.

Conforme discutido por Douglas[80], estender e adaptar métodos ágeis para sistemas críticos acaba levando a um processo muito trabalhoso e bastante burocrático.

Mesmo se forem levadas em consideração as colocações desses dois últimos autores, as adaptações por eles propostas se concentram em tentar aplicar método ágil a sistemas de missão crítica, mas não garantem que funcione para *software* de grande porte também.

Em conclusão, o sistema de eleição eletrônica do TSE, por ser tanto de grande porte quanto de missão crítica, não parece ser adequado para a técnica de desenvolvimento ágil. Principalmente por trazer um *software* legado considerado, parece que um processo mais estruturado, como em Cascata[81], seja o mais adequado para o desenvolvimento incremental e evolutivo do *software*.

---

77 **Sommerville, I**. "*Engenharia de Software - 9ª ed*". São Paulo: Pearson Education BR. 2011

78 **Stober, T; Hansmann, U**. "Agile *Software* Development: Best Practices for Large *Software* Development Projects". Berlin: Springer-Verlag, 2010.

79 **SAPM**. *“Agile and Critical Systems”*. SAPM: Course Blog, 2014. - https://blog.inf.ed.ac.uk/sapm/author/s0841373/

80 **Douglass, B.P., and Ekas, L**. *"Adopting agile methods for safety-critical systems development"*.: IBM, 2012 - http://www.nohau.se/$2/file/douglass-adopting-agile-methods-for-safety-critical-systems-development.pdf

81 SAPM. "Does Waterfall Deserve its Bad Press?". SAPM: Course Blog, 2014 - https://blog.inf.ed.ac.uk/sapm/2014/02/13/does-waterfall-deserve-its-bad-press/

Em especial, tal abordagem é recomendada para cenários em que os requisitos do *software* sejam razoavelmente bem compreendidos, o que deveria ser o caso da urna eletrônica após tantos anos de utilização.

4.4.2.4.5. A documentação associada e entregue junto com o código-fonte disponibilizado, incompleta, é a única documentação que o TSE possui.

Considera-se incompreensível a recusa, mesmo respaldada em resoluções do TSE, de entregar toda a documentação disponível. O objetivo declarado do TSE sempre foi, não apenas nesta Auditoria Especial, disponibilizar todo o *software* para exame dos partidos. Em seis meses, mesmo com as restrições ambientais de trabalho impostas pelo TSE aos auditores, seria possível entender o código sem a ajuda de documentação, caso algum partido se dispusesse a financiar e encontrasse um grupo de especialistas disposto a encarar essa tarefa, demasiadamente cansativa e difícil.

Se é verdade que o TSE está realmente interessado que os partidos analisem e validem o *software* desenvolvido por eles e terceiros associados, então não parece existir motivo real para impedir ou deixar de fornecer aos auditores o acesso a toda documentação disponível. Pelo contrário, o efeito de oferecer o conjunto completo de documentos associados seria facilitar a realização da tarefa e diminuir sensivelmente o tempo de avaliação do código-fonte pelos auditores, ou ao menos permitir uma maior abrangência em tal análise.

Assim, conclui-se que, a menos que o TSE não possua documentação de todo o projeto do *software* da eleição eletrônica, o que configuraria uma situação muito grave, pois o *software* é de missão crítica e deveria possuir uma forte e completa documentação associada, seria do próprio interesse do TSE apresentar toda documentação para demonstrar a alegada transparência do processo de validação do *software*.

4.4.2.4.6. Sendo um software de missão crítica, a documentação do software da eleição eletrônica do TSE deveria ser completa e de qualidade

Por ser um *software* de missão crítica, o TSE deveria estar com documentação preparada para garantir que está conforme as normas nacionais e internacionais de segurança, bem como com a leis e regulamentos que se aplicam ao processo eleitoral; se não por imposição legal, tal transparência poderia ao menos ser motivada por desejo de realizar auditorias internas e se assegurar que seu processo está aderente às melhores práticas e normas de segurança, demonstrando ainda estar pronto para auditorias externas, como a presente Auditoria Especial.

Neste caso, como discutido anteriormente no item E acima, não é especialmente relevante o uso do processo em Cascata – que naturalmente induz a se ter uma forte documentação – ou de algum método ágil adaptado a sistemas de missão crítica e de grande porte: ao final, deverá ser apresentada uma documentação apropriada e condizente com as necessidades do tipo de *software*.

4.4.2.4.7. Conclusão sobre a avaliação da documentação do software

Essa tarefa de auditoria não foi plenamente atendida, pois a documentação do *software* disponibilizada para análise mostrou-se bastante incompleta.

Embora tenha sido possível tirar muitas conclusões importantes na realização dessa tarefa, no que diz respeito ao entendimento mesmo que parcial do código, constata-se que as condições oferecidas pelos TSE foram muito restritivas e impediam a otimização do tempo de análise.

A análise realizada mostra a ausência (ou, ao menos, uma adoção insuficiente) de boas práticas em Engenharia de *Software* voltadas a projetos de grande porte e de missão crítica.

Cabe notar que a presente análise referente à metodologia e à documentação do *software* eleitoral teve resultado bastante semelhante ao descrito no *Relatório da Fundação COPPE-UFRJ*[82], de 2002, no qual também era apontada a incompletude da documentação e a metodologia inadequada no desenvolvimento do *software* eleitoral, sugerindo que esse problema persiste desde então.

4.4.2.5. Análise do Código-fonte

Atividade prevista no PTI: analisar o código-fonte completo de todo o software carregado nas urnas eletrônicas, obtendo o software fonte no DVD lacrado no dia 04.09.2014 no TSE, para avaliar sua completude e a eventual existência de vulnerabilidades que pudessem ser exploradas em ataques internos e externos

No entender dos auditores, na expressão "*todo o software embarcado*" se inclui, ao menos: o *firmware*[83] gravado em circuitos internos, o BIOS (Basic Input e Output

82 **Rocha, A.R.C. et al**. "*Relatório de Avaliação do Software TSE realizada pela Fundação COPPETEC*". Brasília: COPPE/UFRJ, 09/08/2002 - http://www.angelfire.com/journal2/tatawilson/coppe-tse.pdfver resumo em: http://www.votoseguro.org/textos/relcoppetec1.htm

83 *Firmware* - em tradução livre da definição da PC Magazine: "*firm software*", ou instruções de *software* residentes em chips de memória não volátil . Visto em: http://www.pcmag.com/encyclopedia/term/43223/firmware

System), o *Loader* gravado nas mídias de inicialização, o Sistema Operacional e todos Aplicativos com suas respectivas bibliotecas internas e externas

A análise do código-fonte completo de um sistema é parte da validação do *software* e é etapa essencial em um sistema eleitoral que, por concepção, tem a confiabilidade do resultado que publica integralmente dependente da qualidade do *software* embarcado nas urnas no dia da eleição, como no presente caso.

Para ser correta e completa, uma validação de *software* de missão crítica, i.e., que requer alto nível de confiabilidade, deve desenvolver uma análise de todos códigos-fonte de todo o sistema, incluindo o *software* desenvolvido internamente e também o recebido de terceiras partes, deve verificar se os procedimentos de compilação (transformação dos programas fontes em programas executáveis) não provocaram a inserção de adulterações maliciosas e, por fim, deve efetuar testes tão exaustivos quanto possível sobre o programa compilado para verificar eventuais comportamentos indevidos (sejam eles propositais ou causados por um erro ou descuido na programação).

Uma validação desse tipo requer uma equipe ampla de auditores com especializações diversas, muito tempo de trabalho minucioso e resulta em altos custos, normalmente maiores que os custos de desenvolvimento do próprio *software*.

Nesta seção (4.4.2.5) se descreve como foi o processo de análise dos fontes, sendo que a compilação é analisada nas duas seções seguintes (4.4.2.6, p. 109, e 4.4.2.7, p. 111).

Os testes exaustivos dos programas executáveis não foram desenvolvidos por absoluta falta de recursos e de tempo dentro do presente processo de auditoria.

4.4.2.5.1. A obtenção dos dados

O primeiro passo da atividade consistia em conferir se todos os códigos-fontes e executáveis carregados das urnas eletrônicas estavam de fato gravados no DVD produzido na Cerimônia de Lacração dos Sistemas que ocorreu no dia 04.09.2014 no TSE.

Os auditores puderam acompanhar a retirada do DVD do cofre do TSE e puderam conferir suas próprias assinaturas manuais nos lacres da embalagem.

Posteriormente, os códigos-fontes foram copiados para dez computadores oferecidos pela STI para uso dos auditores. Porém, logo se constatou que entre os programas-fonte disponibilizados não estavam presentes:

a) As bibliotecas de segurança desenvolvida pelo CEPESC/ABIN;
b) O BIOS (*Basic Input e Output System*) desenvolvido pela Diebold, fabricante das urnas;
c) O *firmware* ("*firm software*") gravado no circuito MSD de segurança e desenvolvido pela Diebold.

Foi, então, solicitada a disponibilização desses programas-fonte e foram feitos vários pedidos de esclarecimentos sobre esses sistemas.

Os códigos-fonte do CEPESC/ABIN foram instalados no dia seguinte pelos seus próprios funcionários, mas os fontes do BIOS e do MSD não foram apresentados sob alegação de que esses elementos de *software* seriam parte do *hardware* e não do *software* da urna (?!), estando, segundo a concepção da STI, fora do pedido inicial aprovado.

Devido à sua importância, descreve-se a seguir a influência desses três itens na segurança geral das urnas eletrônicas.

4.4.2.5.2. Autenticidade do código do CEPESC/ABIN

O motivo original que levou o TSE, desde 1996, a usar as rotinas de criptografia desenvolvidas pelo CEPESC/ABIN, era encriptar[84] (camuflar) o conteúdo do BU que seria transmitido para a totalização.

No entanto, esse é um procedimento desnecessário uma vez que o BU é um documento público por lei, sendo considerado crime não entregar cópias abertas deles aos fiscais dos partidos imediatamente após o encerramento da votação, que ocorre antes da transmissão dos resultados.

A rigor, para efeito da segurança da transmissão, o BU só precisa ser assinado digitalmente[85] para que se possa garantir a sua integridade e autenticidade no ponto de sua recepção pelo sistema de totalização.

A STI alegou, em sua resposta ao Pedido 44, o seguinte:

> *O arquivo de resultado da votação (Boletim de Urna) é criptografado e assinado digitalmente e, em especial, a criptografia do Boletim de Urna tem o objetivo de impor uma bar-*

84 *Criptografia* ou cifração é uma técnica destinada a garantir a **confidencialidade** de um documento que se quer manter secreto.

85 *Assinatura Digital* é uma técnica destinada a garantir a **integridade e a autenticidade** de um documento digital, seja ele público ou secreto. A técnica que o TSE utiliza para assinatura digital é denominada ECDSA (curvas elípticas) que tem todo o seu código e sua documentação públicos e abertos.

> *reira de segurança adicional sobre o arquivo que é utilizado para a totalização dos resultados. De fato, o resultado no Boletim de Urna é público desde a sua impressão pela urna.*

O argumento de que esta criptografia incrementa a segurança do BU é bastante questionável. Afinal, não se vislumbra como camuflar um dado que já foi tornado público tornaria mais seguro o processo de transmissão desse dado.

Além de encriptar algo que não precisava ser encriptado, segundo informação da STI na resposta ao Pedido de Esclarecimento 36, o *software* (biblioteca de criptografia simétrica) desenvolvido pelo CEPESC/ABIN, que é inserido (ligado) no *software* das urnas eletrônicas, é atualizado antes de cada eleição.

A resposta da STI não esclareceu o motivo dessa atualização a cada ciclo eleitoral já que, usando-se um bom algoritmo de criptografia, bastaria trocar a chave criptográfica a cada ciclo, o que poderia ser feito sem se recorrer a novos códigos “atualizados” do CEPESC/ABIN.

Ademais, o código-fonte referente à eleição de 2014 não estava gravado no DVD oficial do TSE, o que contraria o disposto no Art. 66 da Lei 9.504 e até mesmo o disposto na Resolução 23.397 do TSE[86].

Como consta da ata da cerimônia de análise dos códigos-fonte, os agentes da ABIN tiveram que comparecer ao TSE para instalarem o que seria, em tese, o código-fonte das suas bibliotecas dos aplicativos usados em 2014 (mas não instalaram as do circuito MSD), demonstrando que era incorreta a afirmação do setor SEVIN/STI na resposta ao Pedido de Esclarecimento 35, onde se disse que:

> *A STI/TSE possui o código-fonte desenvolvido pelo CEPESC sob seu controle e responsabilidade.*

Durante a instalação, os agentes do CEPESC/ABIN alertaram que seu código-fonte não poderia ser compilado, sem dar maiores explicações do porquê.

86Resolução 23.397/1993, artigo 10: Os arquivos referentes aos programas-fonte, programas-executáveis, arquivos fixos dos sistemas, arquivos de assinatura digital, chaves públicas e resumos digitais dos sistemas e dos programas de assinatura e verificação apresentados pelas entidades e agremiações serão gravados em mídias não regraváveis.Parágrafo único. As mídias serão acondicionadas em invólucro lacrado, assinado por todos os presentes, e armazenadas em cofre próprio da Secretaria de Tecnologia da Informação do Tribunal Superior Eleitoral.

Não foi permitido aos auditores procederem uma recompilação desse código apresentado para se verificar se dele derivava, de fato, o código compilado gravado no DVD oficial.

Sob tal restrição, os auditores não tiveram como determinar a identidade e correspondência exata entre o código da ABIN apresentado para análise e o código de fato carregado nas urnas eletrônicas usadas em 2014.

Por outro lado, se podem questionar os riscos para a segurança dos eleitores e dos candidatos propiciados pela presença da ABIN, vinculada ao Poder Executivo, entre os fornecedores do *software* eleitoral, principalmente se for considerado que as rotinas fornecidas pela ABIN são:

a) **Desnecessárias** - já que são usadas para encriptar algo que não precisa ser encriptado;
b) **Desnecessariamente atualizadas a cada ciclo eleitoral** - já que, se de boa qualidade, bastaria trocar as chaves de criptografia;
c) **Secretas** - já que não são gravadas no DVD oficial e a autoridade eleitoral não permite verificar se as apresentadas para análise eram, de fato, as usadas na eleição.

4.4.2.5.3. O Conteúdo do BIOS

O BIOS (*Basic Input e Output System*) é um dos *softwares* embarcados (*firmware*) presentes nas urnas eletrônicas mais importante no que diz respeito à segurança do sistema.

O aspecto crítico advém do fato que importantes inicializações do equipamento são feitas por meio do BIOS e, com isso, ele se torna um ponto de ataque para a inserção de *malware*[87] ou exploração de vulnerabilidades, como as seguintes possibilidades:

a) instalação de "*portas-dos-fundos*" para serem exploradas em ataques futuros que tentem burlar a segurança interna dos programas aplicativos;
b) em certas situações basta existir uma falha, mesmo não proposital, no BIOS para que ela seja explorada por uma eventual fraude;
c) não basta assinar digitalmente o BIOS para se afirmar que ele é seguro. A assinatura apenas comprova que ele não foi alterado, quando é necessário auditá-lo e testá-lo em várias situações de exceção para comprovar se não apresenta vulnerabilidades;

87 *Malware*: trechos de códigos maliciosos inseridos em programas de computador.

d) qualquer memória não volátil do equipamento pode carregar instruções que podem ser executadas em uma eventual fraude, incluindo circuitos aparentemente inofensivos, como o relógio de tempo real.

Apesar do BIOS ser um potencial vetor de ataques, sua inserção na urna eletrônica não é feita de forma compatível com esta criticidade: o BIOS é originalmente desenvolvido pelo fabricante do chip que é soldado na placa-mãe, e depois é complementado e regravado pela empresa Diebold, fabricante das urnas, ainda na fábrica. O fornecedor do chip BIOS, o fornecedor das placas-mãe e também o fornecedor das urnas, (empresas estrangeiras) têm, portanto, amplo acesso a este componente do sistema.

Cabe notar que vulnerabilidades na BIOS, caso não sejam corrigidas a priori (i.e., antes que a mesma seja instalada no sistema), permitem ataques extremamente difíceis de detectar: afinal, o BIOS pode "enganar" o *software* inicializado posteriormente à sua própria execução (e.g., injetando código no sistema operacional ou em algum programa aplicativo)[88], como foi demonstrado no caso do *Ataque de Princeton*[89].

De fato, existem diversos casos na literatura especializada sobre vulnerabilidades relacionadas exatamente ao BIOS. Um dos mais notórios é provavelmente os *softwares* maliciosos criados pela NSA para infectar o BIOS de computadores (e.g., o "*DEITYBOUNCE*"[90]) e, assim, permitir espionagem em larga escala de forma indetectável mesmo pelos mais avançados antivírus.

Outro caso de exploração de sistemas no momento de sua inicialização que ganhou notoriedade recentemente é o *software* malicioso batizado de "*Thunderstrike*"[91], voltado a computadores da linha Mac: uma vulnerabilidade no sistema de *boot* permite alterar até mesmo as chaves de segurança utilizadas para garantir que apenas *softwares* assinados pelo fabricante sejam executados, permitindo burlar tais mecanismos sem o conhecimento do usuário.

---

88 Uma discussão interessante sobre este problema é feita em: **A. Sacco, A. Ortega**. *Persistent BIOS Infection*. CanSecWest'09, 2009. Disponível em https://cansecwest.com/csw09/csw09-sacco-ortega.pdf

89 *Ataque de Princeton*: vídeo ilustrativo em : http://www.youtube.com/watch?v=0AKR-Lo-700e relatório técnico em: http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06full.pdf

90 **D. Salihun**. "*NSA BIOS Backdoor a.k.a. God Mode Malware Part 1: DEITYBOUNCE*". InfoSec Institute, 2014. Disponível: http://resources.infosecinstitute.com/nsa-bios-backdoor-god-mode-malware-deitybounce/

91 **D. Goodin**. "*World's first (known) bootkit for OS X can permanently backdoor Macs. Ars Technica*": 2015. Disponível: http://arstechnica.com/security/2015/01/worlds-first-known-bootkit-for-os-x-can-permanently-backdoor-macs/

Estes e outros casos mostram que a segurança de qualquer sistema computacional, incluindo da urna eletrônica brasileira, depende criticamente da segurança do BIOS.

Infelizmente, entretanto, a autoridade eleitoral recusou apresentar os códigos do BIOS das urnas eletrônicas, como consta na resposta ao Pedido de Esclarecimento 27 porque a STI entende que *firmware* é parte do *hardware* e não do *software* (!?). O pedido foi encaminhado à Corte que o negou por não constar da petição inicial.

Sob essas restrições, as poucas informações obtidas foram insuficientes para qualquer avaliação da real segurança do BIOS das urnas eletrônicas usadas em 2014.

4.4.2.5.4. O Circuito de Segurança MSD

Os circuitos de segurança, denominados pelo TSE como MSD (*Master Secure Device*), SMT (*Secure Micro Terminal*) e SCK (*Secure Ciphered Keyboard*) foram introduzidos a partir das urnas de modelo 2009, para evitar possíveis ataques externos que foram identificados como viáveis na análise desenvolvida pela *Fundação de Apoio à Capacitação em Tecnologia da Informação* (FACTI) do Ministério de Ciência e Tecnologia, como revelado na cartilha *Por Dentro da Urna*[92] do TSE.

No restante do presente relatório, esses circuitos serão referidos apenas como MSD, pois este é o núcleo principal que foi criado para evitar o "*Ataque de Princeton*"[93], que adulterava a apuração dos votos explorando a possibilidade de regravar o conteúdo do BIOS nas urnas fabricada pela Diebold nos EUA.

Este tipo de dispositivo tem dois modos de atuação: (i) o modo ativo, usado durante a inicialização da urna para verificar que apenas *softwares* autorizados são colocados em execução; e (ii) o modo passivo, quando um aplicativo da urna acessa o dispositivo e solicita a execução de alguma tarefa (previamente nele programada).

Toda vez que alguma tarefa é solicitada ao dispositivo, ele funciona como uma "caixa preta", pois não se tem como controlar ou se ter certeza do que ele realmente está fazendo. Assim, na prática, é impossível auditar a eficácia desse tipo de dispositivo, a não ser que na sua implementação inicial se tenha deixado outro tipo de porta-

92 **Tribunal Superior Eleitoral** – *Por dentro da Urna*. - 2ª edição revista e atualizada – Brasília: TSE, 2010 – disponível em: http://www.justicaeleitoral.jus.br/arquivos/tse-cartilha-por-dentro-da-urna

93 *Ataque de Princeton*: vídeo ilustrativo em: http://www.youtube.com/watch?v=0AKR-Lo-700e relatório técnico em: http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06full.pdf

dos-fundos que permita acesso real ao seu conteúdo, o que seria uma gravíssima falha de segurança e contrário ao próprio conceito que levou à sua concepção.

Uma análise mais profunda da arquitetura e dos procedimentos de carga do *firmware* do MSD revela a possibilidade de fraudes quase impossíveis de serem eliminadas pelo TSE, pois a mesma tecnologia usada para proteger o sistema impedindo a gravação de *malware* no BIOS, poderia ser usada para esconder um código malicioso, impedindo a sua eliminação do *firmware* do MSD.

Os possíveis riscos de segurança identificados como consequentes da implementação dos circuitos MSD são os seguintes:

a) A carga inicial do *software* (*firmware*) nos dispositivos MSD é um momento extremamente crítico, pois, nesse nele, o próprio dispositivo não tem como verificar a real procedência deste *firmware;*
b) Uma eventual "*porta-dos-fundos*"[94], colocada nesta primeira carga, poderia continuar presente indefinidamente, mesmo se o *firmware* for atualizado para novas versões e ainda que se utilize algum tipo de "*secure download*"[95], pois será o próprio *firmware* corrente, afetado por tal vulnerabilidade, que interpretará e implementará o novo código a ser gravado;
c) Uma fraude nesse *firmware* seria de muito difícil detecção, pois, conforme afirmado anteriormente, a mesma tecnologia utilizada para proteger o sistema, poderia simplesmente esconder a fraude;
d) As únicas ações reais de segurança nesse dispositivo, durante o "*secure download*", seriam verificar a integridade do novo código e a autenticidade de sua origem. Caso tenha sido inserido, por exemplo, um certificado adicional no dispositivo além do certificado legítimo do TSE, quem conhecer essa vulnerabilidade poderia instalar o novo *software* que assuma o controle do dispositivo durante todo o período em que a urna estiver ligada;
e) Se um eventual fraudador tiver como assumir o controle do dispositivo, ou na carga inicial ou durante qualquer atualização do *firmware*, ele não estará limitado a fraudar uma eleição apenas, mas sim todas as eleições nas quais urnas com o referido *firmware* estiverem em uso.

94 Nesse caso específico, uma *porta-dos-fundos* poderia ser a inclusão de um certificado de assinatura digital adicional, além dos certificados do próprio TSE.

95 *Secure Download* é o nome dado pelo TSE ao código responsável por carregar um novo *firmware* no circuito de segurança MSD das urnas de modelo 2009 em diante. Trata-se de um ponto crítico do processo de segurança e faz parte dos aplicativos SCAUE-C e SCAUE-A usados nos TRE´s quando da recepção de novas urnas.

Apesar deste também ser um componente crítico da segurança da urna eletrônica, a autoridade eleitoral se recusou a apresentar o código-fonte e o código compilado do *firmware* dos circuitos de segurança para análise dos auditores sob a alegação que não constavam do pedido inicial.

Ainda mais grave, a STI demonstrou que não tem domínio do *firmware* do MSD, pois declarou, em sua Informação nº 69 ASPLAN/STI de 08.05.2015, que necessitaria de 15 dias para preparar uma eventual apresentação desse código porque *"faz-se necessário convidar o fabricante das urnas eletrônicas para explanar sobre os elementos dos softwares embarcado em hardware"*.

A Resposta à Petição 23 demonstrou que o "*desenvolvimento e compilação do firmware do MSD são realizados pela Contratada para fabricação das urnas*". No caso, esse trecho refere-se à empresa Diebold.

Já a Resposta à Petição 24 revelou que os procedimentos de segurança usados pelo TSE se restringem apenas à assinatura do *firmware* do MSD antes da fabricação de todas as unidades de um modelo. Não foi descrita a existência de quaisquer procedimentos de verificação e validação do *firmware* após entrega das urnas, nem após as eleições terem sido realizadas.

Assim, não se identificou, no andamento do processo eleitoral, qualquer auditoria interna do TSE que seja desenvolvida com relação ao estado desse *firmware* antes e depois da eleição; se for realmente este o caso, essa ausência de controle vai contra o próprio conceito de assinatura digital de *software* (por definição, um voto de confiança de que aquele *software* opera corretamente).

Embora testes "exaustivos" possam mostrar que as funcionalidades do MSD estejam eventualmente condizentes com os requisitos funcionais estabelecidos, não há garantia de que o *firmware* do MSD não esteja realizando alguma funcionalidade oculta e em desacordo com as diretrizes do TSE.

Em resumo, a tecnologia usada no circuito de segurança MSD pode tanto servir para dificultar a gravação de *malware* no BIOS, como para esconder eventual *malware* nele gravado.

4.4.2.5.5. Revelações iniciais da Análise do Software

Independente da análise do código propriamente dita, as repostas obtidas da STI/TSE, no ambiente de análise do *software*, revelaram o seguinte:

a) Contrariando o disposto nos §§ 1º e 2º do Art. 66 da Lei 9.504, parte dos programas fontes e executáveis usados nas urnas eletrônicas não estavam gravados no DVD oficial da eleição de 2014;
b) As urnas fabricadas até 2008 (25% do usado em 2014) permitiam modificação livre do conteúdo do BIOS. Essa característica tem um lado positivo anti-fraude, pois possibilita ao TSE eliminar qualquer eventual "*porta-dos-fundos*" nela inserida pelo fabricante, supondo-se que uma auditoria fosse realizada pelo TSE para este fim.

Tem-se como lado negativo a vulnerabilidade do sistema a ataques de implantação de *malware* na BIOS, como demonstrado no "A*taque de Princeton"* pela equipe do professor Alex Halderman:

a) As urnas fabricadas a partir de 2009 (75% do usado em 2014) possuem circuitos adicionais "*de segurança*", genericamente denominado MSD, que, por um lado, tenta evitar o "A*taque de Princeton*" direto no BIOS, mas, por outro lado, abre oportunidade para o fabricante, ao menos em tese, plantar *portas-dos-fundos*[96] permanentes no seu *firmware*;
b) Além do fabricante, Diebold, também têm acesso ao conteúdo do *firmware* do circuito de segurança MSD os funcionários do CEPESC/ABIN (pelo desenvolvimento de parte do *software*) e os funcionários das empresas terceirizadas contratadas para auxílio no manuseio das urnas eletrônicas nos TRE's, como a Smartmatic[97], por exemplo;
c) O TSE não tem posse do código-fonte das bibliotecas de criptografia desenvolvidas pelo CEPESC/ABIN, que são ligadas (incluídas) aos programas aplicativos de votação e de gerenciamento das urnas, bem como das que são gravadas no *firmware* dos circuitos de segurança MSD;

96 Um exemplo simples de porta-dos-fundos que o fabricante das urnas poderia incluir no circuito MSD seria um segundo certificado raiz para verificação de assinaturas, além do certificado que o TSE solicita que seja gravado.

97 O contrato 80/2012 entre a Smartmatic e o TSE em 2012 previa, entre outros, o seguinte serviço a ser prestado:"f) procedimentos de atualização de *software* embarcado e certificação digital nas urnas de modelos a partir de 2009". Esse serviço descrito no item f) do contrato TSE/Smartmatic é exatamente a carga do *firmware* no circuito MSD das urnas eletrônicas de modelo 2009 em diante, que seria feito com a participação de funcionários da Smarmatic e sem a presença dos Partidos Políticos ou do MP (o que contraria o disposto no Art, 66 da Lei 9.504).

d) O TSE evidenciou não ter domínio técnico sobre o código-fonte do *firmware* incluído no BIOS e no circuito MSD, pois a STI declarou, em sua Informação nº 69 ASPLAN/STI de 08.05.2015, que necessitaria de 15 dias para preparar a apresentação desse código porque *"faz-se necessário convidar o fabricante das urnas eletrônicas para explanar sobre os elementos dos softwares embarcado em hardware"*;
e) No processo de desenvolvimento do sistema da urna, não há auditoria interna do TSE com relação ao estado do *firmware do MSD* antes e depois da eleição;
f) As chaves de segurança que permitem a verificação da integridade do *software* estão gravadas (*hardcoded*) no próprio código compilado, causando uma falha de segurança, pois um *software* malicioso poderia, ao menos em tese, obter essas chaves para assinar arquivos de resultado falsos como se os mesmos fossem gerados por urnas legítimas.

A comprovação dessa vulnerabilidade foi verificada não apenas na análise dos códigos-fonte, mas também foi declarada na resposta ao pedido de esclarecimento 33, onde, para justificar a recusa de apresentação dos códigos compilados, foi dito que *"as chaves de assinatura e de criptografia de arquivos poderiam ser extraídas do binário..."*.

4.4.2.5.6. O volume dos Dados

Os códigos-fonte disponibilizados, ainda que incompletos, compunham mais de 50 mil arquivos com mais de 17 milhões de linhas de código.

A limitação de tempo (apenas 9 dias úteis na prática) e de recursos pessoais (apenas 10 analistas pré-aprovados e 6 disponíveis na prática), implicaria em uma tarefa impossível de cada analista avaliar e compreender a interconexão de mais de 11 linhas de código por segundo, sem parar em um só momento durante o prazo disponível.

Por esse motivo, os auditores tiveram que restringir suas análises a trechos do código que consideraram mais importantes ou críticos. Sob essa condição, não há como afirmar que o código-fonte do sistema eleitoral brasileiro, na sua totalidade, está livre de erros que possam afetar o registro e apuração correta dos votos.

Essa dimensão revela, na prática, que a validação do *software* eleitoral do TSE chega a ser inviável sob condições razoáveis de recursos e custos.

4.4.2.5.7. O ambiente operacional de análise

A avaliação dos códigos permitida se restringia a apenas uma análise estática do código-fonte por meio de sua leitura com auxílio de alguma ferramenta de análise, não sendo permitido desenvolver análise dinâmica do *software* (como a inserção de *breakpoints* e execução controlada de trechos do código para entender seu funcionamento detalhado), resultando numa limitação de recursos totalmente incompatível com uma validação de nível forense.

Uma dificuldade adicional aos trabalhos da auditoria foi a recusa da STI de instalar uma ferramenta de análise de código mais robusta e rápida que a disponível.

Na petição inicial, foi solicitada a instalação da ferramenta de análise denominada *Eclipse* porque esta é normalmente usada e disponibilizada pela STI. Porém, logo no início dos trabalhos a ferramenta se revelou insuficiente para acessar e indexar a totalidade do código, principalmente por funcionar dentro de um sub-ambiente JAVA. Cada tentativa de localizar um outro trecho do código podia demorar algumas dezenas de minutos para se completar.

Como consta na ata da cerimônia, o primeiro dia foi perdido na tentativa de obter uma configuração de melhor desempenho do *Eclipse*. Embora tenha havido alguma melhora, os analistas optaram por solicitar a instalação do sistema *Visual Studio* ou do *Visual C++*, que proveem melhor eficiência para analisar sistemas complexos e grandes (e.g., facilidade de indexação de código).

Porém, a STI decidiu unilateralmente negar a instalação dessa outra ferramenta, alegando o seguinte:

> *Resposta ao ped. 8 – "Na petição de Protocolo TSE Nº 4.455/2015, juntado ao processo judicial Petição Nº 1855-20.2014.6.00.0000, o requerente listou as ferramentas que desejava instaladas no ambiente de apresentação do código-fonte. No pedido original não constava o software Visual Studio, mas tão somente o Eclipse, que foi devidamente instalado e configurado em todos os equipamentos à disposição dos técnicos. A STI/TSE entende que o Eclipse já instalado é ferramenta suficiente para a análise pretendida, porque possui todas as funcionalidades necessárias, além de tratar-se da ferramenta utilizada pela STI/TSE no ambiente de desenvolvimento do software que está sendo inspecionado.*

Em resumo, a STI ignorou as dificuldades operacionais enfrentadas pelos analistas, alegou que sua equipe utilizava o *Eclipse* e negou a facilidade solicitada por alegada preclusão, porque não constava do pedido inicial, mesmo que os auditores só tenham podido constatar as limitações do *Eclipse* frente ao tamanho e à complexa intercorrelação de módulos do código sob análise, depois de iniciados os trabalhos.

4.4.2.5.8. Análise do Código-fonte Disponível

A análise do código disponibilizado ocorreu entre os dias 04 e 15 de maio de 2015 (dez dias úteis), em ambiente controlado nas dependências do TSE.

Os analistas tiveram que ser pré-aprovados pelo TSE, tendo sido recusada a inscrição do professor Alex Halderman[98] e do analista de segurança Rodrigo Branco[99], por alegado risco à soberania nacional[100]. Um pedido de reconsideração dessa recusa não foi respondido até o final dos trabalhos da análise.

Uma parte da análise consistiu na execução do programa de verificação estática de código *CppCheck*, em busca de vulnerabilidades e pontos de atenção. Tal execução apontou mais de 1000 trechos identificados como erros (i.e., problemas considerados graves pelo programa de análise) e mais de 2000 alertas (i.e., sugestões relativas a técnicas de programação defensiva, que podem evitar falhas).

Embora não tenha havido tempo hábil para verificar todos os potenciais problemas apontados pelo *CppCheck*, foi identificada ao menos uma vulnerabilidade bastante grave em um dos códigos-fonte fornecidos: o módulo denominado *secure_download*[101] pode ser explorado por meio de um estouro de buffer ("*buffer overflow*"), o que permitiria a execução de código arbitrário por qualquer pessoa utilizando o referido módulo (burlando qualquer salvaguarda estabelecida, inclusive eventuais assinaturas digitais).

---

98 Alex Halderman é Professor Associado em Ciência da Computação na University of Michigan e diretor do Center for Computer Security and Society. Tem grande experiência bem-sucedida em demonstrar a fragilidade de sistemas eleitorais eletrônicos, já tendo vencido as barreiras de segurança de mais de 10 equipamentos e sistemas eleitorais norte-americanos (da Diebold, similares às urnas brasileiras), da Holanda, da Índia e da Estônia (voto pela Internet).

99 Rodrigo Branco, brasileiro, é engenheiro do ITA com larga especialização em segurança de dados. Ocupa o cargo de *Principal Security Researcher* na Intel Corporation.

100 Conforme decisão do Presidente do TSE, Ministro Dias Toffoli, nos autos da Petição nº 1855-20, na data de 06 de abril de 2015.

101 *Secure Download* é o nome dado pelo TSE ao código responsável por conferir e carregar um novo *firmware* no circuito de segurança MSD das urnas de modelo 2009 em diante. Trata-se de um ponto crítico do processo de segurança e faz parte dos aplicativos SCAUE-C e SCAUE-A usados nos TRE´s quando da recepção de novas urnas.

A presença de tal tipo de vulnerabilidade por si só é considerada grave pelo fato da mesma figurar como o terceiro erro de *software* mais perigoso na lista CWE/SANS de 2011[102].

Este fato, combinado com o grande número de alertas menos graves gerados pela ferramenta *CppCheck*, leva a sérias dúvidas se o processo de desenvolvimento de *software* sendo utilizado para a urna eletrônica brasileira de fato segue boas práticas de segurança para criação de *software* de missão crítica, o que inclui processo de análise estática do código e eliminação de pontos levantados pela ferramenta utilizada.

De fato, a recomendação para execução de tal análise aparece no relatório do Prof. Diego Aranha em 2013[103], na seção "*4.2.3 Ausência de análise estática de código*", até mesmo porque procedimentos deste tipo detectariam a "*família de funções vulnerável utilizada para embaralhamento dos votos*", principal falha apontada no referido relatório.

Para entender a utilização de tais ferramentas no processo de desenvolvimento do código da urna, foi feito o seguinte pedido de esclarecimento durante o processo de auditoria:

> *Pedido de Esclarecimento 43 – "Solicitamos esclarecer se o STI/TSE utiliza alguma ferramenta de análise estática de código fonte, tal como o "CppCheck". Em caso afirmativo, esclarecer adicionalmente como são gerenciadas pelo STI os potenciais problemas evidenciados por este tipo de análise"*

A resposta obtida foi:

> *Resposta ao Pedido de Esclarecimento 43 – "A STI/TSE utiliza a ferramenta "CppCheck" nos projetos codificados em C++. A ferramenta faz parte do processo de integração contínua do software. Os alertas gerados são avaliados e, caso sejam pertinentes, tratados"*

102 A lista CWE/SANS é o resultado da colaboração entre o SANS Institute, MITRE, e vários experts em segurança de *software* nos Estados Unidos e Europa. A lista atualizada pode ser encontrada em http://cwe.mitre.org/top25/

103 **D. Aranha, M. Karam, A. Miranda, F. Scarel** (2013). "*Vulnerabilidades no software da urna eletrônica brasileira* - v. 1.0.2" – 2012. Disponível vem: https://archive.org/stream/vulnerabilidades_urna_eletronica_brasileira/relatorio-urna_djvu.txt

Embora tal resposta seja aparentemente alentadora, pois indica que a recomendação feita no mencionado relatório de 2013 foi acatada, ela gera preocupações sobre o que a STI/TSE considera “pertinente”, por pelo menos dois motivos.

O primeiro é que ignorar um dos erros de *software* listados entre os mais perigosos, quando a solução para o mesmo não é tecnicamente difícil ou trabalhosa (e.g., bastaria trocar um comando “*strcpy*” por outro equivalente, como “*strlcpy*”), é, no mínimo, temerário.

O segundo é que o grande volume de alertas que não foram considerados suficientemente pertinentes para serem tratados provavelmente dificultaria a própria análise dos desenvolvedores durante o “*processo de integração contínua do software*”, pois leva a relatórios um tanto poluídos por parte da ferramenta de análise estática.

Cabe notar que tal poluição de informações pode ser tratada com filtros configurados na própria ferramenta, os quais impediriam que alguns alertas fossem gerados. Entretanto, como tal abordagem melhoraria a capacidade de gerenciamento de alertas ao custo de uma menor visibilidade das potenciais vulnerabilidades existentes, seria mais adequado solucionar o problema apontado pela ferramenta de análise com a correção do próprio *software* sendo analisado, ao invés de configurar a ferramenta para ignorá-lo.

Assim, a recomendação dada com relação a esse ponto é que ferramentas de análise estática como o *CppCheck* e outras adicionais continuem sendo utilizadas, mas que todos os pontos por elas apontados sejam devidamente tratados no sentido de garantir a quantidade de erros/alertas gerados seja mínima ou nula.

Além do código-fonte da urna em si, é importante considerar também o sistema operacional sobre o qual o sistema é executado. Especificamente para as urnas eletrônicas, o TSE optou por utilizar o sistema operacional de *software* livre Linux com algumas adaptações. O Linux foi congelado na versão 2.6.16.62 de 2009.

Por ser esta uma versão antiga, várias atualizações[104] e implementações de segurança, feitas pelo projeto Linux ao longo dos últimos 6 anos, ficaram de fora da versão congelada pelo TSE.

Desconsiderar essas atualizações pode trazer consequências graves. Afinal, um *software*, por ter código aberto, não é automaticamente “seguro” ou “confiável”, pois todo o processo de verificação de sua qualidade depende da efetiva colaboração da comunidade de desenvolvedores (e, idealmente, utilizadores) no sentido de revisá-lo e

104 Atualmente, já está testada e disponível ao menos a versão 3.16.0.41 do *Kernel* do Linux.

evitar a introdução de falhas propositais ou não-intencionais, estando essas análises dentre as fontes de atualizações periódicas.

Há casos reportados de *softwares* de código aberto amplamente utilizados que apresentavam falhas graves de segurança. Por exemplo, em 2014, descobriu-se que um *software* amplamente utilizado para estabelecimento de conexões seguras com servidores web, o *OpenSSL*, apresentava uma séria falha, permitindo o roubo de informações secretas usadas para proteger essas comunicações[105]. Apesar de grave, o problema permaneceu desapercebido desde sua introdução por um programador voluntário em 2011, provavelmente devido à relativa simplicidade do erro.

Ainda pior, existem casos relatados na prática de alterações feitas em *softwares* abertos ou ataques a repositórios desses *softwares* com o propósito específico de introduzir portas dos fundos que, embora não facilmente detectáveis pelos membros da comunidade de desenvolvedores, poderiam ser facilmente exploradas pelo usuário responsável pela alteração realizada.

Exemplos conhecidos incluem: a tentativa (aparentemente fracassada) de introdução de uma sutil porta dos fundos no Linux em 2003[106]; e o caso de 2012 da efetiva introdução de uma porta dos fundos em um dos repositórios do *software* de código aberto *phpMyAdmin* (usado para gerenciamento de bancos de dados) [107].

Ademais, mesmo se fosse possível assumir que a versão do Linux congelada esteja completamente livre de vulnerabilidades, alterações no *kernel*[108], em *device-drivers*[109] e em utilitários do sistema operacional têm sido feitas pelo TSE e seus fornecedores[110].

Tais alterações potencialmente abrem espaço para brechas de segurança, especialmente considerando que mesmo as maiores empresas que desenvolvem sistemas operacionais no mundo, como Microsoft, Apple e Google, não conseguem testar sozi-

105 Heartbleed. http://heartbleed.com/

106 **K. Poulsen**."*Thwarted Linux backdoor hints at smarter hacks*". SecurityFocus - 2003. Disponível em: http://www.securityfocus.com/news/7388

107 **D. Goodin.** "*Questions abound as malicious phpMyAdmin backdoor found on SourceForge site*". ArsTechnica - 2012. Disponível em: http://arstechnica.com/security/2012/09/questions-abound-as-malicious-phpmyadmin-backdoor-found-on-sourceforge-site/

108 *Kernel* é o nome dado ao núcleo do *software* do sistema operacional Linux.

109 *Device-driver* é o nome dado a trechos do *software* do sistema operacional, encarregados de fazer a interface entre o *Kernel* e os diversos equipamentos instalados, como o teclado, monitores, impressoras, leitoras de digitais, etc.

110 Nesse caso, está-se referindo a Diebold, fornecedora dos *device-drivers* das urnas eletrônicas que produz.

nhas as alterações que elas fazem em seus sistemas. Dependem de "*testadores alfa*", de "*testadores beta*" e de milhões de utilizadores que experimentam seus sistemas operacionais e reportam eventuais falhas. É graças a esse processo de intensos testes que, com grande frequência, estas empresas lançam correções de segurança para problemas encontrados.

O Linux conta com uma comunidade enorme, que frequentemente analisa os códigos fontes, em busca de possíveis falhas, e também conta com milhões de usuários reportando problemas diariamente.

Ao adotar um sistema aberto (Linux) transformado em sistema fechado (que denomina UEnux), o administrador eleitoral coloca-se em uma situação crítica relativa à confiabilidade do *software* que produz: usa um *software* livre, mas de maneira fechada; de modo que não possui uma rede de milhões de usuários para testar a funcionalidade das alterações que faz, nem possui um grupo externo de testadores alfa e beta.

Assim, o UEnux do TSE combina os problemas do "*software livre*" (diversos desenvolvedores, com níveis de experiência e idoneidade distintos) com os problemas dos "*softwares proprietários*" (base reduzida de testadores), sem as principais vantagens de cada um desses dois paradigmas de desenvolvimento. Ou seja, se torna questionável a eficiência do TSE em realmente testar o sistema operacional que desenvolve para as urnas eletrônicas brasileiras.

Apesar da importância de se verificar esses aspectos, a análise das alterações feitas no Linux original ficou comprometida pelo pouco tempo disponível e, principalmente, pelas restrições impostas contra a análise dinâmica do *software*.

Foram observados alguns pontos críticos, que mereciam maior atenção e uma análise especifica das implicações das alterações, por exemplo:

a) Não foi encontrada a verificação de integridade do *loader*[111] do Linux pelos *loaders* anteriores. Caso isso se confirme, pode configurar uma gravíssima falha de segurança[112];

111 *Loader* é o nome dado a um trecho do *software* básico responsável por carregar na memória operacional o próximo sistema a ser executado. Costuma haver um grupo de *loaders* que carregam, em sequência, o código BIOS, os códigos adicionais de segurança, o sistema operacional e, finalmente, os *device-drivers* e demais configurações de iniciação.

112 Muitos dos *malwares* mais nocivos, que conseguem evitar sua eliminação posterior, costumam disputar por assumir o controle do sistema operacional justamente nessa fase de carga dos *loaders*.

b) A implementação da criptografia do sistema de arquivos (*file system*[113]) é simples, feita em bloco, setor a setor. Os locais no código compilado onde é feita a cifração e decifração estão sempre associados a chamadas de leitura e escrita de setores, ficando muito fácil localizá-los para efetuar um ataque que localize e identifique a chave de segurança. Salvo melhor análise, a criptografia do sistema de arquivos é passível de ser quebrada;
c) A verificação do *hash* do sistema operacional está implementada de forma que facilita a sua localização no código compilado do seu *loader* (carregador do código). Por ser um trecho de código pequeno e simples de ser entendido, fica fácil encontrar o valor do *hash* a ser verificado para burlar a verificação. Ou seja, essa verificação se caracteriza mais como uma verificação contra falhas (segurança no sentido de *safety*) do que um procedimento de segurança em contra ataques intencionais (segurança no sentido de *security*);
d) O código dos aplicativos não possui qualquer defesa contra engenharia reversa[114]. Assim, a verificação da assinatura digital na carga de cada aplicativo fica localizada em um ponto do código compilado que não é de difícil remoção para quem a ele tenha acesso. Consequentemente, a cadeia de certificação, bem como a própria assinatura digital, pode ser atacada;
e) Verificou-se a existência de várias ferramentas e utilitários de desenvolvimento e de depuração, que possibilitam a suspensão ou desvio de elementos de proteção do sistema. Não houve oportunidade para se verificar como seu uso é controlado e se poderiam ter sido usados em uma quebra de segurança. Eles podem ser comparados às "*portas-do-fundo*" durante o processo de produção do *software*;
f) O conjunto dos programas tem uma complexidade muito grande, o que afeta sua confiabilidade. Quanto mais complexo um *software*, maiores as chances de erros e vulnerabilidades e maior facilidade em se esconder algum trecho de código malicioso.

No entanto, com as condições restritas de trabalho (pouco tempo e somente análise estática) o TSE não possibilitou desenvolver uma análise mais elaborada e conclusiva sobre essas potenciais vulnerabilidades encontradas.

113 *File System* é o nome dado a uma camada do *software* básico encarregada da interface entre os programas que querem ler ou gravar dados e arquivos nos dispositivos de memória não-volatil.

114 *Engenharia reversa* ou *"desassembler"* são as técnicas de análise dos códigos compilados para descobrir sua funcionalidade e eventuais vulnerabilidades resultantes do processo de compilação e que não se encontra nos códigos-fonte.

4.4.2.5.9. Conclusões da Análise dos Fontes

Devido às restrições impostas e acima descritas, os auditores consideram que a validação do *software* usado nas urnas eletrônicas em 2014 foi totalmente prejudicada, tornando-se impossível fazer qualquer afirmação sobre seu funcionamento correto e idôneo.

Por outro lado, mesmo com as restrições enfrentadas, conseguiu-se verificar a existência de diversas vulnerabilidades que poderiam ser exploradas, ao menos em tese, em ataques externos e internos ao *software* original que resultassem em distorção na apuração da verdade eleitoral, não tendo sido possível confirmar ou refutar se as mesmas foram exploradas nas eleições presidenciais de 2014.

A análise estática do código revelou inúmeras ocorrências de alertas e até erros não tratados.

A ausência do código do BIOS e do MSD não permitiu se verificar se é efetiva a alegada defesa contra o "A*taque de Princeton*" e nem se ela impede, de fato, a existência de "*portas-dos-fundos*".

Não foi permitido determinar se o código-fonte apresentado pelo CEPESC/ABIN era o mesmo que, depois de compilado, foi incluído no *software* usado nas urnas eletrônicas.

Verificou-se que pessoas externas ao TSE, como os funcionários da ABIN, da empresa Diebold, da empresa Módulo e das empresas contratadas pelos TRE´s para "*exercitação das urnas*" (dentre as quais se inclui a empresa Smartmatic) têm momentos de acesso ao *software* instalado em pontos críticos das urnas (BIOS e MSD) e nos sistemas de preparação e geração de mídias, podendo, ao menos em tese, inserir "*portas-dos-fundos*" para posterior exploração.

O mesmo ocorre com relação a uma vasta gama de funcionários da própria STI/TSE que têm acesso a pontos críticos do sistema, como a posse de chaves de verificação, a compilação dos códigos e aos próprios códigos compilados.

Esse risco de ataque interno ao *software* é enormemente agravado por dois motivos interconectados:

a) o modelo de máquinas de votar adotado pelo TSE é essencialmente DEPENDENTE da segurança do *software*, impossibilitando qualquer auditoria do resultado por meio independente do próprio *software*;

b) A auditoria (validação) externa do *software* fica totalmente impossibilitada pelas restrições impostas pela própria STI/TSE.

Nesses termos, com a impossibilidade de se conferir o registro e a contagem dos votos em cada urna eletrônica devido a inexistência do VVPAT ou voto impresso conferível pelo eleitor, e com as restrições encontradas para validação segura do *software* usado nessas urnas, considera-se impossível determinar a integridade do *software* usado e, por consequência, se foram justos o registro e a apuração dos votos nas urnas eletrônicas no 2º turno da eleição de 2014.

4.4.2.6. Análise dos Compiladores

Atividade prevista no PTI: analisar os programas compiladores utilizados quanto a sua autenticidade e integridade

A análise da autenticidade e integridade dos programas compiladores usados na confecção do *software* eleitoral final se faz necessária porque o momento da compilação é uma porta para a inserção de *malware* que venha permitir eventuais fraudes no registro e apuração dos votos.

Essa possibilidade de inserção de *malware* via programa compiladores é bem documentada na literatura acadêmica há décadas[115], onde se descreve como se pode adulterar programas compiladores, ou suas bibliotecas, para inserir brechas para ataque externo (*porta-dos-fundos*) ou funcionalidades extras escondidas (*ovos-de-páscoa*) nos programas neles compilados.

Por esta razão, a verificação da integridade do compilador é uma tarefa dada como necessária para se atingir os mais altos níveis de garantia de confiança especificados em normas internacionais de desenvolvimento de *software* seguro, como é o caso do ISO/IEC 15408 – *"Common Criteria"*.

Segundo informação da STI na resposta ao Pedido de Esclarecimento 17, foi usado o compilador GNU GCC - versão 4.7.2, de código aberto, o que viabiliza totalmente o ataque descrito na literatura já citada acima. Um atacante interno poderia, ao me-

115 Thompson, K. - *Reflections on Trusting Trust* : USA, Communications of the ACM, Volume 27 Number 8, August 1984 - http://dl.acm.org/citation.cfm?id=358210&coll=ACM&dl=ACM

nos em tese, alterar o funcionamento do compilador, para inserir *malware* no código compilado, mesmo quando o código-fonte original esteja integro.

Agravando esse risco, foi dito na mesma resposta da STI que:

> *Não há políticas estabelecidas pela instituição (TSE) de auditoria sobre esses compiladores.*

Neste caso, perde-se a maior vantagem de se utilizar um compilador de código aberto, que é a capacidade de realizar-se uma inspeção profunda de seu conteúdo para garantir que não há potenciais brechas de segurança nos mesmos.

Sob essas circunstâncias, uma eventual fraude introduzida no compilador é de muito difícil detecção, e passaria despercebida, e até seria protegida, por todos os mecanismos de segurança que a STI adotou na produção do *software* eleitoral usado em 2014.

Dados estes exemplos contemporâneos e com a reconhecida inexistência de uma política da STI/TSE para a segurança dos compiladores, não é inconcebível que a urna eletrônica brasileira esteja sujeita a vulnerabilidades introduzidas nesses *softwares*, possibilidade que somente poderia ser descartada após uma efetiva análise e auditoria dos mesmos.

Apesar do exposto, não foi permitido aos auditores do PSDB ter acesso aos programas compiladores para verificar a integridade do compilador utilizado, sob a alegação de que esta seria uma atividade que extrapola o concedido na petição inicial.

Ademais, os compiladores alegadamente utilizados não foram gravados e lacrados junto aos códigos-fonte dos programas no DVD oficial. Com isso, também não seria possível a um auditor externo determinar qual realmente foi compilador utilizado e se nele havia alguma adulteração.

Em resumo, a falta de controle da STI sobre os compiladores utilizados caracteriza grande vulnerabilidade que poderia ser explorada por atacantes internos, sem deixar rastros que pudessem ser detectados em qualquer auditoria externa sobre o código-fonte original.

Dessa forma, todo o processo de produção do *software* eleitoral, independente da correção dos programas fontes, está vulnerável ao ataque via compilador. Se alguém internamente efetuar tal ataque, não seria detectado pelas rotinas de segurança do próprio TSE e nem pelos agentes externos que apenas possam assistir os traba-

lhos de compilação, como é o caso dos representantes do MP, da OAB e dos Partidos que comparecem às cerimônias oficiais no TSE.

Essa condição reforça a conclusão acima de que é impossível determinar se estava íntegro o *software* usado nas urnas durante o 2º turno de 2014.

4.4.2.7. Auditoria da Compilação

Atividade prevista no PTI: recompilar o software para fazer uma auditoria da compilação, comparando com os códigos executáveis gravados no mesmo DVD

A conferência dos programas executáveis faz parte dos procedimentos de validação do *software* e, no caso presente, consiste em verificar se os executáveis derivam dos programas-fonte analisados e aprovados e se são eles mesmos que foram gravados no DVD oficial.

Os procedimentos da compilação são de importância vital para a segurança do sistema: todo ambiente deveria ser auditado antes, durante e depois da compilação, por meio de técnicas de auditoria estática e também dinâmica da compilação.

Como exemplo, apresentam-se alguns modos de inserção de código malicioso que podem ser desenvolvidos durante a compilação:

a) Um "*vírus*" instalado no ambiente de compilação altera algum executável recém-gerado;
b) Algum *"script"* (roteiro de tarefas) é alterado exatamente antes do início da compilação, adulterando o processo que deveria ser realizado;
c) Algum *"path"* (localização) do sistema é alterado no início ou durante a compilação para que o compilador inclua bibliotecas (porções de código) incorretas no sistema;
d) Alguém, na rede local ou em algum lugar remoto, altera algum arquivo, logo antes, durante ou logo depois da compilação.

Pela regulamentação estabelecida pela autoridade eleitoral, os representantes dos Partidos, da OAB e do MP só podem acompanhar os procedimentos da compilação

oficial como observadores[116], o que não permite fazer qualquer verificação significativa e minimamente confiável do ambiente em que ocorre tal procedimento.

Na presente Auditoria Especial, o TSE negou acesso dos auditores do PSDB aos programas executáveis contidos no DVD oficial, mesmo estando a possibilidade de análise desses programas pelos partidos prevista no Art. 66 da Lei 9.504/1997 e no art. 5º da Res. TSE 23.39/2013.

Também foi negada permissão para se proceder a uma recompilação dos programas-fonte que pudesse demonstrar que os executáveis produzidos em setembro de 2014 de fato derivavam daqueles disponibilizados para análise.

O argumento apresentado pela STI para se recusar a apresentar os programas executáveis contidos no DVD foi o seguinte:

> *(resp. ao ped.33) Embora a lei e a resolução possibilitem a análise de programas-fonte e programas executáveis, há de registrar que os artigos citados fazem menção a um período que se encerra com a assinatura digital e lacração dos sistemas eleitorais...*
> *... Além disso, as chaves de assinatura e de criptografia de arquivos poderiam ser extraídas do binário e, considerando que os programas executáveis são oficiais, ou seja, ainda são utilizados nas eleições suplementares de 2012, por precaução, decidiu-se por não colocar disponíveis os binários, calcando para tanto, na decisão do presidente, de que procedimentos que extrapolassem a simples análise de códigos-fonte deveriam ser precedidos de plano de uso a ser aprovado pelo TSE"* (grifo nosso)

Destaque-se que:

a) Foi o Presidente do TSE que, acatando sugestão da STI, decidiu que a Res. TSE 23.397/13 seria aplicada aos procedimentos da auditoria especial do PSDB – com isso, a primeira parte do argumento da STI, de que a Resolução não se aplicaria a essa fase da auditoria, se mostra casuística e contraditória;

116 Em 2014, a cerimônia de compilação e lacração dos sistemas, de três dias de duração, só foi parcialmente acompanhada (observada) por representantes do PDT e do PC-do-B/MA, entre os quais um dos autores do presente relatório de auditoria. Os representantes da OAB e do MP compareceram apenas nos momentos finais da cerimônia, para assinarem os programas já compilados, sem terem acompanhado o processo de compilação propriamente dito.

b) A solicitação dos auditores se referia aos programas executáveis de 2014 e não aos executáveis de eleições municipais suplementares de 2012. Estes, embora presentes do DVD, não foram solicitados – com isso, a segunda parte do argumento da STI não se aplica;
c) O art. 66 da lei 9.504/97 e o art. 5º da Res. 23.397/13 não fazem menção à apresentação de planos de uso e nem que partidos devam se restringir a *"análise de códigos-fonte",* pelo contrário, faz explícita menção à análise dos programas executáveis – com isso, a terceira e última parte do argumento da STI não tem fundamento legal e revela autoritarismo e falta de transparência.

Como justificativa para não permitir a recompilação dos códigos-fonte, foi dito que as configurações adotadas no processo de compilação de 2014, não permitiam reproduzir os executáveis de maneira idêntica a partir dos mesmos códigos-fonte.

Foram infrutíferas as tentativas dos auditores, em uma reunião na STI no dia 06 de maio de 2015 e através do Pedido de Esclarecimentos 20, de se desenvolver alternativas de uma recompilação parcial e controlada que permitissem a verificação desejada. A resposta final da STI foi simplesmente que o pedido foi recusado pelo Ministro Presidente do TSE no dia 11 de maio de 2005, por ser considerado procedimento diferente dos autorizados anteriormente.

Constatou-se ainda, como agravante, que os procedimentos de compilação desenvolvidos pela STI/TSE não foram planejados para ser este um processo determinístico e que leve em conta a possibilidade de vir a ser auditado posteriormente.

Especificamente, as configurações, as variáveis gerais de compilação e os metacomandos escolhidos e utilizados não permitiam sua reprodução posterior sob auditoria, pois induzem a compilação a se comportar como um processo não-determinístico, gerando códigos executáveis com diferenças a cada compilação.

Mesmo se tivesse sido permitida a recompilação, isso dificultaria, ou mesmo inviabilizaria, gerar novamente os binários para se verificar se os executáveis que estão nas urnas (utilizadas em 2014) são realmente originados dos códigos-fontes apresentados.

Enfim, com os procedimentos de compilação adotados e sob as restrições impostas, tornou-se impossível se verificar se os executáveis lacrados no DVD oficial de 2014 derivaram mesmo dos código-fontes apresentados para análise.

Em especial, com relação ao código desenvolvido pela CEPESC/ABIN, a situação foi ainda mais obscura. Com a ausência dos códigos-fonte no DVD oficial, não se pôde

determinar, com certeza, nem mesmo se os códigos apresentados para avaliação dos auditores eram realmente os que estavam presentes nos equipamentos de compilação durante a Cerimônia Pública de Lacração.

4.4.2.8. Certificação do *Software* nas Urnas

Atividade prevista no PTI: ter acesso a uma amostra de urnas realmente usadas na eleição para comparação dos códigos executáveis encontrados com os esperados e também para efetuar testes emulando uma votação real, para verificar seu correto funcionamento

A etapa de certificação do *software* consiste em se verificar se o *software* executável carregado nas urnas no dia da eleição é idêntico ao *software* validado.

Normalmente é uma atividade simples de ser executada, pelo uso de recursos de assinatura digital e resumo criptográfico (*hash*)[117], mas que tem que enfrentar um universo de mais de 420 mil urnas espalhadas pelo país, a ser auditado.

Além dessa dificuldade natural do porte, a certificação do *software* não pôde ser desenvolvida pelos auditores de forma correta e confiável porque a autoridade eleitoral não permite a verificação direta das memórias das urnas para confirmar se o *software* nelas gravado contém a assinatura válida esperada.

Usar a própria urna eletrônica para, por via indireta, recalcular os *hashes* dos aplicativos nela gravados, como regulamenta a Res. 23.397/2013, não tem utilidade para auditoria. Isso ocorre porque, se a própria urna já tivesse detectado um erro no *hash*, ela se auto bloquearia e nem executaria o programa verificador de *hash*.

Na hipótese de algum código malicioso ter sido inserido com sucesso dentro do *software* da urna, ele também fraudaria o cálculo do *hash*, de maneira que não o recalcularia e sim simularia esse cálculo, mostrando os resultados já conhecidos.

117 Resumo criptográfico, ou "*hash*", é uma técnica para detectar adulterações num arquivo digital. Conceitualmente é similar aos dígitos verificadores do CPF: se for alterado qualquer número no documento digital, os dígitos verificadores ou *hash* também se alteram.

A verificação direta do conteúdo das mídias de memória das urnas pelos fiscais dos partidos, por outro lado, foi recomendada no Relatório Unicamp[118], de 2002, depois dos seus autores terem constatado, na sua seção 4.3, o seguinte:

> *... não há mecanismos simples e eficazes que permitam que representantes de algum partido, em qualquer lugar do país, possam confirmar que os programas usados na UE correspondem fielmente aos mesmos que foram lacrados e guardados no TSE, exceto através de uma auditoria*

Para contornar esse problema, os professores contratados pelo TSE em 2002 apresentaram a seguinte recomendação na seção 5.5 do seu relatório:

> *"5.5 Verificação, por representantes partidários, dos resumos criptográficos dos arquivos instalados nas urnas inseminadas ...*
> *Como sugestões para a implementação da verificação da autenticidade dos programas, podem ser consideradas as seguintes alternativas:*
> *• utilização de um flash card externo* ***(que permite controlar a inicialização da urna)*** *que contenha um programa verificador;*
> *• verificação* ***(direta)*** *do flash card interno* ***em computador independente****....*
> *• distribuição de um programa fonte de verificação, que pudesse ser* ***analisado e compilado independentemente****...*

Desde então, essas três alternativas da recomendação da Unicamp nunca foram permitidas pelo TSE. No seu lugar, o TSE oferece duas alternativas que impedem o controle da auditoria pelos auditores externos, tais como:

> *• utilização de um pen-drive* ***(que não possibilita controlar a inicialização da urna)*** *com um apontador para um programa verificador compilado pelo TSE e previamente gravado na própria urna;*
> *• autoverificação* ***(indireta),*** *ou pseudo-verificação, do flash card interno por um programa nele incluído que imprime uma tabela de hashes pré-conhecida.*
> *obs.: os programas de autoverificação permitidos (VPP ou Programa dos Partidos) são* ***compilados pelo próprio TSE***

118 **Tozzi C. L. et all** - *Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica)* : Brasil - UNICAMP, maio de 2002: http://www.tse.jus.br/arquivos/relatorio-final-de-avaliacao-do-sistema-informatizado-das-eleicoes

As características destacadas em negrito são aquelas que retiram dos auditores externos a possibilidade de controlar o ato de verificação direta da integridade dos programas executáveis carregados nas urnas. Considera-se muito baixo o nível de confiabilidade dessas alternativas de autoverificação oferecidas pelo TSE.

Em resumo, para se verificar de forma confiável os *hashes* dos arquivos gravados na memória das urnas, o cálculo tem que ser feito em outro equipamento (que seja confiável) que leia diretamente os dados extraídos do cartão de memória (*flash-card* interna da urna) que se quer verificar.

Apesar do procedimento permitido ser de baixa confiabilidade, os auditores recolheram as tabelas de *hash* (resumos criptográficos) de 684 urnas durante suas visitas aos TRE´s listados na seção 4.4.1, p. 73. Nenhuma discrepância foi encontrada nas tabelas obtidas com o uso do programa VPP carregado nas próprias urnas.

Sob as restrições impostas pela autoridade eleitoral, de não permitir acesso direto às memórias das urnas, ficou totalmente prejudicada a possibilidade dos auditores procederem, com razoável nível de confiança, a certificação do *software* embarcado nas urnas utilizadas no 2º turno de 2014.

4.4.2.9. Auditorias Internas

Atividade prevista no PTI: avaliar o resultado e a eficácia das auditorias internas posteriores às eleições de 2014, desenvolvidas sobre os equipamentos usados

Entendia-se que deveria existir um plano de auditoria interna automática, a ser desenvolvido depois das eleições, que procurasse verificar, por amostragem, se o conteúdo das memórias das urnas eletrônicas não apresentava sinais ou rastros de mau uso ou de mau funcionamento.

Por meio do Pedido de Esclarecimento 13, foi solicitado o seguinte:

> *Solicitamos a informação sobre o número de urnas eletrônicas que foram objeto de perícia direta, pelo TSE ou por terceiros nas Eleições de 2014. Consideramos perícia direta a análise forense sobre as memórias não voláteis (Flash Interna, Flash Externa, BIOS, Hardware de segurança, entre outros)*

A resposta obtida foi a seguinte:

> *Não é de conhecimento da STI/TSE qualquer perícia direta em urnas eletrônicas para análise de memórias não-voláteis.*

Assim, essa tarefa do PTI ficou totalmente prejudicada, uma vez que a autoridade eleitoral não efetua qualquer auditoria posterior para avaliar o comportamento real dos equipamentos eleitorais, tentando de identificar potenciais tentativas de fraude ou mesmo refutar denúncias de ocorrências indevidas

4.4.2.10. Lacres das Urnas Eletrônicas

Atividade prevista no PTI: avaliar o sistema de lacres usados nas urnas eletrônicas como meio para revelar uma tentativa de adulteração do software

Embora a autoridade eleitoral tenha recusado informar quais seriam as salvaguardas de segurança do sistema eleitoral informatizado, depreende-se do apresentado na página oficial do TSE que os lacres usados nas urnas eletrônicas têm a função importante de revelar eventuais tentativas de acesso para modificação do *software* carregado nas mesmas.

O uso dos lacres está normatizado na Resolução TSE 23.395/2013, que prevê a sua aplicação logo após a carga do *software* nas urnas e determina que eles devem "*ser confeccionados em material autoadesivo de segurança que evidencie sua retirada após a aplicação*".

São colados seis lacres em cada urna eletrônica. Embora todos eles sejam importantes, considera-se que dois deles apresentam, se rompidos, maior risco de adulteração do *software* carregado. São eles os seguintes, conforme definidos no art. 4º da Res. TSE 23.395/2013:

> *III - **lacre para a tampa do cartão de memória**: impedir que se tenha acesso ao cartão de memória de votação originalmente instalado no momento da carga ou que ele seja removido, modificado, substituído ou danificado;*
> *VII - **lacre do gabinete do Terminal do Eleitor** (TE): impedir a abertura do TE e o acesso indevido aos mecanismos eletrônicos internos da urna;*

Durante o recolhimento dos dados nos TRE's, foi avaliado o estado dos lacres das 684 urnas eletrônicas disponibilizadas. Todos foram filmados e/ou fotografados e se solicitou que constassem das atas oficiais os casos de lacres irregulares.

Foram encontradas as seguintes irregularidades nos lacres:

a) lacres com sinal de rompimento – com as letras TSE legíveis no seu fundo;
b) lacres descolados ou que se desprendiam com facilidade sem apresentar sinais de rompimento;
c) lacres com numeração diferente da que constava no documento de carga.

Encontraram-se irregularidades nos lacres em, aproximadamente, 21% das urnas examinadas, que foram devidamente registradas nas atas nos TRE's.

Constatou-se, também, que nesses casos nenhuma observação constava nas respectivas atas da seção eleitoral e que nenhuma providência administrativa foi gerada por motivo de lacres danificados ou soltos durante a eleição.

Também foram feitos testes com os lacres durante o período de análise do *software* nas dependências do TSE, onde se constatou o seguinte:

a) os lacres demoram algumas horas depois de aplicados para efetivamente aderirem e passarem a funcionar adequadamente;
b) ao serem retirados, depois de esperado o tempo para aderência correto, surgem as letras TSE sobre o fundo branco dos lacres, revelando a sua retirada;
c) se, depois de retirados, forem colocados sobre uma superfície branca as letras TSE ficam camufladas e difíceis de serem percebidas a média distância e sem uma observação atenta e profissional.

Se um lacre da tampa do cartão de memória ou do gabinete do eleitor for retirado com cuidado, colado sobre um papel adesivo branco e depois reaplicado no seu lugar, facilmente passará despercebido por uma inspeção não profissional como a que normalmente é feita pelos eleitores e fiscais de partidos nas seções eleitorais.

Sob essas circunstâncias, a conclusão é que, embora importantes, os lacres colocados nas urnas são só parcialmente efetivos em sua função de revelar eventuais ataques ao *software*, uma vez que podem ser burladas as inspeções amadoras e desatentas que normalmente ocorrem e, principalmente, porque não se encontrou qualquer caso de lacres rompidos ou descolados que tivesse disparado alguma atividade de segurança para sua avaliação e correção.

4.4.2.11. Teste de Votação Paralela

Atividade prevista no PTI: avaliar os Testes de Votação Paralela, realizados nos TRE, quanto a sua efetividade para verificar a integridade do software das urnas quando em uso em condições normais de votação

O Teste de Votação Paralela é atividade obrigatória estabelecida no § 6º do art. 66 da Lei 9.504/1997, com o objetivo de submeter uma amostra de urnas eletrônicas, normalmente preparadas, a um teste de votação controlada e desenvolvido sob condições normais de uso.

Trata-se de um tipo de teste que, se bem realizado, pode denunciar eventual funcionamento irregular do *software* embarcado nas urnas quanto ao registro e apuração dos votos, tornando-se uma ferramenta de detecção de fraudes por adulteração maliciosa do *software* embarcado que se aproveite das vulnerabilidades descritas na seção 4.4.2.4.

O correto desenvolvimento do Teste de Votação Paralela ganha mais importância considerando a dependência e simultânea falta de transparência do *software* eleitoral.

O teste só poderia ser burlado por um *software* adulterado se este conseguisse, durante o seu funcionamento, detectar condições ambientais diferentes do normal e percebesse que está sob o teste e, então, abortasse a fraude. Assim preparado, um *software* adulterado passaria pelo teste sem apresentar irregularidades, mas desviaria votos no seu funcionamento normal nas seções eleitorais.

Tal preocupação é reforçada pela existência de casos reais de *software*s que apresentam comportamento indevido apenas quando certas condições são satisfeitas, ameaça esta conhecida genericamente como "*bomba lógica*".

Um exemplo notório deste tipo de código malicioso refere-se a um caso de tentativa de fraude bancária ocorrido na década de 90 nos EUA: neste caso, um programador inseriu em 1996 uma bomba lógica no sistema do Deutsche Bank, a qual seria ativada quando o relógio do sistema atingisse o mês de julho de 2000[119].

Outros casos semelhantes de bombas lógicas ativadas pelo relógio do sistema (também denominadas de "*bombas relógio*") ocorreram em 2006, em caso que levou

119 The New York Times (2000). "*Man Indicted In Computer Case*". Disponível em: http://www.nytimes.com/2000/02/10/business/man-indicted-in-computer-case.html

a danos superiores a 3 milhões de dólares à UBS PaineWebber[120,121], em 2009, quando a empresa americana Transportation Security Administration (TSA) ficou incapaz de utilizar seus sistemas de verificação de passageiros (e.g., pessoas com mandados de prisão ou impedidas de voar)[122].

Outra consideração é que, facilmente, um possível fraudador poderia criar uma forma de bloqueio da bomba lógica. Alguma sinalização externa, para avisar ao programa fraudador para não se ativar. Por exemplo, apertar duas teclas "*Corrige*" em seguida.

O inverso também é válido, ou seja, pode-se fazer com que o trecho malicioso do código somente seja ativado após algum evento externo. Um evento poderia ser, por exemplo, um eleitor qualquer digitar uma sequência específica de teclas, durante a votação, o que provavelmente seria uma fraude mais viável em eleições municipais.

Para a eleição de 2014, o Teste de Votação Paralela foi regulamentado no CAP. VII (Arts. 45 a 66) da Res. TSE 23.397/2013, onde são estabelecidos a amostragem a ser testada e os vários procedimentos de sorteio e transporte das urnas, da preparação e inserção dos votos e do encerramento do processo. Também é determinada a contratação de uma empresa para desenvolver uma auditoria do teste.

Considerando que as urnas eletrônicas utilizadas na eleição normal são dependentes do *software* e não possibilitam uma auditoria contábil do resultado, que as restrições à auditoria do *software* das urnas não permitiram descobrir se ele estava livre de erros que afetassem o resultado e que também se descobriu a existência de diversas vulnerabilidades que permitiriam um ataque interno ao *software* das urnas, a presente auditoria procurou determinar a efetividade do Teste de Votação Paralela para detectar eventual *software* fraudulento, pela verificação dos procedimentos do teste, desde a amostragem até a emissão dos BU impressos, e se os mesmos foram corretos e efetivos para impedir que um *software* malicioso conseguisse burlar o teste.

O Teste de Votação Paralela foi desenvolvido normalmente em todos os TRE's, no dia da eleição, em acordo com a regulamentação do TSE.

---

120 S. Gaudin (2006). "*Ex-UBS Systems Admin Sentenced To 97 Months In Jail*". Revista Information Week. Disponível em: http://www.informationweek.com/ex-ubs-systems-admin-sentenced-to-97-months-in-jail/d/d-id/1049873?

121 S. Gaudin (2006). "*UBS Trial: Parts Of Attack Code Found At Defendant's Home*". Revista Information Week. Disponível em: http://www.informationweek.com/ubs-trial-parts-of-attack-code-found-at-defendants-home/d/d-id/1044358?

122 J. Ensslin (2011). "*Springs man sent to prison for hacking into TSA computer*". The Gazette. Disponível em: http://gazette.com/article/110969

Foram recolhidas as informações digitais (arquivos de BU, LOG e RDV) sobre os Teste de Votação Paralela realizados em 16 estados, a saber: Acre, Alagoas, Amazonas, Bahia, Ceará, Distrito Federal, Goiás, Maranhão, Minas Gerais, Paraíba, Pará, Paraná, Pernambuco, Piauí, Rio de Janeiro, São Paulo. Em alguns desses estados foi obtido acesso, também, à documentação em papel como a ata da cerimônia e o relatório da empresa auditora.

Devido às limitações de tempo e recursos, não foram coletados os dados de 11 estados: Amapá, Espírito Santo, Mato Grosso, Mato Grosso do Sul, Rondônia, Roraima, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe, Tocantins.

4.4.2.11.1. A Amostragem

A amostra de urnas a serem testadas, determinada no art. 51 da Res. 23.397/2013, estabelece a escolha de 2, 3 ou 4 urnas dependendo da quantidade de Seções Eleitorais de cada estado da Federação, resultando em uma amostra total de apenas 68 urnas testadas em todo o Brasil.

Nos estados analisados na presente Auditoria, foram coletados os dados das 45 urnas testadas, o que representa 130 milionésimos do universo de urnas usadas na eleição, assim distribuídas:

Estado	Testadas	Usadas	%
Acre	2	1.636	0,1222
Alagoas	2	6.111	0,0327
Amazonas	2	6.528	0,0306
Bahia	4	31.268	0,0128
Ceará	3	19.921	0,0151
Distrito Federal	2	6.452	0,0310
Goiás	2	13.145	0,0152
Maranhão	3	15.463	0,0194
Minas Gerais	4	45.762	0,0087
Paraíba	2	9.523	0,0210
Pará	3	15.999	0,0188

Estado	Testadas	Usadas	%
Paraná	3	25.090	0,0120
Pernambuco	3	18.791	0,0160
Piauí	2	7.937	0,0252
Rio de Janeiro	4	32.675	0,0123
São Paulo	4	88.753	0,0045
Total	**45**	**345.054**	**0,0130**

4.4.2.11.2. As Condições Normais de Votação

O ponto principal para que o Teste de Votação Paralela tenha efetividade é que as urnas devem ser testadas sob condições normais de uso, pois qualquer condição de uso que não respeitar o padrão normal poderá ser utilizado por um eventual código malicioso como sinalizador para abortar a bomba lógica e burlar o teste, derrubando toda sua possível eficácia.

A importância da simulação de condições normais de votação durante o teste é reconhecida nas atas oficiais das Comissões de Votação Paralela constituída em cada TRE, como no caso do Paraná onde constava que (grifo nosso):

> *...reunidos... para a realização, por amostragem, da auditoria mediante votação paralela, para fins de verificação do funcionamento das urnas sob condições normais de uso...*

A STI/TSE confirmou que a simulação de condições normais de uso é meta do teste, como consta em sua resposta ao Pedido de Esclarecimento 50, quando também informou que não faz qualquer verificação posterior nos arquivos de controle das urnas (LOG, RDV e BU) para procurar determinar se as condições normais de votação foram cumpridas (abaixo, grifos nossos):

> ***Pedido de esclarecimento 50 do PSDB -****... Para que este método (de Votação Paralela) seja efetivo ... a urna deve ser testada em condições idênticas ou as mais próximas possíveis ao do dia da votação. Queira esclarecer se este entendimento é correto.*
> *Solicitamos esclarecer se o STI/TSE realiza análises comparativas entre os registros produzidos pelas urnas seleciona-*

das pela votação paralela e os registros produzidos pelas demais urnas. Caso afirmativo ... quais os resultados obtidos dessa comparação?

***Resposta da STI ao Pedido de esclarecimento 50** - A Resolução TSE nº 23.397/2013, capítulo VII, disciplina os procedimentos de votação paralela. A votação paralela ocorre em condições idênticas à da votação normal, acrescida de mecanismos para batimento dos votos registrados na urna (todos os mecanismos descritos na resolução). A STI/TSE não realiza qualquer tipo de análise comparativa entre os registros produzidos pelas urnas de votação paralela e as demais urnas.*

No entanto, a comparação dos registros de controle das urnas testadas na votação paralela com aqueles das urnas usadas na eleição normal (2º turno de 2014) revelou sinais claros de uso das urnas sob condições diferentes, permitindo a um eventual *software* adulterado detectar que estava sob o teste e abortar a fraude, para burlá-lo.

São apresentados, a seguir, alguns desses sinais encontrados separando a análise em dois casos: das urnas com biometria e das urnas sem biometria.

Na eleição de 2014 foram usadas 16,7% de urnas com biometria e a previsão do TSE é de chegar a 100% do eleitorado até 2019. Entre as urnas analisadas e que passaram pelo Teste de Votação Paralela no 2º turno de 2014, 37,8% delas eram biométricas (17 de 45).

No caso das urnas com biometria, é gritante a ocorrência de procedimentos totalmente diferentes e fora das condições normais de uso, como revela o quadro a seguir, extraído dos arquivos de LOG das respectivas urnas eletrônicas usadas em 2º turno de eleições presidenciais:

Urnas biométricas usadas na	**Média de liberação do voto pelo mesário**
Eleição de 2014	6,7%
Eleição de 2010	7,1%
Votação Paralela - 2014	98,4% (min. de 94%)

Sob essas condições, fica muito simples para um eventual programa malicioso detectar, com elevada certeza, que está sob o Teste de Votação Paralela, bastando analisar o conteúdo do arquivo de LOG da urna para verificar a porcentagem de liberação de votos pelo mesário no lugar de liberação por identificação biométrica do eleitor, e abortar a bomba lógica se esse valor estiver, por exemplo, acima de 80%.

Na realidade, a ocorrência desse sinalizador é inevitável no caso das urnas biométricas: como não é possível levar os eleitores registrados nas urnas sorteadas ao TRE para simular uma votação normal, o procedimento determinado pelo TSE é que TODOS OS VOTOS sejam liberados por autorização do mesário e não, como é o normal, por reconhecimento da biometria do eleitor.

O resultado esperado da liberação pelo mesário sob essa regulamentação deveria ser de 100%. O fato de ter resultado 98,4% indica a ocorrência de outro problema potencialmente grave no sistema biométrico das urnas eletrônicas que é o *falso-positivo*, isto é, quando o sistema aceita uma identificação biométrica de outra pessoa como se fosse a de um eleitor legítimo. O caso do falso-positivo será analisado com mais detalhes em seção adiante.

A conclusão sobre este sinalizador é que as urnas com biometria, criadas pelo TSE sem haver obrigação legal para tal, simplesmente são incompatíveis com a lei que obriga a realização da Votação Paralela.

Assim, o Teste de Votação Paralela é ineficaz para detectar fraudes por *software* em urnas biométricas que verifiquem a taxa de liberação de votos pelo mesário.

Apenas para fins informativos, já que a distribuição de urnas biométricas pelo Brasil não é uniforme e nenhuma análise estatística comparativa de resultados poderia levar a conclusão de fraude via *software*, no 2º turno de 2014 a distribuição dos votos válidos foi a seguinte:

Identificação do eleitor em	**Votos Dilma (%)**	**Votos Aécio (%)**	**Diferença porcentual**
Urnas com biometria	9.435.906 (53,20%)	8.300.934 (46,80%)	6,40%
Urnas sem biometria	45.065.202 (51,32%)	42.740.221 (48,68%)	2,64%
Total	54.501.118 (51,64%)	51.041.155 (48,36%)	3,28%

No caso das urnas sem biometria, cuja tendência é deixarem de ser usadas no futuro, também existem alguns sinais que indicam a situação de teste, como mostrado no quadro a seguir, relativo ao 2º turno de eleições presidenciais:

Urnas sem biometria usadas na	Horário da Zerésima (média)	Taxa de abstenção	Votos em Branco	Votos Nulos
Eleição 2014	7:26:52**	21,10%	1,70%	4,53%
Eleições anteriores*	n/c	20,32%	1,84%	4,41%
Votação Paralela 2014	7:49:02	9,07%	4,35%	8,54%

** media das eleições de 2002, 2006 e 2010*
*** no Estado do Paraná*

A taxa de abstenção simulada no teste é menor que a metade da taxa histórica e a taxa de votos em branco e nulos simulada é maior que o dobro da taxa histórica.

O horário médio de emissão da zerésima também é bastante diferente entre o simulado e o real de 2014 (não foi possível obter os dados de eleições anteriores).

Assim, esses quatro índices também podem ser controlados por um eventual programa malicioso que só desvie os votos, no final do dia, quando esses quatro índices estiverem simultaneamente em condições “normais” e não sob teste.

Apurou-se situação na qual as condições do teste paralelo foram desenvolvidas de forma ainda mais diferente de uma votação normal: os respectivos arquivos de log revelam que, nas quatro urnas testadas (urnas sem biometria), foi executado o programa VPP[123] antes do início da votação e, em todas elas, a zerésima só foi emitida cerca de uma hora depois do horário médio normal.

Tal uso do VPP não ocorre, e nem poderia ocorrer, em qualquer urna usada em votação normal em todo o país.

O trecho abaixo, extraído do arquivo de LOG de uma das urnas testada pelo TRE local, demonstra o uso não previsto e fora do padrão normal de votação do VPP:

123 O programa VPP nunca é executado no dia da eleição sob condições normais. Os Art. 33 e 34 da Res. TSE 23.397 apenas prevêem o seu uso nos dias anteriores e posteriores à eleição. Para ser executado em uma urna eletrônica, o VPP necessita a quebra do lacre da mídia de resultados para a inserção da mídia de inicialização específica, a qual nunca está disponível nas seções eleitorais em operação no dia da eleição. O rompimento dos lacres das urnas no dia da eleição é terminantemente proibido, a não ser em condições de contingência.

Visualizador de Logs 2014 - (C) Tribunal Superior Eleitoral - TSE
Versão: 4.12.0.0 - Rio Sao Francisco
Arquivo Visualizado: [o00158-4123800350128.l]
UF.....: MG
Município..: 41238 - BELO HORIZONTE
Zona.....: 0035
Seção.....: 0128
Pleito.....: 00158

Data Hora Urna Aplicação - Descrição
==========…
26/10/2014 07:41:17 1198346 GAP - Identificada mídia de resultado - Verificador Pré e Pós Eleição
26/10/2014 07:41:23 1198346 GAP - Solicita código de liberação de aplicativo
26/10/2014 07:41:23 1198346 VCOD - Aguarda entrada do código de liberação do aplicativo [1ª vez]
26/10/2014 07:43:13 1198346 VCOD - Código de liberação digitado
26/10/2014 07:43:13 1198346 VCOD - Código de liberação Ok
26/10/2014 07:43:14 1198346 GAP - Solicita ao INIT a execução do aplicativo de urna
26/10/2014 07:43:14 1198346 GAP - Finalizado
26/10/2014 07:43:19 1198346 VPP - Iniciado: Oficial
26/10/2014 07:43:20 1198346 VPP - versão: 4.12.0.0
26/10/2014 07:45:13 1198346 VPP - Imprimindo relatório de Hash dos Arquivos - FI
26/10/2014 07:46:19 1198346 VPP - Imprimindo relatório de Hash dos Arquivos - FE
26/10/2014 07:47:24 1198346 VPP - Imprimindo relatório de Hash dos Arquivos - FI
26/10/2014 07:47:45 1198346 VPP - Imprimindo relatório de Hash dos Arquivos - FE
26/10/2014 07:47:57 1198346 VPP - Finalizado

Com esse tipo de alteração arbitrária dos procedimentos, em tese permitido pela Comissão da Votação Paralela do TRE local[124], um programa malicioso para fraudar a apuração das urnas poderia detectar que estava sob teste paralelo e abortar sua rotina de fraude, a partir da simples verificação das condições de uso do VPP, no dia da votação.

A decisão da STI/TSE de não efetuar estudos simples como os acima, não lhe permite perceber que o Teste de Votação Paralela, da maneira como vem sendo desenvolvido sob as regras estabelecidas nas resoluções escritas pela própria STI, não atende a condição mínima essencial de simular o mais próximo possível as condições normais de votação.

124 Não foi possível determinar de onde partiu a sugestão e a ordem para o rompimento dos lacres das urnas e a execução do VPP durante os testes paralelos.

E, com isso, o teste perde quase toda a sua capacidade de detectar adulterações de funcionamento do *software* que afetem o justo registro e apuração dos votos, pois só será capaz de revelar um *software* grosseiramente adulterado que não procure se desviar do teste.

Assim, eventuais fraudes bem elaboradas via *software* das urnas, que podem ser implementadas por ataque interno que explore as vulnerabilidades descritas nas seções anteriores, não seriam detectadas nem por auditoria contábil (por não se produzir o VVPAT), nem por auditoria do *software* (devido ao porte da tarefa e ao excesso de restrições impostas aos auditores) e nem pelo Teste de Votação Paralela.

4.4.2.11.3. A Auditoria Interna

Nos artigos 57 e 58, a Resolução 23.397/2013 prevê a contratação de uma empresa "*com a finalidade de fiscalizar os trabalhos da votação paralela*".

Em 2014, a vencedora da licitação foi a empresa Grupo Maciel que produziu um relatório de sua auditoria para cada TRE.

Foram contratados apenas um auditor para cada urna testada (total de 68), diferentemente de 2012 quando também havia sido contratado mais um auditor (total 94) para acompanhar cada computador de apoio que é usado durante os testes.

Considera-se que um auditor por urna testada é muito pouco para uma tarefa que dura mais de 10 horas ininterruptas de trabalho. Para, de fato, fiscalizarem a inserção de cada voto nas urnas testadas, o auditor não poderia, por exemplo, sair para almoçar ou ir ao banheiro.

A empresa auditora fez constar a restrição de pessoal em todos os seus relatórios, onde escreveu que:

> *... assim como no primeiro turno, o número enxuto de auditores contratados para a realização dos trabalhos (94 auditores no ano de 2012 para 68 auditores no ano de 2014), seguiu gerando dificuldade e um desgaste excessivo para a execução do mesmo.*

A análise dos relatórios da empresa auditora revela que se tratava de uma auditoria de característica interna e não externa e independente, pois o plano de trabalho foi elaborado pela STI/TSE e não pelos auditores de forma independente.

Os auditores contratados pelo TSE apenas responderam a um questionário padrão elaborado pela STI. Como esta declarou (pedido 50) que não procura determinar

a efetividade do teste pela análise dos dados produzidos nas urnas testadas, nenhuma questão foi apresentada que procurasse determinar se o teste ocorreu (efetivamente e não apenas formalmente) sob *"condições normais de uso das urnas"*.

As questões preparadas pela STI estavam agrupadas em 20 itens específicos que remetiam apenas à verificação de procedimentos formais, como a constituição da Comissão de Votação Paralela, o sorteio das urnas na véspera, o início e encerramento nas horas exatas previstas, a emissão da zerésima, a comparação dos resultados impressos pelas urnas e pelo sistema de apoio da própria STI, etc.

O subdimensionamento da equipe de auditores contratados condicionou-os a apenas responder as questões da STI, sem ter tempo para qualquer outra verificação ou análise mais profunda. Por exemplo, os auditores do Grupo Maciel não procediam à contagem independente dos votos inseridos em cada urna, confiando cegamente no sistema de apoio fornecido pela STI, sem auditar o seu desempenho de fato.

Os relatórios para cada TRE possuíam o mesmo texto básico com pequenas modificações feitas pelos auditores locais, evidenciando a existência de um modelo prévio padrão das respostas e que houve uma centralização nacional na elaboração dos relatórios com pouca margem de atuação para os auditores locais. Todos os relatórios estavam assinados pelo Presidente do Grupo Maciel e não por cada equipe de auditores de cada TRE.

A resposta-padrão preparada para a questão 12.1 revela uma informação incorreta em todo o Brasil. A pergunta do questionário do TSE e a resposta padrão que foi encontrada nos relatórios, eram as seguintes (grifo nosso):

> *Pergunta da STI – 12.1. Validas (sic) a votação nas urnas eletrônicas, verificando se o servidor encarregado de digitar as inscrições dos eleitores pertencentes à seção sorteada, habilitando o voto par (sic) o votador, não utilizando inscrição sequencial e sim randômica e digitação de títulos de eleitores não pertencentes à seção.*
> *Resposta padrão dos auditores – Não detectamos irregularidade nos procedimentos na votação nas urnas eletrônicas, onde o servidor encarregado digitou as inscrições dos eleitores pertencentes à seção sorteada, habilitou o voto para o votador, não utilizando inscrição sequencial e sim randômica e não digitou títulos de eleitores não pertencentes à seção.*

No entanto, a análise dos arquivos de LOG das urnas usadas no teste de votação paralela mostra a ocorrência de 417 digitações de títulos inválidos pelo operador e de 236 justificativas de voto.

Para uma justificativa ser inserida em uma urna eletrônica que está em regime de votação é necessária a digitação de um número de título de eleitor que não esteja inscrito na seção; e tanto a ocorrência de uma justificativa como a digitação de título inválido são registradas logo depois de digitados pelos mesários, como exemplificam os lançamentos seguintes, extraídos do log de urnas testadas:

26/10/2014 09:41:00 1198346 VOTA - Título digitado pelo mesário
26/10/2014 09:41:11 1198346 VOTA - Justificativa do eleitor foi efetuada com sucesso
...
26/10/2014 10:38:22 1198346 VOTA - Título digitado pelo mesário
26/10/2014 10:38:22 1198346 VOTA - Título digitado pelo mesário é inválido

Em outras palavras, a resposta padrão à questão 12.1, dada pelos auditores contratados pelo TSE, revelou-se incorreta em todos os Estados onde foram simuladas justificativas ou digitados títulos inválidos, evidenciando que os auditores envolvidos no processo de votação paralela não estavam atentos ou não conseguiram perceber mais de 650 ocorrências desse tipo.

Em especial, onde os arquivos de LOG das urnas demonstram a ocorrência de atividades totalmente fora do padrão de uma eleição comum - como o rompimento dos lacres, a execução do programa VPP antes da votação e a emissão da zerésima - poderiam estar acoberto o uso eventual de uma bomba lógica no *software* das urnas, sendo que, nessa situação, o relatório da empresa auditora nada registra nem revela.

No seu item *6. Inconformidades Apuradas*, apresenta a mesma resposta padrão dos demais Estados, nos seguintes termos:

> *Nos dias de acompanhamento da Auditoria Externa da Votação Paralela não foi encontrada nenhuma inconformidade que possa ter prejudicado a lisura dos trabalhos.*

A conclusão é que a auditoria contrata pelo TSE, "*com a finalidade de fiscalizar os trabalhos da votação paralela*" nos termos dos artigos 57 e 58 da Resolução 23.397/2013, caracterizou-se como uma auditoria interna controlada, e não uma auditoria externa independente, e que não teve por objeto e nem por metodologia verificar se o Teste de Votação Paralela atingiu a meta de simular os procedimentos de uma votação normal.

No exemplo ilustrado neste capítulo, a empresa auditora contratada pelo TRE não percebeu que os procedimentos foram arbitrariamente alterados, aceitando, indevidamente, um procedimento fora do padrão normal, que poderia estar servindo de sinalizador para que o programa em execução na urna abortasse uma rotina de fraude. Nessas condições, a votação paralela deixa de identificar que, ao mesmo tempo e com o mesmo programa, estaria havendo fraude na votação oficial.

4.4.2.11.4. Conclusões sobre a Efetividade do Teste de Votação Paralela

Considerando que:

a) os procedimentos do Teste de Votação Paralela não simularam as condições normais de votação;
b) a auditoria da empresa contratada atuou sob orientação estrita da STI e não desenvolveu qualquer procedimento independente para verificar se as "*condições normais de uso*" foram respeitadas durante os testes;

Conclui-se que o Teste de Votação Paralela, ocorrido durante o 2º turno de 2014, não atingiu um nível de efetividade na tarefa de detectar eventuais adulterações maliciosas no *software* embarcado nas urnas eletrônicas testadas, no caso dessas adulterações terem sido produzidas para intencionalmente abortarem a fraude quando sob teste.

O caso das urnas com biometria é mais grave porque elas são incompatíveis com esse tipo de teste legal e sempre será possível para um *software* malicioso facilmente burlar o teste.

Na prática, o uso de urnas com biometria do eleitor torna ineficaz o §6º do artigo 66 da Lei 9.504/1997, que, por motivos de segurança, institui o Teste de Votação Paralela.

Destaque-se, ainda, o sucedido demostrado nesse capítulo, no qual os procedimentos do teste foram arbitrária e injustificadamente modificados, introduzindo sinais indeléveis que poderiam ser detectados por eventuais rotinas fraudadoras do resultado que procurassem tais sinais para se esconderem ou *adormecerem* durante o teste.

Como na ocorrência relatada, o Teste de Votação Paralela simplesmente não detectaria um *software* fraudulento que oculte sua presença durante a votação paralela mediante o simples estratagema de verificar a existência de um registro do VPP no arquivo de LOG, no dia da eleição naquele Estado.

4.4.2.12. Teste de Penetração

Atividade prevista no PTI: fazer um teste de penetração em urnas reais, carregadas com software oficial, para comprovar eventuais vulnerabilidades encontradas como viáveis para ataque

Teste de Penetração é o nome utilizado em normas técnicas sobre segurança de sistemas informatizados, para regulamentar atividades nas quais elementos capazes, atuando com total liberdade de ação, tentam burlar as defesas do sistema contra invasão ou mau uso.

Essa tarefa foi incluída no PTI porque, diante de um sistema cuja confiabilidade é essencialmente dependente do *software*, se pretendia procurar uma confirmação de uma possível exploração de vulnerabilidades que tivessem sido encontradas durante a fase de análise do *software*.

Antes mesmo do início dos trabalhos de análise, a autoridade eleitoral tomou a iniciativa de emitir uma nova resolução para regulamentar "*a realização periódica do Testes Público de Segurança no sistema eletrônico de votação e apuração*".

O uso da expressão "*Teste Público de Segurança*" na resolução do TSE, no lugar de "*Testes de Penetração*", se justifica porque a regulamentação criada pela autoridade eleitoral não estava conforme com os termos de qualquer norma técnica sobre a execução de testes livres de penetração.

O PSDB solicitou permissão para apresentar sugestões sobre a regulamentação que estava sendo desenvolvida. A autoridade eleitoral aceitou a apresentação das sugestões, mas, atendendo orientação da STI, rejeitou o conteúdo de quase todas as sugestões apresentadas.

Em especial, foram rejeitadas todas as sugestões no sentido de tornar mais livre a atuação dos analistas. Entre as sugestões rejeitadas estavam:

a) eliminar a restrição à participação de analistas estrangeiros ou brasileiros residentes no exterior;
b) eliminar a STI como membro das comissões organizadora, de regulamentação e de comunicação dos testes (podendo participar como assessora);
c) permitir a participação dos Partidos Políticos, da OAB e do MP como membros nas comissões organizadora, de regulamentação e de comunicação;
d) limitação do Termo de Confidencialidade à data de apresentação do relatório do teste;
e) permissão para efetuar compilação dos fontes para teste efetivo dos "*hashes*".

Foram aceitas na regulamentação do teste de segurança, porém, rejeitadas na prática, durante a fase de Auditoria do *software,* as seguintes sugestões:

a) permissão para utilização de ferramentas de análise do *software* (negado na resposta ao pedido 2 e 8 durante a análise do *software*);
b) inclusão, no escopo do teste, do *software* embarcado (*firmware*) das urnas (negado na resposta ao pedido 27).

Na resposta ao Pedido 47, no qual se solicitavam os relatórios de testes de penetração já efetuados por terceiros, o setor SEVIN/STI respondeu o seguinte:

> *Resp. ao ped. 47 - "O TSE jamais contratou terceiros para realizar teste de penetração nas urnas eletrônicas"*

No entanto, essa informação da STI aos auditores está incorreta e frontalmente contradiz o que está dito na publicação do TSE denominada *Por Dentro da Urna*[125], na seção "*Auditorias*", na página 14, que diz o seguinte (g.n.):

> *Em 2008, o TSE contratou a Fundação de Apoio à Capacitação em Tecnologia da Informação (FACTI) para a prestação de serviços especializados de suporte na especificação de dispositivos eletrônicos de hardware e de software a serem aplicados no sistema eletrônico de votação brasileiro, com foco na melhoria da segurança e na redução dos custos.*
> *Para viabilizar o trabalho da FACTI, o Tribunal disponibilizou, por meio de acordo de confidencialidade, todos os modelos de urna, computadores, sistemas compilados (prontos para uso) e códigos-fonte dos sistemas eleitorais da urna e do gerador de mídias para uma análise profunda de segurança.*
> *Outro contrato firmado com a FACTI estabeleceu a prestação de serviços de consultoria para a elaboração, o acompanhamento da execução e a análise de testes de vulnerabilidade quanto à segurança da votação. Esse trabalho incluiu: ataque e intrusão em algumas partes do sistema eletrônico de votação e da urna eletrônica; e auxílio na definição e confecção de algumas diretivas de segurança dos novos softwares da urna.*

125 **Tribunal Superior Eleitoral** – *Por dentro da Urna*. - 2ª edição revista e atualizada – Brasília: TSE, 2010 – disponível em: http://www.justicaeleitoral.jus.br/arquivos/tse-cartilha-por-dentro-da-urna

Diante desse quadro e das regras limitadoras criadas, inclusive pela recusa de credenciamento de um renomado especialista em testes de penetração em equipamentos eleitorais (o prof. Alex Halderman) como membro da equipe de auditores do PSDB (sob argumento de ser um atentado contra a soberania nacional), decidiu-se não dar andamento ao pedido de execução de teste de penetração, por se compreender que limitações incontornáveis e sem base em normas técnicas conhecidas estavam sendo impostas pela autoridade eleitoral, para restringir o livre desempenho da Auditoria, o que provocaria resultados inconclusivos, como ocorreu com a análise dos códigos fontes.

4.4.3. Análise da Filmagem de Urnas Selecionadas

Atividade prevista no PTI: filmar as urnas selecionadas para teste, observando eventual comportamento não-uniforme entre as selecionadas

Durante as diligências realizadas nos TRE's pela presente Auditoria Especial, foram filmados teclado e tela de diversas urnas durante sua inicialização e execução de alguns programas. A filmagem foi autorizada pelo TSE e teve os seguintes objetivos principais:

a) Registrar os detalhes do procedimento;
b) Verificar as versões da BIOS utilizadas nas urnas eletrônicas;
c) Verificar se o procedimento de geração do *hash* pelo programa VPP é uniforme entre as urnas de um mesmo modelo;
d) Verificar eventuais anormalidades;

Na amostra referente ao item "b", não foram constatadas divergências. Ressalte-se que todos os modelos de BIOS deveriam ser fornecidos para análise no código-fonte para levantamento de eventuais fragilidades, o que não foi possível conforme já descrito.

Com relação ao item "c", foi verificada uma grande variabilidade no tempo de geração de código *hash*, mesmo entre urnas similares em modelo, uso ou não de biometria, unidade federativa e número de eleitores. De modo geral, nas cerca de 250 urnas analisadas até o momento, foi observado um tempo médio de 5:28 com um desvio padrão de 2:33.

Mesmo para urnas do mesmo estado, do mesmo modelo, ambas com biometria, houve variações de geração e impressão do *hash* entre 1:54 e 8:22. Considerando eventuais variações na velocidade de leitura das memórias *flash* (o que não foi possível constatar pela falta de acesso às mesmas), estas deveriam ser lidas em tempos uniformes, ou seja, várias urnas com tempos similares de geração, ainda que díspares entre si. Deste modo, não é possível afirmar qual é a causa desta anormalidade.

Com relação ao item “d”, foram observadas urnas antigas com longo tempo de *boot* e com diversos erros registrados no log de inicialização. Este comportamento foi observado em diversas urnas modelo 2004. Não é possível saber a causa deste comportamento neste nível de análise.

Além disso, foi constatado que ao menos duas urnas apresentaram travamento logo na tela de *boot*. Esse comportamento não é esperado, uma vez que as urnas apresentadas foram aquelas que foram utilizadas até a finalização da eleição e deveriam estar em perfeito estado de funcionamento.

4.4.4. Auditoria da Transmissão e da Totalização – Item (3) do PTI

De forma diferente do que ocorre com a auditoria da apuração nas urnas, a etapa de transmissão dos dados e a totalização dos votos no Brasil têm como serem auditadas por via externa e independente do *software* usado.

Para tanto, bastaria aos Partidos se organizarem para coletar Boletins de Urna impressos nas seções eleitorais[126] e depois verificarem se estes foram, um a um, corretamente transmitidos e totalizados.

Como são mais de 420 mil seções eleitorais espalhadas por todo território nacional, é natural que cada partido não consiga recolher a totalidade dos BU impressos, forçando que essa auditoria seja feita de forma estatística.

Descrevem-se a seguir os procedimentos efetuados para avaliar a precisão da transmissão e totalização dos resultados.

126 Para a auditoria da transmissão e totalização ser efetiva é necessário que os BU impressos sejam recolhidos ainda nas seções eleitorais e não nos Cartórios Eleitorais, como é comum ser feito por partidos despreparados do ponto de vista da fiscalização efetiva.

4.4.4.1. Os Dados e Resultados Gerais

Atividade prevista no PTI: comparar os dados gerais da eleição (2º turno, 2014 – presidente), como abstenção, votos válidos, brancos e nulos, com eleições anteriores similares em busca de discrepâncias significativas

Os dados oficiais do 2º turno de 2014 fornecidos indicam que estavam inscritos 142.822.046 eleitores (70,87% da população) em 451.501 seções eleitorais agregadas em 428.894 urnas eletrônicas instaladas em 96.146 locais de votação.

Foram utilizadas 429.824 urnas eletrônicas (incluindo as de contingência) sendo 357.926 delas urnas sem biometria. As demais 71.898 eram urnas com biometria (16,7%) utilizadas em 724 municípios com um total de 21.677.955 eleitores aptos.

Dos modelos fabricados até 2008, sem circuito interno de segurança MSD, foram usadas 1.120 como urnas biométricas e 108.302 como urnas comuns. Dos modelos fabricados depois de 2009, com circuito interno de segurança MSD, foram usadas 70.778 como urnas biométricas e 249.624 como urnas comuns.

Compareceram para votar 112.683.879 eleitores, resultando em uma taxa média de abstenção de 21,10%.

Os valores apresentados da totalização dos votos indicam o seguinte resultado:

Dilma Rousseff (13)	54.501.118	48,37%
Aécio Neves (45)	51.041.155	45,30%
Brancos	1.921.819	1,70%
Nulos	5.219.787	4,63%
Comparecimento	112.683.879	100 %
Abstenção	30.137.749	21,10% (dos aptos)
Total Eleitores Aptos	142.822.046	

Os quadros de votos válidos por modelo de urna (com ou sem biometria e com ou sem circuito MSD) são os seguintes:

Votos Válidos biometria	Votos Dilma (%)	Votos Aécio (%)	Diferença porcentual
Urnas com biometria	9.435.906 (53,20%)	8.300.934 (46,80%)	6,40%
Urnas sem biometria	45.065.202 (51,32%)	42.740.221 (48,68%)	2,64%

Votos Válidos circuito MSD	Votos Dilma (%)	Votos Aécio (%)	Diferença porcentual
Urnas com MSD	41.083.280 (52,94%)	36.516.659 (47,06%)	+5,88%
Urnas sem MSD	13.550.552 (48,06%)	14.647.158 (51,94%)	- 3,88%

A comparação dos votos válidos, brancos e nulos com a série histórica de eleições presidenciais em 2º turno indica o seguinte:

2º Turno - %	2002	2006	2010	2014
Abstenção	20,47	18,99	21,50	21,10
Votos Válidos	94,00	93,96	93,30	93,67
Brancos	1,89	1,33	2,30	1,70
Nulos	4,11	4,71	4,40	4,63

Essa série histórica não sugere que tenha havido desvio de votos brancos e nulos para algum candidato, mas nos dois quadros anteriores chama a atenção a inversão de tendências entre candidatos conforme o modelo de urna.

De uma maneira geral, o desempenho do candidato do PSDB foi inferior onde foram utilizadas urnas com *software* mais complexo, como as com o circuito MSD e com biometria.

Considere-se que a complexidade do *software* aumenta a dificuldade de auditoria para detectar eventual *malware* nele inserido, fato que é agravado em sistemas dependentes do *software* como o modelo das urnas eletrônicas brasileiras.

A presente auditoria não teve condições de verificar se essa inversão de tendência foi motivada por eventual *software* adulterado nas urnas com biometria ou com circuito MSD, pois, como detalhado na seção 4.4.2, o Teste de Votação Paralela não é efetivo com urnas biométricas e o *software* embarcado nos circuitos MSD não foi apresentado para avaliação.

4.4.4.2. Coerência dos Dados Digitais sobre a Totalização

Atividade prevista no PTI: verificar a consistência e coerência entre os resultados da apuração de cada seção/urna e o resultado final publicado

Esta tarefa consiste apenas em se somar os resultados oficiais de cada urna/seção para verificar sua coerência com o resultado geral publicado pelo TSE.

É uma tarefa de alcance parcial, pois demanda que também seja feita a verificação, por amostragem, se os valores dos BUweb (resultado de cada seção publicado na Internet) são idênticos aos que foram impressos nos BU nas seções eleitorais (tarefa essa discutida a seguir).

A análise revelou coerência entre os números apresentados nos BUweb e o resultado eleitoral oficial final.

4.4.4.3. Conferência Estatística da Totalização

Atividade prevista no PTI: obter o maior número possível de BU impressos recolhidos por fiscais no dia da eleição, inclusive pelo projeto Você Fiscal[127], e obter cópias dos BU extraídos de uma amostra escolhida de urnas usadas na eleição, para comparar com resultados oficiais por seção eleitoral

Esta tarefa é complementar à anterior e procura verificar, por amostragem, se os resultados dos BU impressos são os mesmos que compõem a base de dados BUweb usada na totalização. Se essa tarefa apontar sucesso, significa que a transmissão e a totalização dos resultados é potencialmente confiável, dependendo essa análise basicamente da relevância estatística da amostragem utilizada.

127 Projeto Você Fiscal – http://www.vocefiscal.org/

Assim, essa é uma tarefa que enfrenta o problema do volume de BU impressos a serem conferidos, pois, por mais que se procure otimizar a amostra por meio de estratificações, qualquer estratégia sempre resultará num número grande de urnas dispersas num vasto território a terem seus dados coletados e conferidos manualmente.

Há também que se enfrentar os problemas logísticos, pois os Partidos não conseguem, de maneira geral, se organizar para cumprir a coleta de uma amostra cientificamente projetada.

Na presente auditoria foram conferidos 503 BU impressos que haviam sido recolhidos pelo Partido e pelos auditores no dia da eleição e mais 7.020 BU fotografados e conferidos pelo projeto Você Fiscal[128]. As seções cobertas nesse caso foram recolhidas ao acaso, sem uma distribuição planejada.

Outros 684 BU foram recolhidos diretamente de urnas auditadas nos TRE e, nesse caso, foram escolhidas urnas que atendiam ao menos dois dos seguintes critérios:

a) Denúncias específicas na imprensa de votos realizados em nome de terceiros;
b) Votos rápidos suspeitos (em menos de 4 segundos);
c) Votos lentos suspeitos (eleitor demorou mais de 5 minutos);
d) Liberação pelo mesário em número excessivo, em urnas biométricas;
e) Arquivo RDV fora da formatação esperada;
f) Urnas cujos logs não foram fornecidos no início;
g) Seções com baixa abstenção e/ou votação em Aécio menor que 10%;
h) Diferenças entre correspondências.

A escolha de apenas 684 urnas nesse caso foi devido a limitações de tempo e de orçamento. Teve-se que enviar equipes de dois ou três auditores para 16 estados, onde eram recolhidos os dados de 30 a 40 urnas de cada vez.

Não foram encontradas divergências entre os BU impressos obtidos e os respectivos valores registrados na base de dados do TSE.

Destaque-se que essa análise não abrange uma auditoria da apuração dos votos nas urnas, ou seja, não avalia a correção do resultado registrado em cada BU em si, mas apenas se são iguais o conteúdo do BU impresso com o respectivo BU recepcionado pelo sistema totalizador.

Considera-se essa amostra, por sua aleatoriedade e volume, o suficiente para indicar, com boa margem de confiança, que a transmissão dos dados produzidos pelas urnas e a totalização desses dados no 2º turno de 2014 ocorreram sem sofrer adulteração capaz de inverter o resultado final.

128 http://www.vocefiscal.org/blog/resultados-da-conferencia-coletiva-dos-boletins-de-urna/

4.4.4.4. Reprodução do Gráfico da Totalização no tempo

Atividade prevista no PTI: analisar os arquivos de eventos (log) dos sistemas de transmissão de resultados a procura de sinais de acessos impróprios e para refazer o gráfico da totalização no tempo, publicado pelo TSE

Essa atividade consistia em se tentar reconstruir o gráfico da totalização no tempo, que foi publicado pelo TSE. Para tanto, seria necessário, além dos resultados de cada seção (BU), do horário em que cada resultado foi totalizado.

No entanto, resultou infrutífera essa tarefa, uma vez que o TSE não mantém documentos de auditoria que permitam saber a que momento cada BU foi totalizado. Além disso, todos os arquivos de log que se obteve, dos vários sistemas de recepção e de transmissão dos resultados, eram parciais ou incompletos e não chegavam a indicar em que momento tal dado foi finalmente considerado, no TSE, na elaboração do gráfico da totalização no tempo.

Um emaranhado de pacotes transmitidos de forma independente e sem sincronia preestabelecida dos Cartórios para os TRE’s e destes para o TSE tornaram impossível a tarefa de reconstruir o gráfico desejado.

O insucesso dessa tarefa revela que a autoridade eleitoral também não se preocupou com a criação de trilhas de auditoria funcionais sobre a sequência da totalização dos resultados.

Entende-se que o administrador eleitoral deveria acrescentar em sua base de dados das seções eleitorais, a informação do horário em que cada BU foi efetivamente considerado na totalização oficial parcial.

4.4.5. Denúncias Específicas – Item (4) do PTI

Nessa seção, são analisadas as denúncias mais específicas que chegaram ao comando da campanha do partido.

4.4.5.1. Geração de Mídias

Denúncia: computadores que geravam as mídias de carga das urnas tinham conexão ativa com a Internet.

Durante as demonstrações dos sistemas no TSE, os auditores puderam confirmar que, de fato, os computadores dos Cartórios Eleitorais onde rodavam o sistema GEDAI, que geram as mídias que serão utilizadas na carga e preparação das urnas eletrônicas, não tinham qualquer restrição quanto a estarem conectados na Internet no momento da geração.

Essa constatação vai de encontro ao que costumeiramente é divulgado como *"salvaguarda"* do sistema eleitoral, de que não haveria conexão com a Internet nos pontos críticos do processo eleitoral, pois, aparentemente, essa preocupação é aplicada apenas à urna eletrônica em si.

O momento da geração das mídias de carga é um momento crítico e deveria estar protegido contra acesso indevido, principalmente se considerado que a própria STI/TSE reconheceu (resposta ao pedido 33) que as chaves de segurança dos programas executáveis foram obtidas dos próprios programas que são gravados na mídia de carga, argumento este que foi usado para negar acesso dos auditores para conferência dos programas executáveis.

4.4.5.2. Smartmatic

Denúncia: a empresa, estrangeira, teria fraudado a contagem dos votos – muitas denúncias com documentação diversa, mas inespecífica.

A empresa Smartmatic foi alvo de inúmeras denúncias elaboradas com amplitude e algum detalhamento, que alegavam que ela tem um histórico de participação em fraudes eleitorais em outros países e que participaria de um esquema de fraude na totalização dos votos no Brasil.

Em 2012, a Smartmatic do Brasil Ltda. integrava o consórcio ESF que foi contratado pelo TSE[129], para fornecimento de serviços de "*exercitação das urnas eletrônicas*". Dois meses depois, a empresa Smartmatic Internacional Corporation foi incluída no contrato por meio de um termo aditivo.

O contrato previa as seguintes atividades:

> *a) carga das baterias internas e de reserva;*
> *b) exercitação dos componentes eletrônicos mediante utilização do programa;*
> *c) STE – Sistema de Testes Exaustivos, desenvolvido e fornecido pelo TSE;*
> *d) limpeza, retirada de lacres, testes funcionais, triagem para manutenção corretiva e preparo para armazenamento das urnas eletrônicas;*
> *e) inserção dos dados coletados das urnas no Sistema de Logística de Urnas e Suprimentos – LOGUSWEB;*
> *f) procedimentos de atualização de software embarcado e certificação digital nas urnas de modelos a partir de 2009, inclusive;*
> *g) preparação, instalação, carga de software de eleição (até 1/3 podendo ser executado em outro local que não o de armazenamento), testes e operacionalização das urnas eletrônicas, suporte à geração do B.U.;*
> *h) recepção de mídias e transmissão dos boletins de urna (BU), via sistema de apuração.*

129 Contrato 80/2012 da licitação TSE 42/2012, com as empresas Smartmatic Brasil, Engetec Tecnologia e Fixti Soluções em TI.Em vários processos na Justiça do Trabalho, a Engetec Tecnologia SA foi declarada sucessora da Probank SA, fornecedora do TSE, ao menos desde 2004, dos mesmos serviços ora contratados.

Os três últimos itens são críticos. Pelo item (f) se tem oportunidade de inserção de *porta-dos-fundos* dentro do circuito de segurança MSD das urnas de modelo 2009 em diante. O item (g) dá acesso às urnas no momento de carga do *software* de eleição. E o item (h) dá acesso às mídias de resultado que são transmitidas para a totalização.

Apenas um eventual ataque às mídias de resultado poderia ser detectado por uma auditoria da totalização. Já eventuais ataques ao *firmware* do MSD ou ao *software* das urnas não poderiam ser detectados pelos procedimentos de auditoria que a autoridade eleitoral permite e pratica atualmente.

Esse contrato de 2012 foi revogado, por interferência do TCU, mas as empresas Smartmatic e Engetec criaram diversos outros consórcios (Engematic, Smartitec, etc.) para participar de outras licitações no TSE e nos TRE's.

Em 2014 teriam sido contratas por, ao menos, 11 TRE's para o fornecimento de serviços similares ao do contrato de 2012, excluindo-se o designado no item (f) de atualização do *firmware* dos circuitos MSD das urnas.

Nesses termos, verifica-se que, em 2012, funcionários da Smartmatic teriam tido, em tese, acesso às urnas eletrônicas novas, recebidas do fabricante, para participar das atividades de atualização do *software* gravado nos circuitos de segurança MSD, que se entende serem passíveis de abrigar *malware* (como *portas-dos-fundos*) que permitam a exploração em um momento posterior. Em 2014 eles também tiveram acesso à carga das urnas e à transmissão dos resultados.

A conferência da transmissão e da totalização dos votos que foi possível desenvolver (seção 4.4.4.3) não detectou sinais de ataques sistemáticos ou abrangentes que tenham ocorrido no 2º turno de 2014.

Já a auditoria da apuração, que não foi possível desenvolver de forma satisfatória (seção 4.4.2), não teve como eliminar a possibilidade de ter ocorrido ataque via *software* das urnas.

4.4.5.3. Eleitor Já Votou

Denúncia: eleitor não pôde votar porque alguém já tinha votado em seu nome – muitas denúncias, algumas documentadas, inclusive em seções com urnas biométricas.

Foram muitas as reclamações de eleitores que não conseguiram votar porque, alegadamente, já teriam votado antes.

Não se obteve uma tabulação extensiva desse tipo de reclamação em todo Brasil e, por isso, não se tem como avaliar o potencial de alteração do resultado eleitoral, mesmo porque os eleitores que não conseguiram votar poderiam votar para qualquer um dos dois candidatos.

Esse problema ocorre sempre que o mesário, por erro, usa o número de um eleitor disponível na lista de votação para liberar o voto para outra pessoa.

Também poderia ocorrer no caso de fraude de uma pessoa que obtenha os documentos de um eleitor e se apresente para votar no seu lugar, mas são eventos de baixa frequência e de baixo potencial de inverter o resultado da eleição presidencial.

A princípio também se pode afastar nesse caso, ao menos parcialmente, a hipótese de fraude do mesário (analisada em seção adiante) pois o mesário mal-intencionado poderia acobertar seu comportamento indevido permitindo que o eleitor votasse no lugar de qualquer outro eleitor que ainda não tivesse votado.

Em urnas sem biometria se pode verificar a incidência de erros de digitação do mesário pela frequência de ocorrências do lançamento "*eleitor já votou*" nos arquivos de LOG. A análise da quantidade de lançamentos *"eleitor já votou"* não indicou a ocorrência de números fora do aceitável ou de ocorrência de erros sistemáticos em uma mesma seção eleitoral.

Já em urnas com biometria, esse tipo de erro não deveria ocorrer pois, em condições normais, ao se verificar a digital do eleitor seria descoberto e corrigido o erro de digitação do mesário.

Porém, durante a análise dos arquivos de LOG das urnas usadas na Votação Paralela, revelou-se um outro problema inesperado: diversos casos de falso-positivo em urnas com biometria, o que possibilita, em tese, que terceiros se passem por eleitores legítimos e votem no lugar deles.

A tecnologia de reconhecimento biométrico é essencialmente um procedimento estatístico não-determinístico que pode, eventualmente, apresentar casos de falso-negativo[130] e de falso-positivo[131]. Em sua página oficial na Internet[132], a autoridade eleitoral reconhece a possibilidade do falso-negativo e também mostra que não espera a ocorrência de casos de falso-positivo, nos seguintes termos:

> *"A medida (biometria) impede que uma pessoa tente se passar por outra no momento da identificação* ***(alegação de não ocorrência do falso-positivo)*** *em um pleito ...*
> *A possibilidade de um eleitor autêntico ser negado pelo sistema biométrico é real* ***(reconhecimento da ocorrência de falso-negativo)****, embora muito rara, fato comprovado nas últimas eleições, que registraram baixíssimo índice de não reconhecimento das digitais..." - comentários em parênteses e negrito por nós incluídos*

Apesar de já estar em uso desde as eleições de 2008, a presidência do TSE revelou insegurança e reconheceu que o uso da biometria das urnas eletrônicas ainda é um processo imaturo ao determinar, no Processo Administrativo nº 188-62, a exclusão da biometria do escopo dos testes públicos de segurança, nos seguintes termos:

> *Sobre a sugestão de inclusão dos dispositivos biométricos como parte do escopo dos testes de segurança, informamos que a verificação biométrica é um sistema ainda em implantação e evolução, representando uma porção minoritária das seções eleitorais. Além disso, a biometria não é um sistema determinístico, e, portanto, seriam complexos os critérios para avaliar se houve ou não subversão de algum dispositivo de segurança.* [133]

130 O falso-negativo ocorre quando um eleitor legítimo não é reconhecido pelo sistema biométrico. A taxa de falso-negativo esperada no início do projeto de biometria em 2008 era de 1%. Quando ocorre um caso de falso-negativo, o TSE determina que o mesário digite uma senha de liberação da urna para que o eleitor vote mesmo sem ter ocorrido o reconhecimento biométrico.

131 O falso-positivo ocorre quando um terceiro é reconhecido no lugar de um eleitor legítimo, permitindo que vote em seu lugar. A taxa de falso-positivo esperada no início do projeto de biometria em 2008 era mínima. Quando ocorre um caso de falso-positivo, o sistema do TSE não consegue detectar e o erro passa despercebido pelo sistema.

132 http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/biometria-1

133 Apesar de considerar o sistema de biometria ainda imaturo, em implantação e difícil de ser avaliado em testes externos de segurança, o TSE já possui mais de 400 mil urnas com biometria, das quais utilizou aproximadamente 80 mil em 2014, e, durante o andamento da presente auditoria, abriu a licitação 40/2015 para a compra de mais 150 mil novas urnas biométricas.

No caso de ocorrência do falso-negativo, o erro é detectável e pode ser compensado pela liberação do voto pelo mesário. Usando o número de liberações do mesário como métrica, a taxa de falso-negativo ocorrida durante a eleição normal pode, portanto, ser determinada pela análise dos arquivos de BU e de LOG das urnas. No 2º turno de 2014 a taxa de falso-negativo foi de 6,7%, similar à eleição de 2010 (7,1%).

São valores muito acima do ideal esperado no início do projeto (1%), e que certamente não deveriam ser considerados como "...*baixíssimo índice de não reconhecimento das digitais...*" como ocorre na referência[134] já citada acima

No caso de ocorrência do falso-positivo em uma eleição normal, o erro não é detectado pelo sistema e uma eventual fraude não é revelada. Por isso, no projeto de sistemas biométricos, se costuma ser rigoroso nesse caso, procurando reduzir a possibilidade de ocorrência de falso-positivo ao mínimo possível, sendo comum procurar-se alcançar índices abaixo de 1 falso-positivo em cada 1000 testes.

Porém, no caso do Teste de Votação Paralela, no qual nenhum eleitor verdadeiro está presente para liberar o voto em seu nome, o arquivo de LOG consegue registrar os casos de falso-positivo, que ocorrem quando a impressão digital do operador do TRE é reconhecida como a de um eleitor legítimo.

A análise dos arquivos de LOG das 17 urnas com biometria submetidas ao teste de votação paralela revelou a ocorrência de falso-positivo em 8 delas, nas quais se atingiu uma taxa média de 1,41% de falsos-positivo[135], com um inesperado máximo de 5,85% de falsos-positivo na urna que seria usada na SE 0473 da ZE 0003 de Recife.

São números um tanto surpreendentes, muito acima da taxa esperada considerando avaliações similares com o mesmo sistema de *software* biométrico.

Mais precisamente, conforme análise realizada pelo NIST[136] com diversos algoritmos de biometria, incluindo os sistemas *Morpho-SAGEM* e *NBIS-EC* (*NIST Biometric Image Software*) utilizados pelo TSE no seu sistema de identificação biométrica do eleitor, esperar-se-ia, por exemplo:

---

134 Textos do TSE sobre o uso da biometria nas urnas, a partir de:http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/biometria-1

135 A taxa de falso-positivo em urnas biométricas usadas na votação paralela é obtido a partir do número de lançamentos de "*eleitor reconhecido*" no dia do 2º turno, obtido no arquivo de LOG, dividido pelo comparecimento registrado no BU.

136 NIST – National Institute of Standards and Technology. "*NISTIR 8034 - Fingerprint Vendor Technology Evaluation*". Dezembro de 2014, DOI: http://dx.doi.org/10.6028/NIST.IR.8034Os dados citados foram extraídos das Tabelas 7 e 8 na página 26 e do gráfico da Figura 90 na página 104 do relatório do NIST.

a) uma taxa de falsos-positivos de 0.1% para uma taxa de falsos-negativos próxima a 2.2%;
b) uma taxa de falsos-positivos inferior a 0.05% para uma taxa de falsos-negativos superior a 2.5%;uma taxa de falsos-positivos da ordem de 50% se fosse usado como taxa alvo de falsos negativos o número de 1%.

Verifica-se, portanto, que o sistema utilizado pelo TSE está se comportando consideravelmente fora da faixa de operação observada no documento do NIST.

O baixo desempenho obtido com relação aos falsos-negativos se deve, aparentemente, à baixa qualidade na coleta dos dados biométricos dos eleitores, como sugere a notícia[137] publicada no dia 04 de maio de 2015 pelo jornalista Ary Filgueira.

O baixo desempenho quanto aos falsos-positivos se deve, aparentemente, à decisão da STI de reduzir para 20 o *score*[138] necessário para considerar positiva uma identificação, com a finalidade de diminuir os casos de falsos-negativos e, assim, reduzir o atraso na votação que a identificação biométrica realizada no próprio equipamento de votação inevitavelmente provoca.

A análise dos arquivos de LOG, de urnas biométricas usadas na votação normal e das usadas na votação paralela, mostra que a identificação biométrica de um eleitor real costuma atingir *score* entre 40 a 60, enquanto os casos de falsos-positivos na votação paralela atingiam *score* entre 20 a 25.

Se o score limite de aceitação tivesse sido estabelecido um pouco acima, em 30 por exemplo, se reduziria a valores mais aceitáveis os casos de falso-positivo.

Ou seja, a necessidade de o administrador eleitoral reduzir a taxa de falso-negativo para reduzir o atraso na votação com urnas biométricas provocou o crescimento dos casos de falso-positivo para muito além do razoável.

Como agravante, tem-se que essa taxa média de falso-positivo em urnas biométricas é superior à taxa de denúncias de "*eleitor já votou*" que chegou ao Partido e, então, a falha mais grave do sistema biométrico (falsos-positivos) pode ser acolhida como uma possível explicação para a ocorrência inesperada desse tipo de denúncia em Seções Eleitorais que usaram urnas biométricas em 2014.

137 "*PF constata erro no cadastro biométrico realizado pelo TRE-DF*" - disponível em: http://www.fatoonline.com.br/conteudo/2430/pf-constata-erro-no-cadastro-biometrico-realizado-pelo-tre-df

138 *Score*: é o termo usado pelo TSE nos arquivos de LOG, como indicador da quantidade de coincidências encontradas em uma identificação biométrica.

4.4.5.4. Eleitor Fantasma

***Denúncia**: eleitor que viajou ao exterior constatou que algum "fantasma" votou em seu lugar. Apresentou documentação da viajem e do certificado de votação dado pelo TSE.*

O eleitor encaminhou a seguinte denuncia[139]:

> *Sou filiado ao PSDB.*
> *Não votei nestas eleições porque fui visitar meu filho e meu neto na cidade de Dallas / Texas, fiquei por lá de 21 de setembro a 22 de novembro 2014*
> *Hoje 22/01/14, fui a 249ª Zona Eleitoral de São Paulo /SP – para justificar a minha ausência e de minha esposa na votação de 2014.*
> *Levei os seguintes documentos, carteira de identidade, passaporte, passagens de ida e volta e título eleitoral.*
> *Primeiramente viram os documentos de minha esposa e expediram para ela o Requerimento de Justificativa Eleitoral – Protocolo de entrega.*
> *Quando apresentei os meus documentos fui informado de que não precisaria justificar, pois eu já havia votado nas eleições, então pedi uma certidão de quitação que me foi entregue.*
> *Se ocorreu isto comigo imaginem o que mais poderia ter ocorrido nesta seção, neste caso acho que deveriam ser interrogados o presidente e mesários da seção.*
> *Anexo copia das passagens ida e volta American*
> *Passaporte com data de entrada nos Estados Unidos*
> *Copia da Certidão da Justiça Eleitoral da 249ª Zona Eleitoral de São Paulo – SP. Dizendo que o eleitor abaixo qualificado está quite com a Justiça Eleitoral na presente data.*
> *Espero que este meu testemunho sirva para a comissão que esta trabalhando nas analise das urnas desta eleição de 2014.*
> *Atenciosamente.*

Os documentos enviados pelo eleitor comprovam que ele estava no exterior no dia da eleição e que o TSE certificou que ele votou na seção eleitoral na cidade de São Paulo.

139 Para preservar a identidade do denunciante, foram excluídos todos os dados que pudessem levar à sua identificação.

O caso de eleitores que apresentaram justificava porque não se encontravam na cidade onde estão cadastrados e, ao mesmo tempo, constam como tendo votado é muito fácil de ser detectado com a simples análise dos arquivos de eleitores aptos/faltosos e arquivos de justificativa.

O caso pode ser provocado por eventual erro ou por fraude do mesário (como descrito na seção a seguir), pois se pode afastar a hipótese do eleitor ter votado normalmente para depois viajar para outra cidade e apresentado uma justificativa falsa, atitude altamente improvável de ocorrer com frequência significativa. Assim, se entende que, nos casos de duplicidade, a justificativa é o dado correto e o voto é o dado incorreto (falso).

Uma vez tabulados os casos, não seria possível determinar e eliminar o voto falso, mas ter-se-ia uma precisa indicação das seções eleitorais onde o problema ocorreu com incidência acima do normal, e, com essa informação, seria possível abrir uma investigação sobre a confiabilidade dos mesários respectivos (como justificadamente foi sugerido pelo denunciante) e, se for o caso, evitar sua convocação em eleições futuras.

Contudo, não foi possível verificar a incidência desse problema porque a autoridade eleitoral negou o fornecimento dos arquivos de eleitores faltosos e de justificativas sob o argumento redundante de que esse fornecimento não estava previsto na própria regulamentação.

Pelo Pedido de Esclarecimentos 49, foi consultada a STI/TSE para responder se tal análise é feita internamente, depois de uma eleição, e, caso positivo, qual foi a incidência e as medidas preventivas tomadas. Obteve-se a seguinte resposta:

> *Compete à Corregedoria Geral Eleitoral adotar as ações corretivas de um pleito eleitoral.*

Como a resposta formal nada esclarece, informalmente se soube que a autoridade eleitoral não desenvolve qualquer cruzamento de dados de votantes e justificativas para orientar medidas preventivas futuras.

Com isso, nos casos de duplicidade, a justificativa (dado com maior probabilidade de estar correto) é simplesmente desprezada e o voto (dado mais provavelmente falso) é considerado válido e computado normalmente.

Essa postura da autoridade eleitoral, de desprezar a informação mais confiável e computar a informação menos confiável, foi comprovada pelos documentos enviados pelo eleitor que, indignado, fez a denúncia.

4.4.5.5. Fraude do Mesário

Denúncia: mesários inseriam votos nas urnas no final do dia – muitas denúncias, pouco documentadas.

Denomina-se como *Fraude do Mesário* a inserção de votos ilegais nas urnas eletrônicas em nome eleitores que ainda não compareceram para votar e outras fraudes de menor efeito, como a indução do voto de um eleitor ou a anulação do restante do voto de um eleitor que demore durante a votação.

A inserção de votos ilegais por ação ou conivência dos mesários não tem solução tecnológica viável, sendo possível de ocorrer tanto nas urnas comuns como nas urnas com biometria e só pode ser inibida, de fato, pela presença atenta de fiscais nas seções eleitorais.

A biometria do eleitor, que costuma ser apresentada como solução para impedir que terceiro vote no lugar de um eleitor legítimo, não consegue evitar a fraude do mesário.

Isso se deve ao problema do falso-negativo, que é inevitável que venha a ocorrer. Para corrigi-lo, o administrador eleitoral permite que um voto possa ser inserido nas urnas biométricas a partir da digitação de um código fixo que é fornecido a todos os mesários.

Normalmente, essa fraude ocorre no final do período de votação, quando os fiscais abandonam a seção eleitoral e abrem a oportunidade para que mesários inescrupulosos, agindo em conluio ou sob coação, insiram votos em nome dos eleitores que ainda não compareceram. A inserção desses votos ilegais costuma ser feita de forma rápida e sequencial depois das 16 ou 16h30 e, por isso, também são chamados de "*votos rápidos e tardios*".

Uma forma de potencialmente identificar a ocorrência dessa fraude é a análise do arquivo de LOG de cada urna para determinar se houve uma alteração no ritmo de inserção de votos no final do período da votação e, no caso das urnas biométricas, se houve crescimento na quantidade de liberações do voto pelo mesário (com a simulação de um falso-negativo).

A tabela abaixo apresenta a quantidade de votos totais e de votos rápidos (dados em até 5 segundos) registrados em todas as urnas, a cada hora do dia de votação:

Horário de votação	Quantidade de votos total	%	Quantidade de votos em até 5 seg	%
08h às 09h	15.303.935	13,6	762.291	13,3
09h às 10h	15.601.460	13,8	717.738	12,5
10h às 11h	15.842.983	14,1	805.703	14,1
11h às 12h	13.845.765	12.3	754.959	13,2
12h às 13h	11.382.648	10,1	622.265	10,9
13h às 14h	10.641.945	9,4	547.891	9,6
14h às 15h	11.066.843	9,8	548.990	9,6
15h às 16h	11.033.383	9,8	539.773	9,4
16h às 17h	7.917.942	7,0	422.987	7,4
17h às 18h	42.046	0.04	3.196	0,05
18h às 19h	48	0	5	0

A quantidade de votos rápidos depois das 17h foi de apenas 3201 votos, um valor insignificante. Mesmo entre às 16h e 17h a quantidade de votos rápidos se reduziu, mostrando um comportamento porcentual similar ao total de votos a cada hora.

A análise mais minuciosa desses dados chegou a encontrar seções eleitorais com comportamento fora do normal, mas não mostrou incidência de votos rápidos e tardios em quantidade e regularidade que pudesse inverter o resultado eleitoral.

Conclui-se que a Fraude do Mesário, no final do período de votação, não ocorreu em intensidade significativa.

4.4.5.6. Problemas Localizados

Denúncias:
Urna fantasma *- urna votava "sozinha" -* ***com vídeo***
Documentos oficiais descartados *- documentos da seção eleitoral jogados no lixo –* ***com vídeo***
Fraude na zerézima *uma zerésima constava com 400 votos para Dilma –* ***com imagem***
Teclado adulterado *- urna registrava 44 quando se tentava digitar 45 –* ***com vídeo***
Fraude na zerésima *- inseriram pen-drive na urna antes do início da votação*

Essas denúncias eram individuais e localizadas, não evidenciando um problema sistêmico. Os três primeiros casos acima foram esclarecidos pelo TSE logo no voto inicial que aprovou a auditoria.

Em especial, o caso da zerésima com 400 votos era grosseira falsificação. Os dados contidos na "*foto*" eram contraditórios e fora da formatação normal, evidenciando ter sido manipulado com o uso de algum programa de edição de imagens.

O caso de urna que repetia a tecla 4 quando esta era digitada caracteriza apenas um equipamento com defeito e não uma fraude pré-preparada. O equipamento deveria ter sido substituído.

Quanto a inserção do "*pen-drive*" não foi encontrada evidência na análise do arquivo de LOG.

Consideram-se todas essas denúncias de fraude infundadas e sem potencial de alterar a verdade eleitoral.

4.5. Voto Impresso

Já nos momentos finais da elaboração do presente relatório, no dia 16.06.2015, a Câmara dos Deputados aprovou, em primeira votação (433 votos a favor), a adoção do *Voto Impresso Conferível pelo Eleitor* dentro do corpo do Proposta de Emenda à Constituição PEC 182/07, do Senado.

O texto aprovado na Câmara é o seguinte:

> *Art. 14 (da Constituição Federal)*
> *§ No processo de votação eletrônica, a urna imprimirá o registro de cada votação, que será depositado, de forma automática e sem contato manual do eleitor, em local previamente lacrado.*
> *§ O processo de votação não será concluído até que o eleitor confirme a correspondência entre o teor do registro do seu voto, após impresso e exibido pela urna eletrônica, e o voto que efetuou.*
> *§ No processo estabelecido nos parágrafos anteriores será garantido o total sigilo do voto. (NR)*

No dia 23 de junho, os Ministros do STF Dias Toffoli (atual Presidente do TSE) e Gilmar Mendes (atual vice-presidente do TSE) reuniram-se com o presidente da Câmara e manifestaram-se contra a adoção do voto impresso nas urnas eletrônicas.

Os argumentos apresentados pelo Min. Toffoli foram os seguintes:

> *Do ponto de vista técnico, a Justiça eleitoral é contrária à introdução do voto impresso"*[140] *e "Toda concepção da urna eletrônica se baseou na intenção de terminar com a intervenção humana, que não deixa digitais muitas vezes*[141]

No dia 24 de junho, o Min. Ricardo Lewandowski (atual Presidente do STF e anterior Presidente do TSE) reuniu-se com o Presidente do Senado quando discutiu, entre outros temas: "*... a questão do voto impresso já considerado inconstitucional pelo tribunal, pela identificação do voto...*"[142]

---

140 Jornal O Globo - http://oglobo.globo.com/brasil/justica-eleitoral-contra-voto-impresso-por-questao-tecnica-diz-toffoli-16530449#ixzz3eeefRIa1

141 Jornal O Estado de São Paulo - http://politica.estadao.com.br/noticias/geral,toffoli-se-manifesta-contra-impressao-do-voto,1711932

Posteriormente, o Congresso Nacional aprovou projeto de lei em que se previa a introdução do voto impresso no Brasil a partir das eleições de 2018.

Este dispositivo legal foi vetado pela Presidente Dilma Rousseff, sob o argumento de que o custo para a implantação desse sistema é de R$1,8 bilhão, conforme informação do próprio TSE.

O veto ainda se encontra pendente de apreciação.

Diante do conflito de informações, apresentam-se, a seguir, alguns esclarecimentos sobre os conceitos de *Voter Veriable Paper Audit Trail* (VVPAT) ou *Voto Impresso Conferível pelo Eleitor*.

4.5.1. Voto Impresso ou Recibo do Eleitor?

É comum o entendimento que o "*voto impresso*" seria entregue como uma espécie de recibo de votação, para o eleitor o levar consigo.

Trata-se de um entendimento incorreto. Se assim fosse, o voto impresso não teria como ser usado numa eventual auditoria da apuração e ainda permitiria a comprovação do conteúdo do voto para terceiros, o que afronta diretamente o *Princípio de Inviolabilidade do Voto Absoluta* e vulnerabiliza o eleitor perante eventual coação.

A ideia do voto impresso conferível pelo eleitor é que o voto seja depositado numa urna comum, antes do eleitor deixar o local de votação, para que se possa usar os votos impressos em auditorias contábeis ou recontagens.

Este fato está devidamente caracterizado no primeiro parágrafo do texto votado na Câmara e o recibo que é entregue ao eleitor deve conter apenas uma comprovação de que ele compareceu para votar e não o conteúdo do seu voto.

4.5.2. Evolução ou Retrocesso?

Os primeiros modelos de máquinas de votar que começaram a serem usados na Holanda (1991) e na Índia (1992) eram equipamentos com gravação eletrônica direta do voto (máquinas DRE), sem *Voto Impresso Conferível pelo Eleitor*. No Brasil esse modelo foi adotado a parir de 1996[143].

142 Senador Jorge Viana - http://www.jorgeviana.com.br/index.php?option=com_content&view=article&id=8230%3Asenadores-destacam-entendimento-para-votacao-da-reforma-politica&catid=22%3Afique-por-dentro&Itemid=9

143 As urnas eletrônicas usadas na eleição de 1996, no Brasil, imprimiam uma via do voto, mas este era depositado numa sacola plástica comum, sem que o eleitor pudesse conferir seu conteúdo. Dessa forma, o modelo deve ser classificado como DRE sem VVPAT.

Desde então, intensificou-se o debate técnico e acadêmico sobre a real confiabilidade dos modelos DRE e que levou ao surgimento da proposta do *Voto Impresso Conferível pelo Eleitor*[144], em 1999 no Brasil, e do *Voter Veriable Paper Audit Trail* (VVPAT)[145], em 2001 nos EUA, como forma de incrementar a transparência e auditabilidade do equipamento DRE.

No Brasil, foi feita uma primeira experiência mundial com VVPAT em 2002, acoplado em 5% das urnas eletrônicas, mas o administrador eleitoral declarou a experiência insatisfatória e o Congresso Nacional revogou os dispositivos da Lei 10.408/2002 que previa o VVPAT a partir de 2004.

Em 2004, foi a vez da Venezuela implantar o uso pleno de equipamentos DRE com VVPAT em suas eleições oficiais. Por solicitação do *The Carter Center*[146], foi estabelecido a recontagem automática dos votos de 53% das máquinas usadas na eleição. O sistema vem sendo usado assim, desde então, demonstrando que os problemas alegados pelo TSE em 2002 foram provocados pela má implementação e não pelo conceito de VVPAT propriamente dito.

Entre 2006 até 2014, máquinas DRE puras, sem VVPAT, passaram a ser proibidas ou foram substituídas em todos os demais países que recorriam a equipamentos eletrônicos de votação.

Por motivos de segurança e de confiabilidade, abandonaram o sistema DRE sem VVPAT, os seguintes países: Alemanha, Bélgica, Holanda, Irlanda, Inglaterra, Rússia, Índia, EUA, Canadá, México, Venezuela, Peru, Equador, Argentina e Paraguai.

Essa realidade indica, de maneira indubitável, que o ***Voto Impresso Conferível pelo Eleitor*** **caracteriza uma evolução dos sistemas eleitorais eletrônicos** em direção a maior transparência e auditabilidade, e não um retrocesso como costuma argumentar o administrador eleitoral brasileiro.

Atualmente, o Brasil é o único país que ainda utiliza urnas eletrônicas sem VVPAT em eleições de larga escala.

---

144 **Brunazo F.,A**. "*A Segurança do Voto na Urna Eletrônica Brasileira*".. In: SIMPÓSIO DE SEGURANÇA EM INFORMÁTICA, SSI1999, São José dos Campos. Anais... São José dos Campos: ITA, 1999. P.19-28 - http://www.brunazo.eng.br/voto-e/arquivos/SSI99int.zip

145 **Mercuri R.** - "*Electronic Vote Tabulation, Checks & Balances*". USA: University of Pennsylvania, 27/10/2000 - http://www.notables*oftware*.com/Papers/thesdefabs.html

146 "*Missioón de Estudio del Centro Carter – Elecciones Presidenciales en Venezuela – Informe Final*". USA: The Carter Center. 14/04/2013 - http://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/venezuela-final-rpt-2013-elections-spanish.pdf

4.5.3. A Intervenção Humana

Carece de clareza o argumento da autoridade eleitoral de que:

> *Toda concepção da urna eletrônica se baseou na intenção de terminar com a intervenção humana, que não deixa digitais muitas vezes.*

A urna eletrônica brasileira, equipamento onde ocorre a captação, o registro e a apuração dos votos, é um equipamento projetado, desenvolvido, implementado, programado, lacrado e operado, durante 100% de sua vida útil, por humanos. Não há qualquer evento que ocorre dentro desses equipamentos, muitos deles registrados nos arquivos de LOG, que não esteja submetido ao manuseio e controle de humanos.

É conhecimento pacífico, na área de tecnologia da informação, que computadores são equipamentos integralmente sujeitos a erros e fraudes provocados por intervenção humana, sendo considerado equivoco primário[147] entender que computadores possam "*terminar com a intervenção humana*".

Em 2006, o *Brennan Center for Justice* da *New York University School of Law* publicou um importante estudo[148] de avaliação de riscos de sistemas eleitorais eletrônicos. Descreveu 128 possíveis tipos de fraude eleitoral e sua principal conclusão é que a fraude "*menos difícil*", ou seja, a de melhor relação custo-benefício para o fraudador, é a adulteração do *software* em máquinas DRE sem VVPAT, o que afasta definitivamente qualquer hipótese de que as urnas eletrônicas brasileiras eliminariam a intervenção humana no processo eleitoral.

Em resumo, as urnas eletrônicas brasileiras nada mais são que ferramentas projetadas e utilizadas pelos oficiais e representantes da autoridade eleitoral para captar e contar votos.

---

147 Costuma-se designar como tecno-fascinação, o comportamento deslumbrado de alguns perante as novas tecnologias, que os impedem de ver as fraquezas do mesmo sistema . Também se usa a expressão: "*fiéis da Seita do Santo Baite*".

148 Norden L.D. et al. - The Machinery of Democracy: protecting elections in an electronic world. New York: Brennan Center of Justice, NYU, 27/06/2006 - disponível em: http://www.brennancenter.org/sites/default/files/press-releases/The%20Machinery%20of%20Democracy.pdf Sumário executivo em: http://organikrecords.com/corporatenewslies/BrennanCenter_ExecutiveSummary.pdf, Sumário em português: http://www.votoseguro.org/textos/brennan-pt.pdf

4.5.4. O Voto Impresso é inconstitucional?

Em 2009, a Corte Constitucional da Alemanha estabeleceu jurisprudência[149] ao decretar que os equipamentos de voto eletrônico DRE sem VVPAT usados em 2005 eram inconstitucionais porque não atendiam o *Princípio da Publicidade* uma vez que eleitores e fiscais dos Partidos não tinham como conferir o processamento do seu voto.

Decisão similar sobre foi tomada em 2013 pela Suprema Corte da Índia[150], quando tornou obrigatório a implantação do VVPAT em suas máquinas DRE denominadas EVM (Electronic Voting Machines) a partir de 2014.

No entanto, em 2013 no Brasil, o Superior Tribunal Federal julgou exatamente no sentido contrário, ao declarar inconstitucional na ADI 4543[151] o art. 5º da Lei 12.034/2009 que previa a impressão do voto nas urnas brasileiras a partir de 2014.

O argumento dos Ministros do STF/TSE para declarar inconstitucional a lei do voto impresso era que a impressão da assinatura digital do eleitor no voto violaria o sigilo. Porém a lei previa a impressão da assinatura digital da urna eletrônica e não do eleitor e, mesmo se esta fosse considerada risco ao sigilo do voto, bastaria revogar esse detalhe da lei, não sendo necessário declarar inconstitucional o *VVPAT*.

O uso em dezenas de países é uma prova irrefutável de que é possível usar o *Voto Impresso Conferível pelo Eleitor* sem violar o *Princípio da Inviolabilidade do Voto*.

Uma possível explicação para a divergência frontal entre as decisões das Cortes Supremas da Alemanha e da Índia em relação à do Brasil é que, naquelas, os juízes não possuem qualquer função de administradores eleitorais, podendo julgar questões administrativas eleitorais com a necessária independência e isenção.

Já no Brasil, os ministros do STF acumulam a função de administradores eleitorais e perdem isenção para julgar casos que dizem respeito a sua própria atuação administrativa. No julgamento da ADI 4543, todos os julgadores eram, foram ou seriam presidentes do TSE. A ministra-relatora da ADI 4543, era também a presidente do TSE.

149 Decisão original do Tribunal Constitucional Federal da Alemanha em 03/03/2009 (em alemão):*http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html*
Princípios e Sentença (em português): *http://www.votoseguro.org/arquivos/Alemanha-ini-port.pdf*
Notícia: Tribunal alemão considera urnas eletrônicas inconstitucionais. Deutsche Welle, 03/03/2009 - *http://www.dw-world.de/dw/article/0,,4070568,00.html*

150 Decisão original da Suprema Corte da Índia em 08/10/2013 (em inglês): http://supremecourtofindia.nic.in/outtoday/9093.pdf

151 Acórdão do STF na ADI 4543, em 06/11/2013, disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=6925215#89%20-%20Inteiro%20teor%20do%20ac%F3rd%E3º

5. MAPAS DE RISCOS DA URNA BRASILEIRA

Este capítulo apresenta 13 mapas de riscos do *software* da urna brasileira com o resultado da análise dos dados e códigos disponibilizados pelo TSE para os auditores.

O resultado final mostra um cenário muito preocupante, com inúmeros riscos de segurança no nível crítico ou catastrófico, que podem propiciar desde sabotagens a mudanças de resultado de eleição. Isso tudo ocorre sem que se possa ao menos se deparar com vestígios das fraudes nas urnas, pois o sistema atual permite que eventuais atacantes da urna possam, ao final do ataque, remover todos os vestígios deixados por eles na urna eletrônica. Constata-se que a comunidade dos agentes de ameaça internos ao TSE (funcionários), pelo acesso e contato próximo do *software* da urna, é a que mais pode expor tal *software* aos riscos mais graves e catastróficos. Como sugestão de melhoria, entendemos que o TSE precisa reverter essa situação com muita urgência, por meio de muito trabalho científico e prático baseado na transparência, aderência a padrões internacionais de segurança e abertura a auditorias externas independentes, incluindo testes de penetração feitos por grupos de pesquisadores nacionais e internacionais.

5.1. Apresentação

“Prediction is very difficult, especially about the future.”

(Nobel Laureate and nuclear physicist, Niels Bohr)

Após o exame de uma grande quantidade de modelos e arcabouços de análise de riscos empregados pela indústria da segurança da informação (incluindo os principais documentos sobre o assunto, entre outros: NIST SP 800-30, NIST SP 800-60, NIST SP 800-53 e 800-53A, FIPS 200, FIPS 199, documentos ISACA), conclui-se que a abordagem FAIR, por se basear em uma taxonomia bastante completa, oferece o entre os melhores ferramentais para documentar apropriadamente os achados. A análise de riscos da urna é feita com base numa versão adaptada do método FAIR, sendo que alguns termos chave estão definidos no Apêndice A e que o livro base para o método é “*Introduction to Factor Analysis of Information Risk (FAIR)*”, de autoria de Jack Jones e publicado em 2006.

Umas das adaptações feitas ao método FAIR refere-se ao uso de valores qualitativos em vez de valores quantitativos para os diversos tipos de fatores usados em FAIR, que é uma das alternativas sugeridas, por exemplo, pelo NIST SP 800-30. O motivo dessa adaptação é o pouco tempo destinado para a análise e principalmente pela falta de informação ocasionada pelas restrições impostas pelo TSE/STI durante os trabalhos de auditoria.

De acordo com a abordagem FAIR, risco de segurança é a probabilidade de ocorrência de algo ruim em uma instituição, combinado com a magnitude ou impacto provável da perda futura resultante dessa ocorrência! Em outras palavras, risco é uma medida do grau em que uma instituição está ameaçada por uma circunstância ou evento potencial, tipicamente em função do seguinte: (i) a probabilidade de ocorrência da circunstância ou evento; (ii) os impactos negativos prováveis que surgiriam se ocorrer a circunstância ou evento.

Assim, riscos de segurança da informação são os riscos que surgem a partir da perda de, entre outras coisas, confidencialidade, integridade e disponibilidade da informação ou dos sistemas de informação; refletem os possíveis impactos adversos para as operações de organização em termos de missão, funções operacionais, imagem ou reputação, ativos da organização e indivíduos, eventualmente atingindo outras organizações e até mesmo a nação como um todo (NIST SP 800-30r1).

A avaliação de riscos é o processo de identificar, estimar e priorizar riscos de segurança da informação (NIST SP 800-30r1). A avaliação de risco requer a análise cuidadosa das informações sobre ameaças e vulnerabilidades para determinar a extensão em que circunstâncias ou eventos poderiam afetar adversamente uma organização e a probabilidade de que tais circunstâncias ou eventos irá ocorrer.

O método de avaliação de risco adotado inclui o processo e modelo de avaliação de riscos FAIR, que define explicitamente os termos-chave e fatores de risco passíveis de avaliação e as relações entre os fatores. A abordagem de avaliação é qualitativa (NIST SP 800-30r1), especificando-se o intervalo ou faixa de valores probabilísticos que esses fatores de risco podem assumir na avaliação de riscos e como os fatores de risco são identificados e analisados para que os valores desses fatores possam ser funcionalmente combinados para avaliar o risco. Em FAIR, a abordagem de análise é orientada a estimar os impactos potenciais causados por agentes de ameaças em ativos (*assets*) da instituição.

As conclusões desta avaliação de riscos são as seguintes:

- Apesar das restrições impostas pelo TSE ao trabalho de auditoria e pelo pouco tempo disponibilizado para que os auditores pudessem examinar a urna brasileira, identificamos e descrevemos 11 principais *assets*, potenciais alvos de ataques de agentes de ameaça;
- Identificaram-se 3 categorias de comunidades de agentes de ameaça que se aplicam ao *software* da urna, que se distribuem em 16 categorias de subcomunidades de agentes de ameaça;
- Dentre os principais *assets*, cerca de 9, se atacados por agentes de ameaça apropriados, exporiam o *software* da urna a riscos catastróficos/gravíssimos;
- Não se tem informação alguma sobre ataques que a urna brasileira possa ter sofrido no passado, mas a situação que relatamos através dos mapas de riscos mostram uma situação muito preocupante;
- A urna brasileira está vulnerável a diversos tipos de ataques, desde atos de sabotagem a atos que podem mudar os resultados de uma eleição;
- Além da urna estar vulnerável a ataques dos mais diversos tipos, muitos ataques podem, em muitos casos, ao seu final ter removidos todos os eventuais vestígios deixados por eles na urna eletrônica durante o ataque. Um crime perfeito!
- Finalmente, constata-se que a comunidade de agentes de ameaça internos ao TSE, identificados por InT abaixo, pelo acesso e contato próximo, é a que mais pode expor os *assets* estudados aos riscos mais graves e catastróficos;

Como recomendação, entende-se que o TSE precisa reverter essa situação com muita urgência, por meio de muito trabalho científico e prático baseado na transparência, aderência a padrões internacionais de segurança e abertura a auditoria externa independente (por meio de licitação), incluindo testes de penetração feitos por grupos de pesquisadores nacionais e internacionais.

5.2. Comunidades de Agentes de Ameaça à Urna Brasileira

De acordo com o modelo de análise de riscos FAIR, comunidades de agentes de ameaça são subgrupos da população total de agentes de ameaça que partilham características-chave. A seguir, enumera-se uma forma de caracterizar comunidades de agentes de ameaça à urna brasileira, em que se identificam três tipos de comunidades, rotuladas por CAA1, CAA2 e CAA3, onde “CAA” é um acrônimo para “Comunidade

de Agente de Ameaça”. Identificaram-se também as principais subcomunidades dentro de cada comunidade, rotuladas com um número inteiro entre parêntesis, sem se preocupar em esgotar todas as possibilidades.

CAA1: Interno ao TSE/STI (Comunidade de Agentes InT):

- O agente de ameaça tem vínculo formal com o TSE/STI, operando na gerência, desenvolvimento do *software*, compilação final do *software* da urna eletrônica ou como consultor formalmente contratado pelo TSE/STI para tarefas específicas;
- Tem acesso privilegiado ao projeto e ao *software* da urna, em grau variado de acesso;
- Tem informação privilegiada tanto do projeto quanto do *software* da urna, em grau variado de conhecimento;
- Exemplos de subcomunidades de agentes de ameaça do tipo InT: (1) desenvolvedores de *software* do STI, (2) funcionários em cargos de gerência do STI, (3) consultores envolvidos no projeto e desenvolvimento dos *software*s da urna etc.

Observações:

a) Não se está acusando ou se insinuando que alguma pessoa específica que se enquadra em um dos tipos de agente de ameaça InT fez, faz ou fará qualquer tipo de ataque às urnas;

b) Isto apenas ilustra um reconhecimento que alguma pessoa que se enquadra na categoria InT potencialmente poderá, em situações especiais e por motivação própria diversa ou sob coação de algum tipo, estar apta a perpetrar algum tipo de ataque às urnas;

c) A numeração acima é usada apenas para indicar de forma breve o tipo de agente de ameaça desta categoria; de nenhuma forma indica que os números de menor valor oferecem maior ameaça em comparação com os de maior valor, pois isso dependerá de cada tipo de *asset* e das correspondentes vulnerabilidades envolvidas com cada agente de ameaça;

d) Representação de comunidades de agentes de ameaça:
   - Utilizada nos diagramas representativos dos mapas de riscos: [CAA1: (nr. da subcomunidade)]; por exemplo, [CAA1:1], que representa [Comunidades de Agentes de Ameaça: InT; Subcomunidade: (1) desenvolvedores de *software* do STI];
   - Utilizada nos textos descritivos dos mapas de riscos, temos dois tipos alternativos, exemplificados com base no item acima:
     - [InT: (1) desenvolvedores de *software* do STI];
     - [InT: (1)].

CAA2: Externo Com Vínculo com TSE/STI (Comunidade de Agentes ExTComVinc):

- O agente de ameaça tem algum tipo de vínculo com o TSE/STI ou trabalha na área de TI de parceiros formais do TSE/STI, a saber, empresas ou órgãos associados formalmente ao projeto da Urna, tais como CEPESC/ABIN, Diebold, Módulo, produtora do chip MSD, fabricante e desenvolvedor do BIOS e funcionário formalmente contratado para distribuição de mídia por meio de empresas contratadas por processo licitatório (como a Smartmatic e outras contratadas), ou opera de maneira informal em conluio com funcionário do TSE/STI ou de parceiro;
- Tem acesso privilegiado ao projeto e ao *software* da urna, em grau variado de acesso;
- Tem informação privilegiada tanto do projeto quanto do *software* da urna, em grau variado de conhecimento;
- Exemplos de subcomunidades de agentes de ameaça do tipo ExTComVinc: (1) ex-funcionário desenvolvedor de *software* do TSE/STI em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI, (2) hacker em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI, (3) hacker em conluio com funcionário de parceiro do TSE/STI, (4) ex-funcionário desenvolvedor de *software* ou gerente do TSE/STI em conluio com funcionário de parceiro do TSE/STI, (5) funcionário de parceiro do TSE/STI dedicado à urna eletrônica, (6) ex-funcionário desenvolvedor de *software* do TSE/STI em conluio com funcionário de fabricante que desenvolve o BIOS etc.

Observações:

a) Não se está acusando ou se insinuando que alguma pessoa específica que se enquadra em um dos tipos de agente de ameaça ExTComVinc fez, faz ou fará qualquer tipo de ataque às urnas;
b) Isto apenas ilustra um reconhecimento que alguma pessoa que se enquadra na categoria ExTComVinc potencialmente poderá, em situações especiais e por motivação própria diversa ou sob coação de algum tipo, estar apta a perpetrar algum tipo de ataque às urnas;
c) A numeração é usada apenas para indicar de forma breve o tipo de agente de ameaça desta categoria; de nenhuma forma indica que os números de menor valor oferecem maior ameaça em comparação com os de maior valor, pois isso dependerá de cada tipo de *asset* e das correspondentes vulnerabilidades envolvidas com cada agente de ameaça;
d) Representação de comunidades de agentes de ameaça:
   - Utilizada nos diagramas representativos dos mapas de riscos: [CAA2: (nr. da subcomunidade)]; por exemplo, [CAA2:1], que representa [Comunidades de Agentes de Ameaça: ExTComVinc; Subcomunidade: (1) ex-funcionário em conluio com funcionário do TSE/STI];
   - Utilizada nos textos descritivos dos mapas de riscos, temos dois tipos alternativos, exemplificados com base no item acima:
     - [ExTComVinc: (1) ex-funcionário em conluio com funcionário do TSE/STI];
     - [ExTComVinc: (1)]

CAA3: Externo Sem Vínculo com TSE/STI (Comunidades de Agentes ExTSemVinc):

- O agente de ameaça não tem vínculo formal algum com o TSE/STI nem com parceiros contratados;
- Pode ter ou não alguma informação privilegiada;
- Exemplo: (1) hackers, (2) ex-funcionários desenvolvedores de *software* ou gerentes sem ligação interna com o TSI, (3) hackers associados a mesários e presidente de mesa de seção eleitoral, (4) fiscais de partidos atuando no TSE, (5) auditores externos atuando no TSE/STI (por exemplo, os auditores desta Auditoria Especial), (6) mesários de seção eleitoral, (7) cidadão comum etc.

Observações:

a) Não se está acusando ou se insinuando que alguma pessoa específica que se enquadra em um dos tipos de agente de ameaça ExTSemVinc fez, faz ou fará qualquer tipo de ataque às urnas;
b) Isto apenas ilustra um reconhecimento que alguma pessoa que se enquadra em ExTSemVinc potencialmente poderá, em situações especiais e por motivação própria diversa ou sob coação de algum tipo, estar apta a perpetrar algum tipo de ataque às urnas;
c) A numeração acima é usada apenas para indicar de forma breve o tipo de agente de ameaça desta categoria; de nenhuma forma indica que os números de menor valor oferecem maior ameaça em comparação com os de maior valor, pois isso dependerá de cada tipo de *asset* e das correspondentes vulnerabilidades envolvidas com cada agente de ameaça;
d) Representação de comunidades de agentes de ameaça:
    - Utilizada nos diagramas representativos dos mapas de riscos: [CAA3: (nr. da subcomunidade)]; por exemplo, [CAA3:1], que representa [Comunidades de Agentes de Ameaça: ExTSemVinc; Subcomunidade: (1) hackers];
    - Utilizada nos textos descritivos dos mapas de riscos, temos dois tipos alternativos, exemplificados com base no item acima:
        - [ExTSemVinc: (1) hackers];
        - [ExTSemVinc: (1)]

A informação privilegiada é um diferencial entre agente interno (InT), externo com algum tipo de vínculo ao TSE/STI (ExTComVinc) e externo sem nenhum tipo de vínculo ao TSE/STI (ExTSemVinc). No geral, o agente InT ou ExTComVinc tem mais informação do que o agente ExTSemVinc. Mas o maior diferencial é o acesso físico ou virtual aos ambientes e recursos e também o acesso a mais informação, quando necessário. A maior oportunidade de acesso físico a ambientes, recursos e informação pode favorecer o agente a ter menos dificuldade para cometer uma fraude ou introduzir um “*backdoor*” no ambiente alvo, de acordo com a seguinte ordem do maior para o menor: InT >= ExTComVinc >> ExTSemVinc, onde “>=” significa “maior ou igual”, e “>>” significa “muito maior”.

5.3. Mapas de Riscos: Descrição Detalhada

Nesta seção, associamos, de acordo com o modelo de análise de riscos FAIR, uma comunidade de ameaça a cada um dos *assets* ou ativos das urnas eletrônicas. Em FAIR, no contexto de risco da informação, podemos definir *Asset* como qualquer dado, dispositivo ou outro componente do ambiente que apoia as atividades relacionadas com um sistema de informação, que podem ser ilicitamente acessados, usados, divulgados, alterados, destruídos ou roubados, resultando em perda de algum tipo para a instituição detentora do *Asset*.

A esse par (*asset*, ameaça), após a análise de riscos FAIR, obtemos um valor de Risco Geral. Para identificar o par nos diagramas ou mapas de riscos, agregamos um rótulo, aqui representado pelo termo ***Tag***, ao par. Um Tag, por sua vez, tem a seguinte estrutura: {[tag do Asset]:[tag da Comunidade de Ameaça]:[tag da Subcomunidade de Ameaça].

Dessa forma, um mapa de risco corresponderá a uma quádrupla formada por esses quatro elementos: [Tag:, Asset:, Comunidade de Ameaça:, Risco Geral:]!

Por exemplo, o primeiro mapa de risco analisado corresponde ao [Tag: **A1:CA-A2:2**, Asset: **Compilador Open Source GCC GNU**, Comunidade de Ameaça: **ExT-ComVinc: (2) hacker em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI**, Risco Geral: Crítico ou Catastrófico]. Esse mapa de risco pode ser representado de forma sintética da seguinte forma em alguns diagramas ou para referência textual: [**A1:CAA2:2**, Crítico], [**A1:CAA2:2**, C] ou apenas [**A1:CA-A2:2**] quando não se está interessado no valor do impacto.

Como definimos 11 assets no nosso estudo e 16 subcomunidades de agentes de ameaça, se fôssemos ser exaustivos, teríamos que contabilizar a apuração de 11x16 = 176 riscos ao *software* da urna.

Por limitação de tempo e de acesso a informações necessárias, iremos estudar apenas alguns riscos mais importantes. Para reduzir o número de estudos, associaremos a cada *asset* apenas uma subcomunidade para cada comunidade de agentes de ameaça listados na seção anterior, geralmente a subcomunidade que possuímos mais informação aplicável ao dado *asset*.

Como exceção e com o objetivo de ilustrar, associamos ao *asset* A1 três tipos diferentes de comunidades de agentes de ameaça.

Como resultado do estudo, encontramos 09 riscos do tipo Crítico ou Catastrófico, 01 de Médio a Crítico, 01 de Baixo a Médio e 02 Baixo, totalizando 13 riscos examinados.

A seguir descrevemos cada um dos 13 riscos identificados no presente trabalho. Começaremos nossa análise pelo agente de ameaça [**CAA2:2**] por ele apresentar maior potencial de explorar o *asset* A1 e ajudar a exemplificar melhor a aplicação da abordagem FAIR.

Tag	*Asset*	Comunidade de Ameaça	Risco Geral
A1:CAA2:2	A1: Compilador Open Source GCC GNU	ExTComVinc: (2) hacker em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI	Crítico ou Catastrófico

1 - Probabilidade de Ocorrência de Evento de Ameaça (Threat Event Frequency – TEF)

A TEF é a probabilidade de ocorrência, dentro de um determinado prazo, que um agente de ameaça vai entrar em contato e agir contra um ativo. A TEF é composta de dois fatores, Contato e Ação, pressupondo-se que a Ação só ocorrerá se houver antes algum tipo de Contato.

Para esta etapa, estamos definindo **TEF = VH** (*Very High* ou Muito Alta), por causa dos seguintes dois fatores:

- Contato = {Modo de Contato: Físico e Lógico, Tipo de Contato: Intencional} = VH, que é a probabilidade de ocorrência que um agente de ameaça, dentro de um determinado prazo, entrará em contato com o *asset*. O *hacker* tem contato lógico, o funcionário em conluio tem contato lógico e físico e ambos procuram intencionalmente o *asset* GCC para fraudá-lo de alguma forma;
- Ação = {Valor do Asset: VH, Nível de Esforço: L, Risco: L} = VH, que é a probabilidade de que um agente de ameaça agirá contra o *asset* uma vez que o contato ocorra!

Observações:

a) Considera-se a seguinte classificação para valores de Probabilidade de Ocorrência, lembrando que nesta análise é feito uso apenas dos valores como probabilidades, não como frequências:

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between .1 and 1 times per year
Very Low (VL)	< .1 times per year (less than once every ten years)

b) Considerando o fator Contato, tem-se os seguintes valores para cada subfator associado:
   - O Valor do *asset* tem valor VH, considerando-se sempre do ponto de vista do agente de ameaça: usando o compilador GCC, o agente de ameaça pode espalhar ao máximo a sua ameaça;
   - O Nível de Esforço para comprometer o *asset* é moderado ou M, dado que o código do GCC é aberto, não é auditado pelo TSE/STI e o agente de ameaça supõe-se ter nível de conhecimento alto o suficiente para manipular o GCC, além de nível de contato VH com o *asset*;
   - O Risco do agente de ameaça é baixo ou L, dado que a probabilidade de ocorrência de consequências negativas para o agente de ameaça ser baixa (L) – ou seja, tudo que ele fizer poderá ser mantido incógnito ou ser desfeito sem que o TSE/STI, com os controles atuais, tome conhecimento;

c) Dado que (i) o contato do agente de ameaça com o *asset* tem probabilidade de ocorrência muito alta (VH) e que a Ação contra o *asset* pelo agente de ameaça é facilitada pelo alto interesse em atuar no *asset*; (ii) não será muito difícil o agente de ameaça lidar com o *asset* (M); (iii) o risco do agente de ameaça de lidar com o *asset* é baixo (L), então pode-se considerar que a probabilidade de ocorrência do agente de ameaça do tipo [ExTComVinc, (2) *hacker* em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI] entrar em contato com o *asset* e agir contra o *asset* será muito alta (**VH**), pois os ganhos poderão ser altos e a possibilidade de sofrer sanções provavelmente será pequena;

d) Tanto o contato quanto a ação da comunidade de ameaça ExTComVinc é extremamente facilitada pelo seguinte:
   - O compilador GCC GNU é de domínio público com fontes abertos e bem documentados, possuindo um grande número de colaboradores voluntários;
   - Segundo despacho do Ministro, o TSE não tem controles de segurança sobre as versões de compiladores utilizadas;
   - O TSE, por meio da Resposta à Petição 17 desta Auditoria Especial, informa que "***Não há políticas estabelecidas pela instituição (TSE) de auditoria sobre esses compiladores"***! Foi informado que apenas "*a versão do compilador é atualizada, em geral, após a realização de cada eleição quando se inicia um novo ciclo de especificação e desenvolvimento de software*".

e) O nível de dificuldade de se alterar um compilador Open Source é baixo (L), pois o fonte é bem documentado e aberto, independentemente do tipo de agente de ameaça;
f) O nível de dificuldade de se introduzir uma "porta dos fundos", nesta alteração do compilador, é baixo, pois existem muitos pontos em que se pode colocar a "porta dos fundos", independentemente do tipo de agente de ameaça;
g) O nível de dificuldade de se introduzir diretamente uma fraude no compilador por uma comunidade de agentes de ameaça do tipo [ExTComVinc: (2)] é baixo (L), pois quanto mais informações privilegiadas, menos difícil de se introduzir diretamente uma fraude;
h) O nível de dificuldade de se introduzir uma fraude ou uma "porta dos fundos" no compilador utilizado, especialmente se tiver vínculo de colaboração com a comunidade livre de desenvolvedores do GCC GNU, é Moderado (M), pois é preciso fazer as modificações de maneira que não sejam facilmente percebidas e com grande antecedência em relação às datas das eleições.

2 - Capacidade de Ameaça (Threat Capability – TCAP)

A TCAP designa o nível provável de força que um agente de ameaça é capaz de aplicar contra um *asset*. Neste caso, estimamos que um agente de ameaça ExTComVinc apresenta **TCAP = H**; ou seja, que pelo menos 84% da comunidade de ameaça representada pelo [ExTComVinc: (2)] é capaz de aplicar uma força alta (H) contra (ou atacar) o compilador GCC GNU. Três motivos explicam essa possibilidade: (i) supõe-se que o agente de ameaça tenha forte conhecimento computacional; (ii) esse tipo de ataque nem é adequadamente catalogado na literatura; (iii) e o TSE/STI não

audita as versões atualizadas do compilador usadas no desenvolvimento do *software* da urna.

Considera-se a seguinte classificação para valores de capacidade de ameaça (TCAP):

Rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

3 - Força do Controle (Control Strenght – CS)

A CS designa a força de um controle de segurança de um *asset* para resistir à força que um agente de ameaça é capaz de aplicar contra o *asset*. Neste caso, estimamos que CS = **L**, por tudo que foi citado no item 1 acima. O valor L = Low, neste caso, indica que os controles de segurança do compilador GCC GNU e o seu acesso apenas protegem contra 16% da comunidade de ameaça representada pelo [ExTComVinc: (2)]. O fato do TSE/STI não auditar as versões atualizadas do compilador GCC GNU explicam o baixo valor de CS. O valor só não é mais baixo (VL = Very Low) porque a dificuldade de manipular o *asset* para produzir uma fraude ou introduzir um “backdoor” em si constitui uma forma de controle de segurança do *asset*.

Considera-se a seguinte classificação para valores de força do controle (CS):

Rating	Description
Very High (VH)	Protects against all but the top 2% of an avg. threat population
High (H)	Protects against all but the top 16% of an avg. threat population
Moderate (M)	Protects against the average threat agent
Low (L)	Only protects against bottom 16% of an avg. threat population
Very Low (VL)	Only protects against bottom 2% of an avg. threat population

4 - Vulnerabilidade (VULN)

No item 2 acima, examinamos o grau do agente de ameaça comprometer o *asset* (TCAP = H); e em 3, a capacidade do *asset* resistir à ameaça (CS = L).

Vulnerabilidade, de acordo com o modelo de análise de requisitos FAIR, é a probabilidade de que um *asset* será incapaz de resistir às ações de um agente de ameaça. Ou seja, TCAP e CS são fatores de VULN. Neste caso, uma vulnerabilidade existe quando há uma diferença entre a força sendo aplicada pelo agente de ameaça e a habilidade (ou a qualidade dos controles e salvaguardas de segurança) de um *asset* resistir àquela força.

Essa diferença é retratada pela tabela de Vulnerabilidade abaixo, onde o eixo vertical representa a TCAP e o eixo horizontal a CS. Assim, VULN = (TCAP = H, CS = L) = **VH**; ou seja, a vulnerabilidade do *asset* compilador GCC GNU em relação à comunidade de ameaça representada pelo [ExTComVinc: (2) *hacker* em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI] é muito alta ou VH.

5 - Probabilidade de Ocorrência de Evento de Perda (*Loss Event Frequency* – LEF)

A LEF é a probabilidade de ocorrência, dentro de um determinado período de tempo, de uma ação pelo agente de ameaça capaz de infligir danos em ou comprometer um *asset*. O método FAIR básica determina LEF através da tabela de consulta a seguir, que leva em consideração as dimensões “Probabilidade de Ocorrência de Evento

de Ameaça” (“Threat Event Frequency – TEF) e “Vulnerabilidade” (“Vulnerability” – VULN).

Para esta etapa, foi definido **LEF = VH**, porque, de acordo com a fase 1, TEF = VH, e, de acordo com a fase 4, VULN = VH resultando no valor conforme a tabela.

6 - Estimativa de Perda do Pior Caso (*Worst-Case Loss* – WCL)

A partir desta fase, descreve-se a outra metade da equação de risco: os fatores que impulsionam a perda de magnitude quando ocorrem eventos de ameaça. Pelo modelo de análise de riscos FAIR básico, existem dois tipos de perda: pior caso (WCL) e perda provável (ou esperada – PLM). Nesta fase será tratado o WCL. O FAIR pede para determinar a ação de ameaça (*threat action/event*) que mais provavelmente resultaria em um resultado de pior caso, estimar a magnitude para cada forma de perda (*loss form*) associada a essa ação de ameaça, e “somar” a magnitude de perda resultante.

A perda potencial de um *asset* deriva do valor que ele representa para uma organização ou da responsabilidade que o valor do *asset* atrela a uma organização. Ou seja, a perda é sempre avaliada da perspectiva da organização sob análise. Por exemplo, embora clientes possam se prejudicar pelo roubo de informação pessoal, a análise nesta fase se centra em verificar o grau de perda experimentada pela organização em vez de se preocupar com as perdas experimentadas pelos clientes.

Seis formas de perda são definidas dentro do FAIR: produtividade (*productivity*), resposta (*response*), substituição (*replacement*), multas e decisões judiciárias (*fines/judgments*), vantagem competitiva (*competitive advantage*) e reputação (*reputation*).

Todos os fatores de perda caem dentro de uma das quatro categorias seguintes: *asset*, ameaça, organização e externo. Fatores de perda de *asset* e de ameaça são referidos como fatores de perda primários ou principais, enquanto fatores de perda de organização e externos são referidos como fatores de perda secundários. Por isso, para definir o Impacto Provável da Perda (*Probable Loss Magnitude* – PLM), FAIR define dois grupos de fatores de perda: Principal (*Primary*) e Secundária (*Secondary*).

Por simplicidade e pelo fato da Auditoria Especial ter sido impedida de realizar as análises devido às restrições da auditoria impostas pelo TSE, aqui não se analisam os fatores de perda organizacional e de perda externa, que compõem os Fatores de Perda Secundária (*Secondary Loss Factors*). Com isso, ao estimar o WCL dos Fatores de Perda Secundária, o que está sendo definido é o WCL do impacto ou magnitude da perda.

Os Fatores de Perda Principais são compostos por Fatores de Perda do Asset e Fatores de Perdas de Ameaças. Os Fatores de Perda do *Asset* são constituídos pelos seguintes subfatores: Valor e Volume. O subfator Valor é descrito por Criticidade, Custo e Sensibilidade, do ponto de vista da organização. A Criticidade diz respeito ao impacto que o *asset* comprometido pode ter na produtividade da organização; o Custo, com as despesas associadas a substituir ou consertar um asset comprometido; e a Sensibilidade, com o impacto resultante do *asset* comprometido expor informação confidencial ou anonimato, por exemplo.

No caso do *asset* GCC GNU, a Criticidade é VH, pois o *asset* comprometido poderá ser usado no mínimo para sabotar uma eleição; o Custo poderá ser H para substituir o compilador, pois envolverá auditoria sofisticada para provar que a versão nova do Compilador GCC GNU não estará comprometida; e a Sensibilidade é VH, pois informação sigilosa, como o voto do eleitor, poderá ser exposta e/ou alterada. Considerando então o valor do pior caso, o subfator Valor = {Criticidade = VH, Custo = H, Sensibilidade = VH} = VH.

O subfator Volume simplesmente reconhece que mais versões do *asset* em risco fariam o impacto da perda maior. Embora apenas uma versão do GCC GNU seja empregada em cada eleição pelo TSE/STI, essa versão será distribuída e utilizada por

todo o STI, aumentando o grau do impacto ou magnitude da perda potencial. Assim, o subfator Volume = VH.

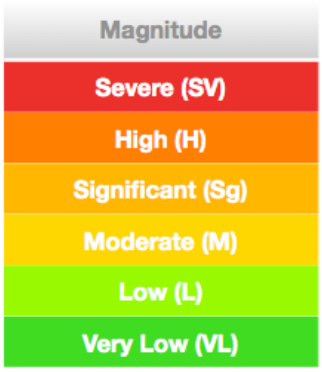
Assim, tem-se que os Fatores de Perda do *Asset* = {Valor = VH, volume = VH}. Considerando o valor do pior caso, o valor de Fatores de Perda do *Asset* = VH.

Os Fatores de Perda das Ameaças é composto de três subfatores: Ação, Competência em Agir, Agente Interno versus Externo. Como esses dois últimos subfatores foram aqui usados para definir as Comunidades de Agentes, eles serão desconsiderados neste ponto.

Os agentes de ameaça podem assumir uma ou mais das seguintes ações contra um *asset*:

- Acessar – Acesso não autorizado simples
- Usar indevidamente – Utilização não autorizada de *assets*
- Divulgar – O agente de ameaça divulga ilicitamente informações confidenciais
- Modificar – Alterações não autorizadas ao *asset*
- Negar acesso – Inclui a destruição, roubo de um *asset* não dados, etc.

A seguinte tabela será usada para mensurar probabilidades de impacto ou magnitude, sem considerar faixas de valores financeiros decorrentes dos impactos, como usual no FAIR:



O diagrama a seguir é usado para se exibir as estimativas de formas de perdas para cada tipo de ações de ameaças, ajudando a se definir as perdas de pior caso. No caso do *asset* GCC GNU, apenas a ação de ameaça Modificar é a que faz mais sentido.

Estimamos que a forma de perda *Fine/Judgments* é H (High), pois se o *asset* for comprometido e o julgamento ocorrer em um tribunal diferente, por suposição, a organização TSE/STI poderia ser condenada a multas e decisões judiciais de grande valor

financeiro, por causa de eventuais problemas com eleições fraudadas ou no mínimo sabotadas.

Estimamos que a forma de perda Reputation é SV (Severe), pois se o *asset* for comprometido e se provar esse comprometimento (que ao final leve à introdução de fraude ou “porta dos fundos” e se comprove eventual resultado indevido numa eleição ou sabotagem virtual que atrapalhe a eleição), a reputação da organização TSE/STI poderia ser severamente abalada.

Estimamos que a forma de perda *Competitive Advantage* também poderia ser SV, pois o *asset* comprometido poderia atrapalhar eventual vantagem competitiva das urnas brasileiras. Estimamos que as demais formas de perdas são VL (*Very Low*) ou insignificantes se o *asset* for comprometido.

	Loss Forms					
Threat Actions	Productivity	Response	Replacement	Fine/Judgments	Comp. Adv.	Reputation
Access						
Misuse						
Disclosure						
Modification	VL	VL	VL	H		
Deny Access						

Como resultado, a perda no pior caso ou **WCL = SV** para os Fatores de Perda Principal (*Primary Loss Factors*) e, em consequência, o WCL do impacto ou magnitude da perda também será **SV**!

7 - Impacto Provável da Perda (Probable Loss Magnitude = PLM)

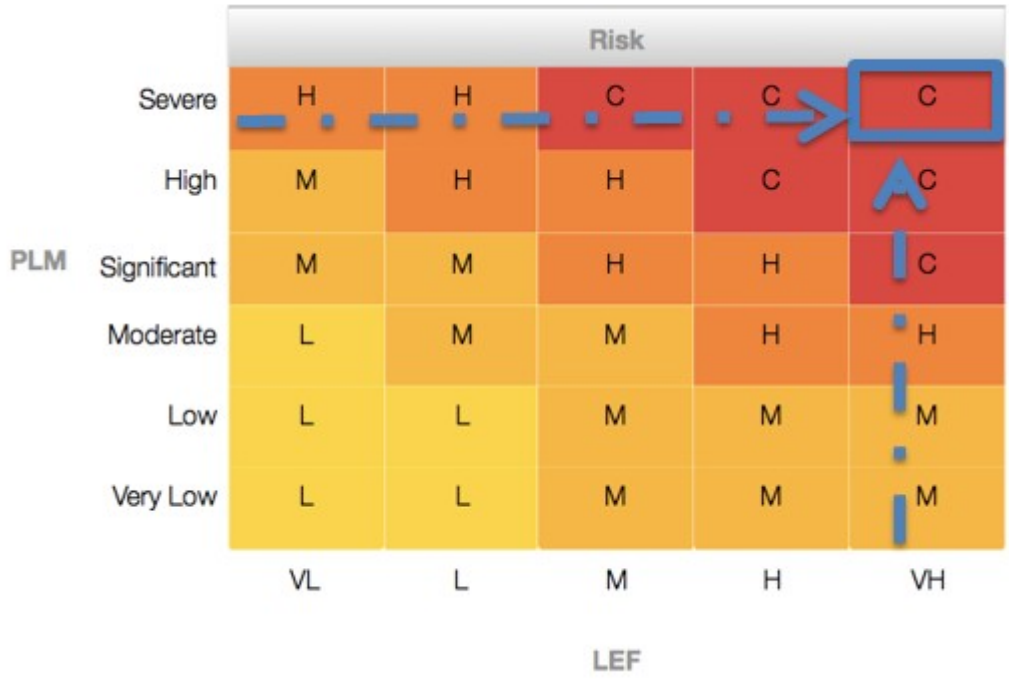
Lembre-se que o Impacto Provável de Perda ou PLM será representado apenas pelos Fatores de Perda Principal. O FAIR pede para determinar a ação de ameaça mais provável de ocasionar de um resultado esperado, estimar a magnitude para cada forma de perda associada a essa ação de ameaça, e "somar" a magnitude ou impacto da perda.

A Perda provável é para a maior parte da análise e sempre vai ser menor que ou igual à perda do "pior caso". Neste caso, vai ser igual ao cálculo feito no item anterior para o pior caso (WCL), por falta de informações decorrente das limitações da audito-

ria imposta pelo TSE. Ou seja, o valor mais provável dos Fatores de Perda Principal será igual a **SV**, de modo que, por consequência, o Impacto Provável da Perda é dado por **PLM = SV**.

8 - Derivar o Risco Geral

Considerando o *asset* GCC GNU e a comunidade de ameaça [ExTComVinc: (2) hacker em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI], o risco geral é dado pela tabela a seguir que mescla a Probabilidade de Ocorrência de Evento de Perda ou **LEF = VH** e o Impacto Provável da Perda ou **PLM = SV**



Como resultado, o **Risco Geral é igual a Crítico (C)**, conforme tabela também abaixo com valores de risco. Em alguns modelos e arcabouços de riscos o Risco Crítico equivale a Catastrófico ou Gravíssimo, que dá uma perspectiva mais realista do grau de problemas decorrentes.

Key	Risk Level
C	Critical
H	High
M	Medium
L	Low

9 - Comentários Complementares

a) Possibilidade de detecção após a introdução da fraude ou do "backdoor":

- Muito baixa, mesmo que o TSE/STI melhore muito os controles de segurança e nível de auditoria atuais da urna.

b) Facilidade de distribuição:

- Fraude direta:
  - Muito alta, pois poderá atingir a totalidade dos programas compilados pelo TSE.
- Explorar a “porta dos fundos”:
  - Moderada, pois a “porta dos fundos” facilitaria muito a introdução de uma fraude, mas continuaria sendo necessário instalar a fraude propriamente dita em outro ponto.

c) **Potencial de danos: Catastrófico**

- Se a fraude for bem feita, será praticamente impossível detectá-la com o nível de auditoria interna atual;
- Poderá com facilidade alterar o resultado de uma eleição ou no mínimo promover uma sabotagem impedindo a realização do pleito!

d) Agravantes do potencial de danos:

Caso o agente de ameaça [ExTComVinc: (2) hacker em conluio com funcionário do TSE/STI] também seja colaborador da comunidade de desenvolvimento do *software* livre Compilador GCC GNU, o cenário ficará mais crítico, pois o seguinte poderá acontecer:

i) A fraude poderá ser utilizada em mais de uma eleição.

ii) Uma “porta dos fundos” bem elaborada não dependerá de uma eleição isolada, de modo que será mais eficiente fraudar inúmeras eleições.

iii) Uma associação do "backdoor" e da fraude direta poderá potencializar os danos.

iv) O Compilador GCC GNU poderia apresentar “portas dos fundos” previamente instaladas para uso genérico (ilação possível, pois até a Microsoft e a Intel já confirmaram ter feito uso de “porta dos fundos” em seus sistemas operacionais e microprocessadores, respectivamente), o que facilitaria o trabalho do agente de ameaça em criar uma “porta dos fundos” específica ou instalar uma fraude acoplada mais facilmente ainda.

e) **Conclusão sobre o *asset* Compilador GCC GNU comprometido pelo agente de ameaça [ExTComVinc: (2) hacker em conluio com funcionário do TSE/STI]:**

O Risco resultante é Crítico/Catastrófico/Gravíssimo devido ao seguinte:

- Será relativamente fácil de se fazer e introduzir uma fraude no *asset*, bem como distribuí-lo por todo o TSE/STI.
- Existe um potencial enorme de causar danos, que poderão variar de uma simples (mas nociva) sabotagem até a possibilidade de se mudar os resultados de uma eleição!
- Poderá ser usado em conjunto com outros assets comprometidos.
- Potencial existência prévia de “portas dos fundos” que não foram desenvolvidas para as eleições brasileiras, mas poderiam ser explorados para facilitar a execução de diversos tipos de fraude.
- A auditoria e fiscalização permitida aos partidos pelo TSE/STI é insuficiente para detectar uma fraude que explore as vulnerabilidades deste *asset*.
- O TSE/STI confirmou que não realiza auditoria específica (Resposta à Petição 17 desta Auditoria Especial) capaz de verificar se o asset Compilador GCC GNU está comprometido ou não.

- Pelo que notou-se quando da avaliação do *software* da urna, devido aos problemas de inadequação da metodologia de desenvolvimento empregada e da documentação do *software* produzido, bem como pela confissão documentada do TSE/STI de não realizar auditoria de *software*s de terceiros usados na urna (Resposta à Petição 17 desta Auditoria Especial), em especial do *software* de criptografia do CEPESC que, além disso, não se encontrava no CD lacrado com o *software* da Eleição de 2014, conclui-se que requer-se dos desenvolvedores do TSE/STI treinamento adequado para realizar o tipo de auditoria delineado no item anterior.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A1:CAA1:1	A1: Compilador Open Source GCC GNU	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) Nível de dificuldade de se introduzir diretamente uma fraude no compilador:

- Baixo, pois quanto mais conhecimento sobre o sistema alvo, mais fácil de introduzir diretamente uma fraude!

b) Nível de dificuldade de se introduzir uma fraude ou "porta dos fundos" no compilador utilizado:

- Baixo, pois quanto mais livre o acesso ao compilador, mais fácil de introduzir uma fraude ou uma "porta dos fundos". Além disso, o agente de ameaça [InT: (1)] não necessitará de muita antecedência em relação às eleições, em comparação com a necessidade do agente de ameaça do risco anterior, [ExTComVinc: (2)].

c) Para evitar redundância no texto, assume-se como aplicáveis para este mapa de risco todos os comentários complementares de a) a e) do Item 9 do mapa de risco [A1:CAA2:2] acima, uma vez que os agentes de ameaça [InT: (1)] e [ExTComVinc: (2)] são assemelhados em termos de poder de ameaça.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A1:CAA3:1	A1: Compilador Open Source GCC GNU	ExTSemVinc: (1) hacker	Baixo (L)

Comentários Complementares:

a) Nível de dificuldade de se introduzir diretamente uma fraude no compilador:

- Alto, pois quanto menos conhecimento sobre o sistema alvo, mais difícil de introduzir diretamente uma fraude!

b) **Nível de dificuldade de se introduzir uma fraude ou "porta dos fundos" no compilador utilizado:**

- Alto, pois, embora o acesso ao compilador seja fácil, pois ele é *software* livre, introduzir uma fraude ou uma "porta dos fundos" não será uma tarefa fácil, uma vez que dependerá do acesso do agente de ameaça à(s) máquina(s) utilizadas antes da compilação oficial pois quanto mais livre.

b) Estimativas iniciais: TEF = L; TCAP = L; CS = H; VULN = VL

c) A estimativa de perda do pior caso ou WCL é M ou Moderado; mas o efeito provavelmente seria no máximo conseguir sabotar a eleição, provavelmente sem conseguir modificar o resultado da eleição.

d) Estimamos a Probabilidade de Ocorrência de Evento de Perda ou LEF = VL e o Impacto Provável da Perda ou PLM = L. Dessa forma, o **Risco Geral**, ilustrado na tabela a seguir, é **Baixo ou L**.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A2:CAA1:1	A2: Certificados Digitais	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) **Problemas identificados no esquema de certificados digitais usado na urna:**

- Não se permite qualquer verificação ou auditoria externa.
- Falta o mecanismo de *timestamp*, para reforçar os controles de segurança dos certificados. *Timestamp*, ou marca temporal em português, é uma cadeia de caracteres denotando a data e hora do dia que certo evento ocorreu, às vezes com uma precisão de uma pequena fração de segundo.
- O TSE é a certificadora raiz e seus certificados não são públicos, por isso os certificados do TSE não podem ser conferidos por terceiros, quer sejam fiscais de partidos ou qualquer outro fiscal externo ao TSE e seus contratados.
- Os certificados digitais são usados de forma *off-line*.
- As assinaturas digitais são utilizadas como um dos elementos mais importantes na segurança de todos os processos e elementos do sistema. Porém, as urnas não estão conectadas para se fazer uma verificação de assinatura de uma forma mais segura. Ou seja, as verificações são feitas na própria urna, com base apenas nos dados internos que, em dado momento, podem ter sido falsificados.

b) Nível de dificuldade de se obter uma chave privada ou utilizá-la de maneira indevida:

- Baixo, pois o sigilo das chaves privadas, em última análise, fica sob a guarda de pessoas, direta ou indiretamente.

c) Nível de dificuldade de se fraudar a cadeia de confiança da certificação utilizada nas urnas:

- Se o agente de ameaça [InT: (1)] for:

1) Externo à certificadora do TSE:

- Moderado, pois quanto mais informação privilegiada, mas fácil será possível se alterar o certificado raiz utilizado nas urnas.

2) Interno à certificadora do TSE:

- Baixo, pois, com informação e acesso privilegiado, pode-se facilmente gerar e introduzir certificados válidos, mas não oficiais, para se aceitar uma possível fraude ou utilização de algum código malicioso.

3) De qualquer forma, o fato de o agente de ameaça [InT: (1)] ser interno ou externo à certificadora do TSE não altera o Risco Geral apurado.

d) Possibilidade de detecção de uso indevido de uma chave privada:

- Muito baixa, uma vez que obtida uma chave privada, não se tem como saber, apenas pela assinatura, quem a fez. Qualquer detecção é muito difícil e, se houver, será apenas de forma indireta. Tudo isso é muito agravado pela falta de *timestamping* na geração das assinaturas, cujo uso poderia fornecer um indício para se começar a trabalhar a questão.

e) Possibilidade de detecção de uma cadeia de confiança alterada:

- Muito baixa, pois, se o certificado raiz foi alterado, a própria urna não será capaz de detectar tal ação. Além disso, não existe a transparência necessária para fiscais externos poderem fazer verificações e auditorias independentes.

f) Facilidade de distribuição:

- Muito alta, pois, uma vez gerada uma assinatura que a urna aceite como correta, o código hostil será distribuído pelos mecanismos oficiais de distribuição dos sistemas da urna.

g) Potencial de danos:

- Muito alto, pois será praticamente indetectável pela urna, com os mecanismos de segurança atuais.
- Embora em alguns pontos se utilize do *hash* para se tentar detectar um código hostil, em vários pontos o desconhecimento da chave privada pelo agente da ameaça é a única real segurança existente.
- Pode com facilidade propiciar a alteração do resultado de uma eleição.

h) **Agravante do potencial de danos:**

1) O projeto de segurança do sistema eleitoral é baseado em assinaturas digitais, mas o uso delas é praticamente só interno aos próprios sistemas, o que dificulta ou inviabiliza qualquer auditoria nessas assinaturas digitais.
2) O próprio TSE não tem um mecanismo eficiente, externo à própria urna eletrônica, de se verificar as assinaturas digitais efetivamente utilizadas.
3) Tanto as assinaturas digitais quanto os *hashes* são testados pela própria urna. Isto caracteriza mais um autoteste do que realmente uma verificação de segurança, pois não se evita que um possível código hostil simplesmente simule que fez as verificações necessárias.
4) Não existe um mecanismo externo de verificação de *timestamping* para realmente identificar, de forma precisa e sem ambiguidades, em que momento (data e hora) uma assinatura digital foi realmente feita.

i) **Conclusão sobre o asset Certificados Digitais comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:**

O Risco resultante é Crítico/Catastrófico/Gravíssimo devido ao seguinte:

- Permite o controle quase completo dos *software*s que serão executados nas urnas.
- Tem um potencial muito alto de causar danos graves ao funcionamento do *software* da urna.
- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça.
- Tanto a auditoria quanto a fiscalização permitida aos partidos é insuficiente para se detectar uma fraude que explore certificados digitais comprometidos pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI].

Tag	Asset	Comunidade de Ameaça	Risco Geral
A3:CAA1:1	A3: Sistema Operacional	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) Problemas identificados:

- O sistema operacional utilizado (Linux) é *Open Source*, o que facilita se planejar a introdução e funcionalidades de um código hostil, diminuindo a necessidade de se fazer engenharia reversa.
- Embora grande parte do sistema operacional seja derivada de código *Open Source*, o *software* da urna é um *software* proprietário, em que o acesso aos seus códigos fonte e executável é restrito. Como resultado, isso dificulta-se muito a fiscalização e auditoria do sistema operacional.
- Como o número de usuários frequentes do sistema operacional é bastante reduzido, a testabilidade do sistema operacional como um todo fica prejudicada.

b) Nível de dificuldade de se introduzir um código hostil no sistema operacional:

- Muito baixo, pois quanto mais informação privilegiada e mais fácil acesso ao ambiente de desenvolvimento, mais facilidade em se introduzir um código hostil no sistema operacional. Inclusive, pode-se introduzir um código hostil sem a necessidade de se quebrar uma única verificação ou controle de segurança.

c) **Nível de dificuldade de se utilizar uma falha de segurança ou *bug* existente na versão do Linux inicialmente utilizada pelo TSE:**

- Moderado, pois é necessário se encontrar a falha a ser explorada e introduzir um código hostil para se explorar essa falha.
- **Atenuante**: Explorar a falha existente pode ser desnecessário, já que continua havendo a necessidade de se introduzir um código hostil. Ou seja, o código hostil já poderia fraudar por si só, sem a necessidade de se explorar uma falha preexistente.

d) **Nível de dificuldade de se introduzir um código hostil em um novo *device driver* para o Sistema Operacional:**

- Muito baixo, pois quanto mais informação privilegiada e mais fácil acesso ao ambiente de desenvolvimento e informações sobre o novo hardware, maior a facilidade em introduzir um código hostil sem inviabilizar as funcionalidades básicas do *device driver*.

e) Facilidade de distribuição:

- Muito alto, pois pode-se simplesmente substituir a versão original do sistema operacional, sendo calculado o "hash" e assinado digitalmente já com o código hostil introduzido.

f) Potencial de danos:

- Introdução de código hostil no sistema operacional:
  - Muito alto, pois, se a fraude for bem-feita, será praticamente impossível de se detectar com o nível de fiscalização e auditoria atual
  - Poderá com facilidade propiciar a alteração do resultado de uma eleição.
- Utilizar uma falha já existente:
  - Baixo, pois não é o caminho mais fácil de se introduzir uma fraude via sistema operacional.
- Fraude em um novo *device driver* para o sistema operacional:
  - Muito alto, principalmente se for introduzida por quem faça parte da equipe responsável pela implementação do novo *device driver*, pois dificilmente alguém fora da equipe será capaz de descobrir este tipo de fraude.
  - Poderá com facilidade propiciar a alteração do resultado de uma eleição.

g) Agravante do potencial de danos:

- Uma fraude instalada num sistema operacional poderá ser utilizada em mais de uma eleição, enquanto não se mudar a versão.
- Esta fraude poderá facilmente ser associada a outros tipos de fraudes.

h) **Conclusão sobre o *asset* Sistema Operacional comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:**

O Risco resultante é Crítico/Catastrófico/Gravíssimo devido ao seguinte:

- Um código hostil introduzido no sistema operacional poderá fazer praticamente tudo que o agente de ameaça desejar, de forma escondida e possivelmente com autorremoção, interferindo em toda leitura e gravação da memória *flash*.
- Tem um potencial muito alto de causar danos graves ao funcionamento do *software* da urna.
- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça.
- Tanto a auditoria quanto a fiscalização permitida aos partidos é insuficiente para se detectar uma fraude que explore o sistema operacional comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI].

Tag	Asset	Comunidade de Ameaça	Risco Geral
A4:CAA1:1	A4: Processo de Compilação	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) **Problemas identificados:**

- Os códigos fontes compilados são muito grandes para as reais funcionalidades necessárias.
- São utilizados vários *scripts* diferentes durante a compilação, sem uma justificativa convincente para tal utilização.
- Utiliza-se um compilador já particularmente exposto (vide *asset* A1), potencialmente comprometido!
- O tempo de compilação é relativamente grande (entre dezenas de horas a dias) sem uma explicação plausível.

b) **Nível de dificuldade de se alterar algum *software* ou introduzir um código hostil durante a compilação:**

- Muito baixo, pois, quanto maior o conhecimento dos diferentes *scripts* de compilação e maior o conhecimento do processo de compilação como um todo, mais fácil de se fazer uma adulteração ao *software* da urna.
- Uma dificuldade é a necessidade de se ter o acesso antecipado ao ambiente de compilação.

c) **Facilidade de distribuição:**

- Muito alta, pois, uma vez introduzida a fraude durante a compilação, o produto compilado será a versão oficial do *software* da urna do TSE.

d) **Potencial de danos:**

- Muito alto, pois irá para todas as urnas e computadores utilizados no processo das eleições.
- Poderá com facilidade propiciar a alteração do resultado de uma eleição.

e) Agravante do potencial de danos:

i. A compilação é um momento muito difícil de ser auditado. Seria necessário que os fiscais pudessem repetir a compilação em outros ambientes e chegassem em produtos compilados idênticos.

ii. A compilação teria que ser configurada de tal forma a ser determinística, de modo que, sempre que se repetisse a mesma compilação, o resultado compilado deveria ser o mesmo.

f) Conclusão sobre o asset Processo de Compilação comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:

O Risco resultante é Crítico/Catastrófico/Gravíssimo devido ao seguinte:

- Tem um potencial muito alto de causar danos graves ao funcionamento do *software* da urna.
- Em comparação com outros possíveis ataques, sua implementação faz uso de tecnologia de baixo nível. O mais importante ao agente de ameaça é ter acesso ao ambiente de compilação.
- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça.
- Tanto a auditoria quanto a fiscalização permitida pelo TSE é insuficiente para se detectar uma fraude que explore o processo de compilação comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI].

Tag	Asset	Comunidade de Ameaça	Risco Geral
A5:CAA2:6	A5: BIOS	ExTComVinc: (6) ex-funcionário desenvolvedor de *software* do TSE/STI em conluio com funcionário de fabricante que desenvolve o BIOS	Crítico ou Catastrófico

Comentários Complementares:

a) **Problemas identificados:**

- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça [CAA2:6].
- Existem diferentes versões de BIOS para diferentes modelos de urnas.
- Existem extensões de BIOS introduzidas pelo TSE e contratados.
- No contexto da Auditoria Especial do PSDB, não se permitiu fiscalização e/ou auditoria nas versões de BIOS utilizadas no *software* da urna.
- O BIOS é o primeiro código executável a ser executado na urna.
- O BIOS pode ser acessado diversas vezes durante o funcionamento da urna.
- A arquitetura de hardware utilizada na urna eletrônica é basicamente a arquitetura PC, com poucas alterações.

b) Nível de dificuldade de se introduzir um código hostil no BIOS:

- Muito baixo, pois, uma vez que o agente de ameaça tenha acesso ao código fonte do BIOS, será fácil introduzir o código hostil ou um *backdoor* para ser explorado por outra fraude associada.

c) Facilidade de distribuição:

- Muito alto, pois quem tem acesso para fazer a alteração antes do BIOS ser inseminado nas urnas terá a fraude distribuída pelos mecanismos do fabricante.

d) Potencial de danos:

- Muito alto, pois a fraude será incorporada ao hardware de cada urna do TSE.
- Poderá com facilidade propiciar a alteração do resultado de uma eleição.

e) Agravante do potencial de danos:

i) A fraude existirá durante toda a vida útil da urna ou até uma BIOS nova e eventualmente não comprometida ser instalada.

ii) Uma “porta dos fundos” (*backdoor)* bem elaborada não depende de uma eleição específica e, por isso, é mais eficiente em fraudar inúmeras eleições.

iii) Uma associação da “porta dos fundos” (*backdoor)* e de uma fraude direta instalada poderá potencializar os danos.

f) **Conclusão sobre o asset BIOS comprometido pelo agente de ameaça [ExTComVinc: (6) ex-funcionário desenvolvedor de *software* do TSE/STI em conluio com funcionário de fabricante que desenvolve o BIOS]:**

O Risco resultante é Crítico/Catastrófico/Gravíssimo devido ao seguinte:

- O *asset* BIOS comprometido pelo agente de ameaça tem um potencial muito alto para causar danos.
- O comprometimento do *asset* BIOS será quase impossível de ser detectado com o nível de fiscalização e auditoria permitido pelo TSE.
- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A6:CAA3:3	A6: Visual da Urna e da Interface do Usuário	ExTSemVinc: (3) hackers associados a mesários e presidente de mesa de seção eleitoral	Baixo a Médio

Comentários Complementares:

a) Problemas identificados:

- O visual da urna e da interface do usuário é um *asset* suscetível de clonagem pelo agente de ameaça [CAA3:3].
- Não existe um procedimento de verificação de clonagem da urna definido e autorizado pelo TSE.
- Foi possível simular o não rompimento do lacre de algumas das urnas auditadas.
- Não há um procedimento de controle de acesso à urna pelos mesários e presidente de seção eleitoral.

b) Nível de dificuldade de fazer uma urna com a mesma aparência da urna oficial:

- Muito baixo, pois não é um problema técnico e sim mecânico e estético. Além disso, o *software* da urna falsa é simples de implementar.

c) Facilidade de distribuição:

- Muito baixa, pois a substituição será urna a urna.
- Além disso, deve-se fazer uma votação simulada na urna real, fazendo uso dos mesmos resultados já programados na urna falsa, para se obter documentos assinados que sejam válidos.

d) Potencial de danos:

- Baixo, pela dificuldade de logística e distribuição.

e) Agravante do potencial de danos:

i) Em eleições municipais, poucas urnas são suficientes para uma fraude mudar o resultado das eleições.

f) **Conclusão sobre o *asset* "Visual da urna e da interface do usuário" comprometido pelo agente de ameaça [ExTSemVinc: (3) *hackers* associados a mesários e presidente de mesa]:**

O Risco resultante é Baixo a Médio devido ao seguinte:

- Para eleições estaduais e nacionais:
  - Baixo, pois dificilmente poderá mudar o resultado de uma eleição.
- Para eleições municipais
  - Médio, pois, embora seja difícil distribuir e implementar, para eleição em pequenas cidades pode ser suficiente, uma vez que poucas urnas clonadas poderão mudar o resultado da eleição.
- Reconhece-se que este risco específico precisa ter seus elementos melhor avaliados. Contudo, a sua presença nesta lista de riscos é ilustrativa dos riscos que a urna como um todo é portadora.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A7:CAA1:1	A7: Rotinas de Segurança do CEPESC	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) Problemas Identificados:

- Foi constatado pela equipe técnica de auditoria que os códigos desenvolvidos pelo CEPESC não foram lacrados após o processo de compilação para as eleições de 2014.
- O CEPESC tem alguma participação ––que não foi bem explicada aos auditores–– na Certificadora do TSE.
- O CEPESC troca a criptografia do BU a cada ciclo eleitoral, quando o normal seria manter os códigos fontes praticamente inalterados e apenas trocar as chaves criptográficas de uma eleição passada por outras (eventualmente mais fortes) para a próxima eleição.
- A criptografia do BU é desnecessária, pois o dado já é público. Basta assinar digitalmente o BU.

b) Nível de dificuldade de se introduzir um código hostil nas rotinas do CEPESC:

- Muito baixo, pois é a mesma dificuldade de se alterar qualquer código fonte que já faça parte do sistema da urna.

c) Facilidade de distribuição:

- Muito alto, pois as alterações podem ser feitas diretamente no código fonte das rotinas do CEPESC entregue ao TSE.

d) Potencial de danos:

- Muito alto, pois as rotinas do CEPESC são chamadas com frequência durante a votação e, ao seu final, na geração do BU. Pode-se alterar os resultados ali gravados com facilidade.
- Poderá com facilidade propiciar a alteração do resultado de uma eleição.

e) **Conclusão sobre o *asset* "Rotinas de Segurança do CEPESC" comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:**

O Risco resultante é Crítico ou Catastrófico devido ao seguinte:

- Será muito fácil criar e distribuir o *asset* comprometido.
- O comprometimento do *asset* será quase imperceptível nas auditorias de código fonte autorizadas pelo TSE.
- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça.
- Tanto a auditoria quanto a fiscalização permitida aos partidos pelo TSE é insuficiente para se detectar uma fraude que explore o *asset* comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI].

Tag	Asset	Comunidade de Ameaça	Risco Geral
A8:CAA1:1	A8: *Software* da Urna para Votação Paralela	InT: (1) desenvolvedores de *software* do STI	Médio a Crítico ou Catastrófico

Comentários Complementares:

a) Problemas identificados:

- O *Software* da Urna para Votação Paralela cria a falsa sensação que o sistema está sendo realmente testado.
- Pela auditoria nos TREs, constatou-se que algumas votações paralelas não seguiram os ritos previstos, oferecendo oportunidades para o *Software* da Urna para Votação Paralela perceber que estava ocorrendo uma votação paralela, não uma votação real.
- Como o *asset* foi implementado pelo TSE e não foram contados manualmente os votos introduzidos na urna de teste, a votação paralela é simplesmente um teste de sincronismo entre 2 programas: o que roda na urna e o que roda no computador de apuração paralela.

b) Nível de dificuldade de se enganar o teste de Votação Paralela:

- Urnas com biometria:
  - Muito baixo, pois é facilmente detectável que a biometria está sendo ignorada, ou seja, que a urna está sob teste.
- Urnas sem biometria:
  - Moderado, pois existem vários possíveis critérios para se detectar que está ocorrendo uma Votação Paralela, mas nenhum é 100% confiável.
  - Por isto, para que o código malicioso diminua o risco de acabar falhando no teste, é prudente se fraudar o *software* que executa no computador de apuração, mantendo sincronizadas as fraudes.
  - Podem-se criar também gatilhos manuais para avisar que determinada urna está sendo submetida à Votação Paralela.

c) Potencial de danos:

- Urnas com biometria:
  - Muito alto, pois será fácil para o código hostil descobrir que está sendo submetido à Votação Paralela.
- Urnas sem biometria:
  - Médio, pois é possível enganar o teste, mas a fraude se torna mais complexa.

d) **Conclusão sobre o asset "*Software* da Urna para Votação Paralela" comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:**

O Risco resultante é Médio a Crítico ou Catastrófico devido ao seguinte:

- Urnas com biometria:
  - Catastrófico, pois o teste é praticamente inútil para as urnas com biometria.
- Urnas sem biometria:
  - Médio, pois esse é um teste que ajuda a diminuir a gravidade de todas as outras possíveis fraudes, uma vez que praticamente obriga o código hostil a fazer duas ações básicas: fraudar as eleições e enganar a Votação Paralela.
  - Existem formas de se detectar e se evitar a Votação Paralela, mas isso exige que a fraude seja mais elaborada em relação ao caso das urnas com biometria.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A9:CAA1:1	A9: Hardware de segurança (MSD)	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) Problemas Identificados:

- O *asset* corresponde a uma caixa preta agregada à arquitetura de hardware das urnas a partir do modelo de 2009.
- Até o momento, o *asset* é uma caixa preta não auditável.

b) Nível de dificuldade de fraudar o MSD:

- Baixo, pois quem tem acesso à inicialização do *software* desse componente, ou a atualizações, poderá introduzir uma “porta dos fundos” (*backdoor)* ou até mesmo uma fraude completa.
- Se bem feita, será indetectável inclusive por outras pessoas internas ao processo.

c) Nível de dificuldade de se enganar o MSD:

- Baixo, pois, conhecendo-se corretamente a ação do *hard lock* (que impede a execução do processador principal), pode-se simular corretamente o que o componente espera, mesmo tendo um código hostil sendo executado.

d) Facilidade de distribuição:

- Muito alta, pois a fraude no componente será executada antes de um processo automático de inicialização ou atualização.

e) Potencial de danos:

- Muito alto, pois o MSD controla o processo de inicialização das urnas, podendo permitir a entrada de código hostil.
- Poderá com facilidade propiciar a alteração do resultado de uma eleição.

f) Agravante do potencial de danos:

i) O componente MSD e o *software* que é executado nele não podem ser auditados e verificados, pois todo o contato com os dados internos é mediado pelo próprio *software* do componente.

ii) Uma vez introduzido um código hostil, não existe uma maneira fácil de se verificar ou reiniciar o *asset*.

iii) Quanto mais eficiente o MSD for em evitar ataques de terceiros, mais eficiente ele será para evitar uma verificação e auditoria.

g) **Conclusão sobre o *asset* "Hardware de segurança (MSD)" comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:**

O Risco resultante é Crítico ou Catastrófico devido ao seguinte:

- O *asset* foi um componente introduzido para se aumentar a segurança contra ataques de agentes de ameaça externos, mas que, como consequência, diminuiu drasticamente a possibilidade de se detectar ataques perpetrados por agentes de ameaça internos.
- Pode-se fazer uma fraude quase perfeita por meio desse *asset* comprometido.
- Toda a segurança contra ataques externos baseia-se na certificação dos componentes de *software*; havendo uma quebra de segurança grave na certificação, esse componente poderá ser enganado facilmente.

Tag	Asset	Comunidade de Ameaça	Risco Geral
A10:CAA1:1	A10: Segurança dos Aplicativos	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Comentários Complementares:

a) Problemas Identificados:

- Não existem boas proteções ou salvaguardas de segurança contra engenharia reversa.
- A segurança do sistema não foi projetada de forma monolítica (e.g. como uma biblioteca única que concentra as funcionalidades de segurança), o que facilita possíveis ataques.
- A segurança do sistema é composta de vários componentes que foram acrescentados de forma não necessariamente bem conectada.

b) **Nível de dificuldade de se introduzir um código hostil nos aplicativos**:

- Baixo, pois pode-se introduzir a fraude até no código-fonte, de forma quase imperceptível.

c) Facilidade de distribuição:

- Muito alta, pois, se estiver no próprio código-fonte, será distribuído oficialmente pelo TSE.

d) Potencial de danos:

- Muito alto, pois, se a fraude for bem feita, será quase imperceptível, uma vez que o código hostil será executado com parte da aplicação.
- Poderá com facilidade propiciar a alteração do resultado de uma eleição.

e) **Conclusão sobre o *asset* “Segurança dos Aplicativos” comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI]:**

O Risco resultante é Crítico ou Catastrófico devido ao seguinte:

- Será muito fácil criar e distribuir o *asset* comprometido.
- O *asset* Segurança dos Aplicativos comprometido pelo agente de ameaça tem um potencial muito alto para causar danos.
- Poderá ser usado em conjunto com outros ataques pelo agente de ameaça.
- Tanto a auditoria quanto a fiscalização permitida aos partidos pelo TSE são insuficientes para se detectar uma fraude que explore o *asset* comprometido pelo agente de ameaça [InT: (1) desenvolvedores de *software* do STI].

Tag	Asset	Comunidade de Ameaça	Risco Geral
A11:CAA3:6	A11: Votar Como um Eleitor Que Ainda Não Votou	ExTSemVinc: (6) mesários de seção eleitoral	Baixo

Comentários Complementares:

a) Problemas Identificados:

- Em muitas seções eleitorais, em especial de grotões em regiões longínquas e de difícil acesso no Brasil, os fiscais de partido nem aparecem ––ou são impedidos de aparecer nas seções por opositores–– para cumprir o seu papel de fiscalização do andamento dos trabalhos de votação dentro e fora das seções eleitorais.
- O TSE não desenvolve qualquer cruzamento de dados de votantes e justificativas para orientar medidas preventivas futuras.
- Em casos de duplicidade comprovada, a autoridade eleitoral é obrigada a desprezar a justificativa (dado com maior probabilidade de estar correto) e considerar válido o voto realizado (dado mais provavelmente falso), por causa do sigilo do voto e do anonimato do eleitor ao votar.
- O TSE não toma medidas para coibir ou diminuir a ocorrência desse problema no futuro, por exemplo analisando os logs da seção da ocorrência para verificar se o mesário é reincidente e afastá-lo de eleições futuras, se necessário!
- Como consequência, não existe publicidade sobre punições para mesários fraudadores.

b) Nível de dificuldade para um mesário votar como um eleitor que ainda não votou:

- Baixo, pois ele tem uma lista com o número do título de eleitor de quem ainda não votou.
- A verificação biométrica não é mandatória.
- Como discutido acima, não existe uma ação do TSE visando a coibir este tipo de fraude.

c) Facilidade de distribuição:

- Baixa, pois será feita urna a urna.
- Dependerá de ter mesários desonestos em conluio com fiscais de partidos ou ausência de fiscais de partidos nas seções eleitorais.

d) Potencial de danos:

- Eleições estaduais e nacionais:

a) Baixo, pois, mesmo que este tipo de fraude seja largamente utilizada, existe uma tendência a distribuir a fraude entre vários candidatos.

- Eleições em cidades pequenas:

b) Médio, pois, por existir um número relativamente pequeno de urnas em jogo, tem maior potencial em influenciar o resultado.

e) Conclusão sobre o *asset* "Votar Como um Eleitor Que Ainda Não Votou" comprometido pelo agente de ameaça [ExTSemVinc: (6) mesários de seção eleitoral]:

O Risco resultante é Baixo devido ao seguinte:

- O *asset* tem potencial baixo de causar danos, mesmo quando acontecer de eventualmente reverter o resultado de uma eleição em cidade pequena, embora nunca se poderá ter certeza disso.
- O impacto do *asset* poderia ser minimizado se com a mitigação da impunidade neste tipo de fraude.
- Este tipo de fraude foi utilizado para justificar as urnas biométricas, que até agora não resolveram o problema.

5.4. Mapas de Riscos: Quadros Resumidos

Risco Geral = Crítico ou Catastrófico

Tag	Asset	Comunidade de Ameaça	Risco Geral
A1:CAA2:2	A1: Compilador Open Source GCC GNU	ExTComVinc: (2) hacker em conluio com funcionário desenvolvedor de *software* ou gerente do TSE/STI	Crítico ou Catastrófico
A1:CAA1:1	A1: Compilador Open Source GCC GNU	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico
A2:CAA1:1	A2: Certificados Digitais	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico
A3:CAA1:1	A3: Sistema Operacional	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico
A4:CAA1:1	A4: Processo de Compilação	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico
A5:CAA2:6	A5: BIOS	ExTComVinc: (6) ex-funcionário desenvolvedor de *software* do TSE/STI em conluio com funcionário de fabricante que desenvolve o BIOS	Crítico ou Catastrófico
A7:CAA1:1	A7: Rotinas de Segurança do CEPESC	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico
A9:CAA1:1	A9: Hardware de segurança (MSD)	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico
A10:CAA1:1	A10: Segurança dos Aplicativos	InT: (1) desenvolvedores de *software* do STI	Crítico ou Catastrófico

Risco Geral = Médio a Crítico ou Catastrófico

Tag	Asset	Comunidade de Ameaça	Risco Geral
A8:CAA1:1	A8: *Software* da Urna para Votação Paralela	InT: (1) desenvolvedores de *software* do STI	Médio a Crítico ou Catastrófico

Risco Geral = Baixo a Médio

Tag	Asset	Comunidade de Ameaça	Risco Geral
A6:CAA3:3	A6: Visual da Urna e da Interface do Usuário	ExTSemVinc: (3) hackers associados a mesários e presidente de mesa de seção eleitoral	Baixo a Médio

Risco Geral = Baixo

Tag	Asset	Comunidade de Ameaça	Risco Geral
A1:CAA3:1	A1: Compilador Open Source GCC GNU	ExTSemVinc: (1) hacker	Baixo (L)
A11:CAA3:6	A11: Votar Como um Eleitor Que Ainda Não Votou	ExTSemVinc: (6) mesários de seção eleitoral	Baixo (L)

5.5. Termos Básicos do Método FAIR

Ameaça

Ameaça é qualquer coisa (por exemplo, objeto, substância, humano etc.) que é capaz de agir contra um asset (ativo) de uma forma que pode resultar em danos. Um tornado é uma ameaça, como é uma inundação, como é um hacker. A questão fundamental é que as ameaças aplicam a força (água, vento, código de exploração etc.) contra um asset que pode causar um evento de perda de ocorrer.

Vulnerabilidade

Vulnerabilidade é comumente reconhecida como uma "fraqueza que pode ser explorada", mas vamos deixá-la neste contexto como uma condição em que a capacidade de ameaça (força) é maior do que a capacidade de resistir a essa força da parte do asset.

Asset (ativo)

No contexto de risco da informação, podemos definir Asset como qualquer dado, dispositivo ou outro componente do ambiente que apóia as atividades relacionadas com um sistema de informação, que pode ser ilicitamente acessado, usado, divulgado, alterado, destruído ou roubado, resultando em perda de algum tipo para a instituição detentora do Asset.

Risco de Segurança

Risco de segurança é a probabilidade de ocorrência de algo ruim em uma instituição, combinado com a magnitude ou impacto provável da perda futura resultante dessa ocorrência! Em outras palavras, risco é uma medida do grau em que uma instituição está ameaçada por uma circunstância ou evento potencial, tipicamente em função do seguinte: (i) a probabilidade de ocorrência da circunstância ou evento; (ii) os impactos negativos prováveis que surgiriam se ocorresse a circunstância ou evento.

Agentes de Ameaça

Agentes de ameaça são indivíduos dentro de uma população de entes, vivos ou inanimados, de ameaça. Praticamente qualquer pessoa e qualquer coisa pode, sob certas circunstâncias, ser um agente de ameaça. Por exemplo: o operador de computador bem-intencionado, mas inepto, que desperdiça um trabalho diário inteiro, ao digitar o comando errado; o regulador pelo simples fato de realizar uma auditoria; ou o esquilo que mastiga um cabo de dados.

Comunidades de Ameaça

Comunidades de ameaça são subgrupos da população total de agentes de ameaça que partilham características-chave. As seguintes comunidades de ameaça são exemplos do cenário de ameaças humanas maliciosas que muitas organizações enfrentam:

- Comunidade Interna
  - Empregados
    - ✓ Quem tem privilégios de acesso elevados e uma maior especialização técnica (por exemplo, administradores de sistemas e redes)
    - ✓ Quem não tem privilégios elevados ou altos níveis de especialização (por exemplo, a população de empregados em geral)
  - Empresas contratadas e fornecedores
  - Parceiros
- Comunidade Externa
  - Ex-funcionários
  - Cibercriminosos (hackers profissionais)
  - Espiões
  - Hackers não profissionais
  - Ativistas de alguma causa
  - Serviços de inteligência da própria nação ou de outras nações
  - Autores de malware (código hostil, tais como vírus, worm, cavalos de tróia, backdoor etc.)

Características de Ameaças

Podemos identificar uma grande variedade de características de agentes de ameaça com o objetivo de representar as comunidades de ameaça. Na maioria das circunstâncias, existem relativamente poucas características realmente importantes. Incluir muitas características em nossa análise torna o modelo muito mais difícil de usar, com relativamente pouca melhora nos resultados. Este é um exemplo de onde a modelagem de risco tipicamente vai substituir precisão por maior praticidade. Há qua-

tro componentes fundamentais da taxonomia de risco da abordagem FAIR para os quais queremos identificar as características do agente ameaça; a saber, aquelas características que afetam o seguinte:

A frequência com que agentes de ameaça entram em contato com as nossas organizações ou assets
A probabilidade de que agentes de ameaça agirão contra nossas organizações ou assets
A probabilidade de ações de agentes de ameaça serem bem sucedidos em superar os controles de proteção
A natureza provável quanto ao tipo e gravidade do impacto em nossos assets

Características de Assets

Assets têm características relacionadas com valor, responsabilidade e força de controles de segurança que representam fatores de risco, tais como:

Criticidade – Aquela característica de um asset que tem a ver com o impacto na produtividade de uma organização. Por exemplo, o impacto que um banco de dados corrompido teria sobre a capacidade da organização para gerar receita
Custo – Os custos associados em substituir um asset que tenha sido roubado ou destruído. Exemplos incluem o custo de substituir um notebook roubado ou reconstruir um edifício bombardeado
Sensibilidade - O impacto resultante de informações confidenciais sendo divulgadas ou utilizadas indevidamente

A Organização

Existe risco no contexto de uma organização ou entidade. Em outras palavras, danos a assets afeta uma ou mais das proposições de valor da organização. É a organização que perde recursos ou a capacidade de operar. Características da organização também pode servir para chamar a atenção de certas comunidades de ameaças, que podem aumentar a probabilidade de ocorrência de eventos.

O Ambiente Externo

O ambiente em que uma organização funciona desempenha um papel significativo quanto ao risco em que ela está exposta. Várias características externas, como a paisagem regulatória, a concorrência dentro da atividade industrial da organização etc., todas ajudam a impulsionar a probabilidade de perda. Por exemplo no caso da urna brasileira, considere a participação do CEPESC, Módulo, Diebold e manufaturadora do chip de segurança MSD.

6. CONCLUSÕES

6.1 Síntese

O resumo das conclusões da presente auditoria especial sobre o 2º turno da eleição presidencial de 2014 é o seguinte:

a) ***Sobre a coleta de dados -*** A coleta de dados para auditoria teve sua confiabilidade prejudicada porque enfrentou restrições administrativas, tendo sido negada a entrega de parte dos dados solicitados e, em especial, foi negada permissão para coletar os dados diretamente das mídias de memória das urnas eletrônicas;

b) ***Sobre a apuração dos votos nas urnas eletrônicas –*** Não foi possível se determinar a confiabilidade dos resultados produzidos pelas urnas eletrônicas, porque:

   i. Não é possível se fazer uma auditoria contábil da apuração dos votos em um sistema de urnas eletrônicas que é essencialmente dependente de *software* e não produz um registro material do voto (o voto impresso) que tenha sido visto e conferido pelo eleitor e que possa ser utilizado como trilha de auditoria;

   ii. Não foi possível se fazer uma validação e certificação minimamente confiável do *software* embarcado nas urnas eletrônicas para verificar sua integridade devido a restrições impostas pela autoridade eleitoral.

   iii. Mesmo sem tais restrições, a validação e certificação do *software* das urnas é uma tarefa que, pra ser bem executada, demanda tempo e recursos muito elevados, inviabilizando, na prática, esse tipo de procedimento como garantidor da confiabilidade do sistema;

   iv. o Teste de Votação Paralela, como executado, não é eficiente para detecção de *software* adulterado nas urnas que verifique as condições de uso fora do comum.

c) ***Sobre a transmissão e a totalização dos votos -*** Não foram encontrados indícios de fraudes ou de erros sistemáticos que pudessem alterar os resultados depois que estes saem das urnas eletrônicas;

d) ***Sobre a auditabilidade em geral*** -

i. o sistema eletrônico de votação do TSE não está projetado e implementado para permitir uma auditoria externa **independente e efetiva** dos resultados que publica;

ii. O modelo de auditoria imposto pela autoridade eleitoral ("*auditoria comandada pelo auditados*") não se enquadra em qualquer modelo reconhecido e padronizado por entidades internacionais que normatizam auditoria de sistemas de informação;

iii. As urnas biométricas são incompatíveis com o Teste de Votação Paralela, e tornam inócua a lei que o criou.

A seguir apresentam-se as conclusões mais detalhadas sobre a confiabilidade do resultado eleitoral do 2º turno de 2014, relativas às quatro etapas previstas no PDI. Ao final são apresentadas outras conclusões gerais, sobre a transparência e a auditabilidade do processo eleitoral eletrônico do TSE, decorrentes de todas as atividades desenvolvidas durante a auditoria especial no sistema eleitoral de 2104.

6.2 Coleta de Dados

A coleta de dados digitais e físicos (em papel) enfrentou dificuldades e impedimentos desde o seu início.

Algumas dificuldades foram contornadas, provocando apenas atraso no andamento dos trabalhos, como foi o caso do fornecimento dos dados digitais de controle das urnas eletrônicas (BU, LOG e RDV), que deveriam ser entregues em apenas 3 dias, só foram entregues incompletos depois de 2 meses, levando mais um mês para ser entregue o restante.

Outros impedimentos não se conseguiu contornar, como a recusa de entrega dos dados de controle do sistema de Geração de Mídias e a inexistência dos dados claros relativos à sequência de totalização, o que criou lacunas na abrangência da auditoria permitida, inclusive sobre pontos críticos do processo.

Porém, ocorreu um caso grave de restrição imposta pela autoridade eleitoral que comprometeu fortemente a qualidade da auditoria: o impedimento de se obter os dados digitais pela leitura direta das mídias de memória das urnas.

Especificamente, a autoridade eleitoral só permitiu o acesso indireto ao conteúdo das mídias das urnas eletrônicas, pelo uso de programas previamente carregados nas próprias mídias que se quer avaliar.

Sob tal regramento, é impossível para os auditores ter certeza sob a integridade dos dados obtidos das urnas, o que criou uma grave lacuna na auditoria, afastando-a em termos de qualidade e de confiabilidade de uma auditoria forense.

6.3 Auditoria da Apuração

A auditoria da apuração por validação do *software* eleitoral teve seu resultado totalmente prejudicado pelas restrições impostas ao trabalho dos auditores. Dez das doze tarefas previstas no PTI não puderam ser concluídas a contento e as duas restantes (avaliação dos lacres e da Votação Paralela) revelou impropriedades.

Restou incompleta a verificação da coerência dos totais dos votos gravados nos arquivos de controle das urnas por não ter sido permitido comparar os dados de todos os arquivos disponíveis, mas apenas dos arquivos escolhidos pelos auditados (especificamente, não foi permitida a conferência da quantidade de eleitores faltosos)

Com a recusa de informar quais são os requisitos de segurança e a relação das normas técnicas adotadas no projeto do sistema, não foi possível afastar as hipóteses de que a autoridade eleitoral não segue qualquer especificação formal de segurança e de que o sistema eleitoral eletrônico brasileiro não está em conformidade com qualquer norma técnica reconhecida de projeto e de segurança.

A negativa de apresentar os códigos-fonte do BIOS e do circuito MSD impediu a análise completa dos programas das urnas, tornando-se impossível fazer qualquer afirmação sobre seu funcionamento correto e idôneo.

Não foi permitido se determinar se o código-fonte apresentado pela ABIN era o mesmo que, compilado, foi incluído no *software* usado nas urnas eletrônicas.

Não foi permitido acesso aos programas compiladores para verificar sua integridade e não foi permitido desenvolver qualquer procedimento para conferência real e confiável da integridade do *software* executável carregado nas urnas.

Pelas restrições impostas pela autoridade eleitoral, é impossível a validação e certificação, pela equipe de auditores, do *software* eleitoral usado nas urnas eletrôni-

cas e, por seu porte, é inviável a validação do *software* eleitoral do TSE sob condições razoáveis de recursos e custos.

Os lacres colocados nas urnas são só parcialmente eficientes para revelar eventuais ataques ao *software*. Embora tenha se encontrado inúmeros casos de lacres com irregularidades, não se encontrou qualquer caso que tivesse disparado alguma atividade de segurança para sua avaliação e correção.

O Teste de Votação Paralela não conseguiu reproduzir as necessárias "*condições normais de votação*", tornando-se ineficaz na detecção de *software* adulterado que explore essa condição.

Em especial, as urnas biométricas são incompatíveis com o § 6º do Art. 66 da Lei 9.504, que institui o Teste de Votação Paralela, tornando-o inócuo.

Nesses termos:

a) pela inexistência do VVPAT – trilha material, em papel, para auditoria;
b) com as restrições e limitações encontradas para validação e certificação segura do *software* das urnas eletrônicas;
c) com a ineficácia da Votação Paralela;

considera-se impossível determinar, com algum nível de confiabilidade, se foram justos o registro e a apuração dos votos no 2º turno da eleição de 2014.

6.4 Auditoria da Transmissão e Totalização

A análise estatística da transmissão e da totalização dos resultados no 2º turno de 2014, não encontrou sinais de erros ou eventuais fraudes sistemáticas que pudessem inverter o resultado.

Contudo, não foi possível reconstruir o gráfico da evolução da totalização, devido à inexistência de dados de controle que permitissem a sua reprodução.

6.5 Denúncias Específicas

A Geração de Mídias para carga do *software* nas urnas eletrônicas ocorre em computadores conectados à Internet.

Pelos termos dos contratos com o TSE e com os TRE´s, funcionários da empresa S*martmatic* teriam tido acesso em momentos críticos de carga do *software* e da transmissão dos resultados. Considere-se, no entanto, que a carga do *software* das urnas não pôde ser certificada com confiabilidade, enquanto a transmissão dos resultados pôde ser auditada e não mostrou sinais de erro.

Fraudes na Votação são possíveis mas costumam ser localizadas e sem potencial de alterar significativamente uma eleição presidencial.

No entanto, constatou-se que a autoridade eleitoral não faz qualquer análise dos dados gerados durante a eleição para detectar eventuais irregularidades, como a inserção de votos pelos mesários e a duplicidade de votação e justificativa, com finalidade preventiva.

As demais denúncias de fraudes foram consideradas falsas ou apenas falhas localizadas (sem potencial de afetar o resultado).

6.6 Constatações Gerais sobre o Sistema

Claramente, o sistema eletrônico de votação do TSE não foi projetado para permitir uma auditoria externa independente e efetiva dos resultados que publica.

O modelo de auditoria imposto pela autoridade eleitoral (”*auditoria comandada pelo auditados*”) não se enquadra em qualquer modelo reconhecido e padronizado por entidades internacionais que normatizam auditoria de sistemas de informação.

O sistema de votação do TSE também não está preparado para uma auditoria interna, que deveria ser realizada antes, durante e após as eleições. Não está preparado para obter, por exemplo, certificação do *software* de votação, em especial da urna eletrônica, de acordo com padrões internacionais de segurança.

Muitos procedimentos críticos efetuados sob controle dos administradores (como o registro e a apuração dos votos, a compilação dos códigos-fonte e a sequência de totalização) não podem ser repetidos ou, ao menos, conferidos.

A documentação do projeto continua incompleta e a metodologia usada ainda revelam a mesma imaturidade no desenvolvimento que já havia sido apontada no Relatório COPPE/UFRJ[152] de 2002.

Contrariando o disposto nos §§ 1º e 2º do Art. 66 da Lei 9.504, parte dos programas fontes e executáveis usados nas urnas eletrônicas não estavam gravados no DVD oficial da eleição de 2014.

A ABIN produz parte crítica do *software* embarcado nas urnas e o TSE não tem posse do código-fonte e fica sem condições de verificar a integridade do código executável desenvolvido pela ABIN.

A tecnologia usada no circuito de segurança MSD, presente nas urnas a partir do modelo 2009 (75% do total usado em 2014), pode tanto servir para dificultar a gravação de *malware* no BIOS, como para esconder eventual *malware* nele gravado.

Ademais, o modo de implantação da tecnologia MSD abre oportunidade para que pessoas externas ao TSE, como os funcionários da ABIN, da empresa Diebold, da empresa Módulo e das empresas contratadas pelo TSE e TRE para "*exercitação das urnas*" (dentre as quais se inclui a empresa Smartmatic) tenham, em tese, momentos de acesso ao *software* instalado em pontos críticos das urnas (BIOS e MSD) e nos sistemas de preparação e geração de mídias, podendo, em tese, inserir "portas dos fundos" para posterior exploração.

O mesmo ocorre com relação a uma vasta gama de funcionários da própria STI/TSE que têm acesso a pontos críticos do sistema, como a posse de chaves de verificação, a compilação dos códigos e aos próprios códigos compilados.

O risco de ataque interno é agravado porque o modelo de máquinas de votar é essencialmente DEPENDENTE do *software* e a validação do *software* não é viável pelas restrições impostas pela própria STI/TSE.

As chaves de segurança que permitem a verificação da integridade do *software* estão gravadas (*hardcoded*) no próprio código compilado, causando uma falha de segurança, pois um *software* malicioso poderia, ao menos em tese, obter essas chaves para assinar arquivos de resultado falsos como se eles fossem gerados por urnas legítimas.

---

152 **Rocha, A.R.C. et al.** *Relatório de Avaliação do Software TSE realizada pela Fundação COPPETEC*. Brasília: COPPE/UFRJ, 09/08/2002 - *http://www.angelfire.com/journal2/tatawilson/coppe-tse.pdf*ver resumo em: *http://www.votoseguro.org/textos/relcoppetec1.htm*

A falta de controle da STI sobre os compiladores utilizados caracteriza grande vulnerabilidade que poderia ser explorada por atacantes internos, sem deixar rastros que pudessem ser detectados em qualquer auditoria externa sobre o código-fonte original.

O uso de urnas com biometria torna ineficaz o §6º do Art. 66 da Lei 9.504, que institui o Teste de Votação Paralela.

A avaliação de riscos mostrou que os seguintes itens usados no desenvolvimento ou compondo o *software* da urna, se atacados por agentes de ameaça internos (correspondentes a funcionários, ex-funcionários, parceiros do TSE/STI) ou hackers associados a algum agente interno, exporiam o *software* da urna a riscos catastróficos/gravíssimos: compilador GCC GNU, certificados digitais usados, sistema operacional, processo de compilação, BIOS, rotinas de segurança do CEPESC, hardware de segurança (MSD), segurança dos aplicativos e *software* da urna para votação paralela.

Esses riscos catastróficos/gravíssimos significam que a urna brasileira estaria vulnerável a diversos tipos de ataques, desde atos de sabotagem para atrapalhar as eleições a atos que poderiam mudar os resultados de uma eleição e, pior, sem deixar rastros que poderiam detectar indícios de fraudes, como relatado anteriormente.

7. RECOMENDAÇÕES

Diante dos achados da auditoria e, principalmente, considerando as precárias condições de auditagem impostas pelo Tribunal Superior Eleitoral, recomenda-se:

I. Promova-se o armazenamento, na cerimônia de assinatura digital, em ao menos duas mídias idênticas, de todos os programas, fonte ou compilados, utilizados no desenvolvimento, funcionamento e compilação dos sistemas de informática, inclusive das bibliotecas de segurança do CEPESC e do firmware da BIOS e do circuito de segurança MSD das urnas eletrônicas;

II. Promova-se, logo após a assinatura digital dos programas, à análise pericial de amostras das mídias, de forma a permitir a análise conteúdo e especificamente do código fonte do programa lacrado pelos técnicos da Justiça Eleitoral, representantes dos partidos políticos, da OAB, do CREA, da SBC e do Ministério Público Eleitoral, sendo que a análise poderia ser feita até depois da eleição durante seis meses;

III. Permita-se, nas fases de verificação e acompanhamento do desenvolvimento dos sistemas de informática e após a realização da eleição, a utilização de qualquer programa de verificação desenvolvido ou adquirido pelos partidos políticos, garantido o prévio exame pela Justiça Eleitoral para identificação da ausência de código maliciosa ou perigo no programa que será utilizado;

IV. Regulamente-se e promova-se a execução de testes LIVRES de penetração nas urnas eletrônicas para busca e confirmação de eventuais vestígios de vulnerabilidades ou fraudes, sem restrições de acesso e de recursos, por investigadores nacionais ou estrangeiros indicados pelos Partidos Políticos e que o teste possa ser acompanhando pela STI mas que não seja coordenado nem regulamentado por membros da STI;

V. Promova-se o desenvolvimento de estudos para implantar novo sistema de votação paralela adaptada ao sistema biométrico que respeite rigorosamente as condições normais de votação quanto a liberação do voto do eleitor;

VI. Crie-se um órgão composto por representantes de todos os participantes do processo eleitoral para, de forma independente, acompanhar, ininterruptamente, todo o processo eleitoral;

VII. Promova-se a unificação do horário da eleição em todo o território nacional, considerando-se os horários previstos na legislação como o horário de Brasília, a fim de se evitar atrasar e permitir o acompanhamento da divulgação dos resultados desde o primeiro momento;

VIII. Promova-se a utilização de metodologia de desenvolvimento de *software* certificada e apropriada para o desenvolvimento de *software* crítico, como é o da urna, incluindo o desenvolvimento de documentação completa do sistema e das salvaguardas de segurança, de modo a facilitar as atividades futuras de manutenção e evolução do sistema, bem como de auditoria interna e externa;

IX. Promova-se a realização de testes por amostragem no seu parque de urnas a cada novo lote que seja adquirido, para acessar diretamente os dispositivos de memória e de firmware para verificar e atestar a ausência de qualquer programa ou código malicioso que possa estar contido nas peças de fábrica, inclusive BIOS e dispositivos de memória da urna, com acompanhamento de representados dos partidos políticos, Ministério Público e Ordem dos Advogados do Brasil, do CREA e da SBC;

X. Regulamente-se o voto impresso conferível pelo eleitor (VVPAT) com um Sistema Eletrônico de Votação que deverá atender, ao menos, aos seguintes Princípios e Controles:

- **Princípio da Publicidade** – o eleitor tem o direito de ver e conferir o conteúdo do registro digital do seu voto e os fiscais de candidato têm o direito de ver e acompanhar a contagem dos votos.
- **Princípio da Inviolabilidade Absoluta do Voto** – inclusive sendo proibido que o equipamento de auxílio à votação e o equipamento de auxílio à identificação dos eleitores tenham interconexões lógicas ou elétricas.
- **Princípio da Independência do *Software*** – para que nenhum erro não detectado no *software* possa provocar erros indetectáveis no resultado ou violação sistemática do voto.
- **Direito a refutação** – antes de deixar o local de votação, o eleitor pode refutar o conteúdo do voto impresso e iniciar nova votação.
- **Auditoria Contábil Automática** – determinar a quantidade de urnas que deverão ter seus votos impressos contados para comparação com o resultado do BU. A escolha dessas urnas deve ser necessariamente feita depois de encerrada a votação e de forma aleatória.

- **Solução de Divergências** – no caso de divergências entre os votos impressos e os digitais em uma urna, deve prevalecer os resultados da contagem dos votos impressos.
- **Auditoria do *Software*** – determinar em que condições deve ser realizada uma auditoria completa e independente sobre o *software* eleitoral, após a eleição.
- **Boletim de Urna Impressos** – determinar que o fechamento das portas dos locais de votação só deve ocorrer depois de disponibilizados aos fiscais dos partidos as cópias dos BU impressos produzidos em cada seção eleitoral.

XI. Promova-se a alteração das resoluções vigentes de forma a suplantar todos os obstáculos à realização de auditoria plena para confirmação da confiabilidade do sistema de votação eletrônico;

XII. Permita-se acesso **direto** ao conteúdo das mídias das urnas para poder verificar sua integridade e a inexistências de dados inesperados;

XIII. Permita-se acesso ao código-fonte completo, inclusive da ABIN e do firmware, com tempo suficiente e sem restrições de recursos operacionais;

XIV. Permita-se realização de análise dinâmica do *software*, incluindo eventuais recompilações parciais e totais;

XV. Permita-se analisar os compiladores e o ambiente de compilação utilizados;

XVI. Permita-se conferir efetivamente a integridade dos executáveis, por meio de acesso livre aos dados gravados em mídias ou em firmware;

XVII. Separe-se as funções eleitorais de administração, de regulamentação e de julgamento do contencioso de modo a garantir um processo isento, de acordo com os mais comezinhos princípios de governança;

XVIII. Determine-se que qualquer procedimento de auditoria externa da votação, da apuração, da transmissão e da totalização dos votos deva ser realizado de forma independente do administrador eleitoral, não tendo este os poderes de limitá-lo ou de restringi-lo;

XIX. Regulamentem-se os procedimentos de auditoria interna após as eleições, com estabelecimento de rotinas para documentação e processamento dos indícios de irregularidade no processo de votação, transmissão e totalização dos votos.

8. REFERÊNCIAS BIBLIOGRÁFICAS

(s.d.). Fonte: Justiça Eleitoral: http://www.tse.jus.br/

(2014). Fonte: Heartbleed: http://heartbleed.com/

(2015). Fonte: Você Fiscal - Fiscalize a eleição, garanta seu voto: http://www.vocefiscal.org/

Ansari, N., Sakarindr, P., Haghani, E., Zhang, C., Jain, A. K., & Shi, Y. Q. (May-June de 2008). Evaluating Electronic Voting Systems Equipped with Voter-Verified Paper Records. *IEEE Security & Privacy*, pp. 30-39.

Aranha, D. F., Karam, M. M., Miranda, A., & Scarel, F. B. (2013). *Vulnerabilidades no software da urna eletrônica brasileira.* Brasília.

Ataque de Princeton: vídeo ilustrativo. (s.d.). Fonte: http://www.youtube.com/watch?v=0AKR-Lo-700: http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06full.pdf

(2002). *Avaliação do Sistema Informatizado de Eleições.* Unicamp.

Braga, I. (2015). *Justiça eleitoral é contra voto impresso por questão 'técnica', diz Toffoli*. Fonte: O GLobo: http://oglobo.globo.com/brasil/justica-eleitoral-contra-voto-impresso-por-questao-tecnica-diz-toffoli-16530449#ixzz3eeefRIa1

Comissão de avaliação formada por professores Unicamp. (2002). *Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica).* Campinas.

Comitê Multidisciplinar Independente CMind. (2009). *Relatório sobre o Sistema Brasileiro de Votação Eletrônica.*

Comitê Multidisciplinar Independente CMIND. (2009). *Relatório sobre o Sistema Brasileiro de Votação Eletrônica.*

Douglass, B. P., & Ekas, L. (2012). *Adopting agile methods for safety-critical systems development.* IBM. Fonte: http://www.nohau.se/$2/file/douglass-adopting-agile-methods-for-safety-critical-systems-development.pdf

Eleitoral, T. S. (s.d.). *Planejamento Estratégico do TSE 2011/2014.*

Free Software Foundation's Licensing and Compliance Lab. (s.d.). *Frequently Asked Questions about the GNU Licenses*. Fonte: http://www.gnu.org/licenses/gpl-faq.en.html#v3VotingMachine

Goodin, D. (2012). *Questions abound as malicious phpMyAdmin backdoor found on SourceForge site*. Fonte: ArsTechnica: http://arstechnica.com/security/2012/09/questions-abound-as-malicious-phpmyadmin-backdoor-found-on-sourceforge-site/

Goodin, D. (2015). *World's first (known) bootkit for OS X can permanently backdoor Macs. Ars Technica.* Fonte: http://arstechnica.com/security/2015/01/worlds-first-known-bootkit-for-os-x-can-permanently-backdoor-macs/

Hursti, H. (2006). *Diebold TSx Evaluation - Security Alert*. Acesso em 2015, disponível em Black Box Voting: http://www.blackboxvoting.org/BBVtsxstudy.pdf

ISACA. (2015). *Information Systems Auditing: Tools and Techniques – IS Audit Reporting. Professional Practices Report 2015.* Fonte: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/information-systems-auditing-tools-and-techniques.aspx

Mercury, R. (2000). *Electronic Vote Tabulation, Checks & Balances.* University of Pennsylvania, USA. - http://www.notablesoftware.com/Papers/thesdefabs.html

Meyer, B. (2014). *Agile! The Good, the Hype and the Ugly.* (Springer, Ed.) Fonte: http://www.springer.com/978-3-319-05154-3

National Institute of Standards and Technology. (2009). *Draft Voluntary Voting System Guidelines.* Election Assistance Commission (EAC), USA. Fonte: http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf

National Institute of Standards and Technology. (2014). *NISTIR 8034 - Fingerprint Vendor Technology Evaluation.* doi:http://dx.doi.org/10.6028/NIST.IR.8034

New Jersey Division of Elections. (2007, April). *Criteria for Voter-Verified Paper Record for Direct Recording Electronic Voting Machines.* New Jersey. Retrieved 2015, em http://www.state.nj.us/state/elections/voter-critertia/Final-VVPRS-Criteria.pdf

Oliveira, E. L. (2001). Voto Eletrônico – Processo Eleitoral Brasileiro. *IP - Prodabel*.

Poulsen, K. (2003). *Thwarted Linux backdoor hints at smarter hacks*. Fonte: SecurityFocus: http://www.securityfocus.com/news/7388

Rivest, R. L., & Wack, J. P. (2006). *On the notion of 'software independence' in voting systems.* Massachusetts Institute of Technology, Cambridge.

Rocha, A. R., Travassos, G. H., Souza, G. S., & Mafra, S. (2002). *Relatório de Avaliação do Software do TSE realizada pela Fundação COPPETEC.* COPPE, Rio de Janeiro.

Sacco, O. A. (s.d.). Persistent BIOS Infection. *CanSecWest'09.* Fonte: https://cansecwest.com/csw09/csw09-sacco-ortega.pdf

Salihun, D. (2014). *NSA BIOS Backdoor a.k.a. God Mode Malware Part 1: DEITYBOUNCE.* InfoSec Institute. Fonte: http://resources.infosecinstitute.com/nsa-bios-backdoor-god-mode-malware-deitybounce

SAPM. (2014). *Agile and Critical Systems*. Fonte: SAPM: Course Blog: https://blog.inf.ed.ac.uk/sapm/author/s0841373/

SAPM. (2014). *Does Waterfall Deserve its Bad Press?* Fonte: SAPM: Course Blog: https://blog.inf.ed.ac.uk/sapm/2014/02/13/does-waterfall-deserve-its-bad-press/

Scott, A. (2012). *Agile/Lean Documentation: Strategies for Agile Software Development*. Em: Agile Modeling: www.agilemodeling.com/essays/agileDocumentation.htm

Sommerville, I. (2011). *Engenharia de Software* (9ª ed.). São Paulo: Pearson Education BR.

Stober, T., & Hansmann, U. (2010). *Agile Software Development: Best Practices for Large Software Development Projects.* Berlin: Springer-Verlag.

Tarouco, G. d. (jan de 2014). Governança eleitoral: modelos institucionais e legitimação. *Cadernos Adenauer*, pp. 229-243.

TENÓRIO, Rodrigo. *Direito eleitoral.* Rio de Janeiro: Forense, São Paulo: Método, 2014.

The New York Times. (s.d.). Man Indicted In Computer Case. Fonte: http://www.nytimes.com/2000/02/10/business/man-indicted-in-computer-case.html

Thompson, K. (August de 1984). Reflections on Trusting Trust. *Communications of the ACM, 7*. Fonte: http://dl.acm.org/citation.cfm?id=358210&coll=ACM&dl=ACM

Tribunal Superior Eleitoral. (2010). *Por dentro da Urna.* Brasília. Fonte: http://www.justicaeleitoral.jus.br/arquivos/tse-cartilha-por-dentro-da-urna

VGA Portal - Fato Online. (s.d.). *PF constata erro no cadastro biométrico realizado pelo TRE-DF*. Fonte: http://www.fatoonline.com.br/conteudo/2430/pf-constata-erro-no-cadastro-biometrico-realizado-pelo-tre-df

Ziff Davis, LLC. PCMag Digital Group. (2015). *Encyclopedia*. Fonte: PC Magazine: http://www.pcmag.com/encyclopedia/