UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LUÍS FERNANDO SCHAUREN

SEGURANÇA NO SISTEMA BRASILEIRO DE VOTAÇÃO ELETRÔNICA

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Raul Fernando Weber

Porto Alegre
2016

CIP - Catalogação na Publicação

Schauren, Luís Fernando
Segurança no Sistema Brasileiro de Votação Eletrônica / Luís Fernando Schauren. -- 2016.
93 f.

Orientador: Raul Fernando Weber.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Instituto de Informática, Curso de Ciência da Computação, Porto Alegre, BR-RS, 2016.

1. Voto Eletrônico. 2. Urna Eletrônica. 3. Eleições. 4. Segurança. 5. Transparência. I. Weber, Raul Fernando, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

AGRADECIMENTOS

Quando entrei para a UFRGS, em 1998, me faltava o foco e a maturidade necessários para seguir adiante com o curso. Na época, havia encontrado em minha profissão um sentido para minha vida. Anos mais tarde, já com relativa estabilidade profissional, pude compreender a importância de concluir o curso de graduação como forma de complementar a minha realização profissional e poder alçar vôos mais altos. E foi assim, já meio fora de forma, que retomei os estudos, encarando um novo vestibular e um curso de graduação depois de mais de 7 anos sem estudar. Entretanto, nada disso seria possível se não fosse o apoio e o incentivo de muitas pessoas queridas que merecem os destaques a seguir.

Agradeço principalmente à minha esposa, Taís Rossi da Silva, que me incentivou de maneira decisiva para que voltasse à Universidade e terminasse o curso que eu havia começado em 1998. Tenho certeza absoluta que muitas vezes ela sofreu mais que eu, com as minhas ausências, indisponibilidades para atividades de lazer e falta de atenção em momentos caros e dolorosos para ela. Agradeço também ao Telmo e à Rita, sogros queridos e excepcionais que me paparicaram e me deram apoio (até mais do que o necessário) durante todo o tempo em que estudei para o vestibular.

Agradeço à minha mãe e meu pai que sempre me incentivaram a valorizar e investir meus esforços na Universidade Federal, desde o curso técnico na Escola Técnica de Comércio da UFRGS.

Agradeço aos meus colegas de aula e parceiros de inúmeros trabalhos ao longo da faculdade, que colaboraram e me ajudaram a concluir o curso.

Por fim, agradeço aos meus colegas da Justiça Eleitoral, que me incentivaram, me apoiaram e seguraram a barra para que eu pudesse concluir o curso – apesar dos horários de muitas disciplinas, totalmente conflitantes com o nosso horário de expediente – e também àqueles que me ensinaram o pouco que sei, fornecendo informações importantes para a materialização desse trabalho.

RESUMO

A segurança do voto eletrônico é um fator crítico no processo democrático dos países que, cada vez mais, adotam soluções tecnológicas em busca maior controle, confiabilidade, integridade e agilidade na votação, apuração, totalização e divulgação dos resultados das eleições. Especialmente no Brasil, a segurança do voto eletrônico tem sido alvo de muitas polêmicas e constantes ataques nas mídias e redes sociais. Entretanto, muito do que se discute é fruto de desinformação, pois, embora o voto eletrônico seja discutido mundialmente, de maneira genérica, não há muita literatura disponível tratando especificamente do sistema brasileiro de votação eletrônica. Este trabalho apresenta um panorama da eleição eletrônica no Brasil e alguns dos mecanismos e barreiras de segurança mais importantes envolvidos em cada etapa do processo: hardware da urna eletrônica, instalação do sistema, votação, transmissão, totalização e divulgação dos resultados. Também serão abordados aspectos relevantes como identificação biométrica, voto impresso, testes públicos de segurança, inspeção do código e votação paralela. Ao longo de cada etapa, juntamente com a descrição do funcionamento desses mecanismos de segurança e auditoria, será feita uma análise de cada um desses eventos.

Palavras-chave: Voto eletrônico. Urna eletrônica. Segurança. Eleições. Biometria. Voto impresso. Votação paralela. Transparência.

SECURITY ON THE BRAZILIAN ELECTRONIC VOTING SYSTEM

ABSTRACT

Electronic voting security is a critical factor for the democratic process in many countries progressively seeking technological solutions for more control, reliability, integrity and expedition in voting, counting, totaling and announcing election results. Particularly in Brazil, vote security has been target of much polemic and constant attack from both the traditional media and social networks. Nonetheless, much of what is discussed is caused by disinformation. Even though electronic voting in, in a general fashion, debated all over the world, there is not much available literature dealing specifically with the Brazilian system of electronic voting. This work presents an overview of electronic voting in Brazil, introducing some of the mechanisms involved and the most important security barriers in each step of the process: the voting machine hardware, system deployment, voting, transmitting data, totaling and announcing results. Relevant aspects such as biometric identification, printed ballot, public testing of security measures, code inspection and parallel voting will also be addressed. Together with the step by step description of these security and auditing measures, each of these events will be analyzed.

Keywords: Electronic voting. Voting machine. Security. Elections. Biometry. Printed ballot. Parallel voting. Transparency.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
BIOS	*Basic Input/Output System*
BU	Boletim de Urna
CEPESC	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
DRE	*Direct Electronic Recording*
E2E	*End-to-End Verifiability*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
FE	*Flash* Externa
FI	*Flash* Interna
GAP	Gerenciador de Aplicativos
GEDAI-UE	Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica
MI	Módulo Impressor
MR	Mídia de Resultado
MSD	*Master Secure Device* (Dispositivo Microcontrolado de Segurança)
RDV	Registro Digital do Voto
RED	*Software* Recuperador de Dados
RTC	*Real Time Clock* (Relógio de Tempo Real)
SA	Sistema de Apuração
SAVP	Sistema de Apoio à Votação Paralela
SCUE	*Software* de Carga da Urna Eletrônica
TRNG	*True Random Number Generator*
USB	*Universal Serial Bus*
VOTA	*Software* de Votação
VVPT	*Voter Verified Paper Trail*

SUMÁRIO

1 INTRODUÇÃO

Este trabalho tem o objetivo de apresentar as principais características do sistema brasileiro de votação eletrônica e os motivos que levaram à adoção desse sistema. Juntamente com a descrição de cada etapa do processo e seus mecanismos de segurança, será feita uma análise de sua função relacionada à segurança do processo eleitoral, identificando protocolos e barreiras de segurança, processos de auditoria e verificação de resultados que visam garantir a transparência do processo eleitoral.

As informações constantes neste trabalho são fruto de intensa pesquisa e estudo sobre as características do sistema brasileiro de votação eletrônica, da legislação eleitoral brasileira, de material institucional disponibilizado na internet e intranet dos sites da Justiça Eleitoral, de trabalhos acadêmicos, artigos e trabalhos publicados sobre a urna eletrônica e/ou sistemas de votação eletrônica e de sistemas e protocolos de segurança. Além disso, também baseia-se em informações sobre o funcionamento da urna eletrônica e sistemas eleitorais obtidos em contato com os responsáveis pelo desenvolvimento desses sistemas e também pela experiência do autor, adquirida nos 20 anos que atua na Secretaria de Tecnologia da Informação do Tribunal Regional Eleitoral do Rio Grande do Sul, prestando suporte e treinamento em sistemas eleitorais e urnas eletrônicas, desde a introdução da primeira urna eletrônica em 1996. Todas as informações presentes nesse trabalho são públicas ou foram cedidas mediante autorização para divulgação em trabalho acadêmico.

Ao final, faremos uma retrospectiva de todos os conceitos e análises apresentadas para que, através de uma visão ampla do processo eleitoral, possamos identificar as necessidades, os principais riscos e quais barreiras de segurança, processos de verificação e auditoria atuam para resolver essas questões.

2 PANORAMA DA ELEIÇÃO ELETRÔNICA NO BRASIL

O Brasil possui uma das maiores eleições informatizadas do mundo, com quase 460 mil urnas eletrônicas em todas as seções eleitorais do país. O fato de existir uma Justiça Eleitoral, órgão governamental vinculado ao Poder Judiciário da União – composta hierarquicamente por um Tribunal Superior Eleitoral, Tribunais Regionais Eleitorais e Cartórios Eleitorais – que organiza, fiscaliza e realiza as eleições regulamentando o processo eleitoral, permitiu que a mesma solução tecnológica fosse implantada em todos os locais de votação do país.

A Justiça Eleitoral possui atualmente o maior cadastro biométrico da América Latina[1]. Os dados estatísticos no site do TSE[2] (maio de 2016), apresentam 144.088.012 eleitores no Brasil, sendo que 46.305.957 eleitores (32,1371%) possuem cadastro biométrico. Dos 5.568 municípios do país, 1.541 tem votação biométrica e 840 tem votação híbrida, na qual somente os eleitores que já possuem o cadastro biométrico são habilitados com a identificação da digital.

2.1 Necessidades e requisitos para a implantação do voto eletrônico no Brasil

Embora muitas pessoas possam pensar que a urna eletrônica brasileira foi desenvolvida para conferir agilidade à apuração e divulgação dos resultados, isso, na verdade, é apenas uma consequência do modelo eletrônico. Para compreendermos os motivos da implantação do voto eletrônico no Brasil, precisamos retornar ao passado e identificar os inúmeros problemas e vícios inerentes ao processo de votação e apuração que ocorriam no Brasil até 1994, última eleição em que foram utilizadas as cédulas de papel e urnas de lona em todo o país.

O primeiro problema estava relacionado com a interpretação da vontade do eleitor. No modelo de cédulas em papel era permitido ao eleitor votar em um determinado candidato ou legenda de partido (nos cargos proporcionais) identificando o nome ou número do candidato desejado. Ocorre que, frequentemente, havia problemas com a caligrafia, ou o eleitor escrevia

---

[1] Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2016/Janeiro/serie-urna-eletronica-biometria-garante-registro-unico-de-cada-eleitor

[2] Disponível em: http://www.tse.jus.br/eleicoes/estatisticas/estatisticas-eleitorais-2016/eleicoes-2016

o nome incompleto, ou ainda, utilizava um apelido para o candidato. Esses problemas acarretavam em situações de homonímia (vários candidatos com o mesmo nome) ou de impossibilidade de identificar com clareza o candidato a que se destina o voto. Essas situações poderiam incorrer na anulação do voto ou destinação a outro candidato, por solicitação dos fiscais presentes, ficando a decisão à critério da junta eleitoral responsável pela apuração.

O segundo problema estava relacionado à manipulação dos resultados, seja a partir da cédulas (marcação de votos em cédulas em branco ou troca de cédulas) ou dos mapas de votação (alteração das tabelas de resultados após a contagem dos votos), o chamado mapismo. Eram frequentes as denúncias de manipulação de resultados, assim como os recursos e pedidos de impugnação de seções eleitorais e anulação dos resultados baseadas nesses vícios. Conforme Cunha[3], em 1994 *houve mais oito mil recursos interpostos em todo o Estado do Rio Grande do Sul, tendo por objeto o escrutínio daquelas eleições gerais*.

O terceiro problema diz respeito ao sigilo do voto do eleitor, que frequentemente era coagido a votar em determinado candidato – o chamado voto a cabresto e os famosos currais eleitorais. Havia ainda a fraude por compra de votos, que privilegiava a elite econômica local. A própria caligrafia do eleitor ou a inclusão de marcas na cédula de papel muitas vezes poderiam incorrer na identificação da pessoa que havia preenchido aquela cédula.

As características do modelo utilizado anteriormente ao advento da urna eletrônica não permitiam a implantação do controle necessário do processo. Esse modelo dependida de uma forte e intensa fiscalização por todas as partes interessadas – prejudicando os partidos menores e que não dispunham de tantos fiscais – e da idoneidade absoluta das pessoas envolvidas em todas as fases do processo, o que acabava se tornando um verdadeiro tormento para os juízes eleitorais, maculando o processo eleitoral e colocando em cheque a transparência e confiabilidade das eleições em todo o país.

Com a evolução da tecnologia, era natural que se pensasse em um modelo eletrônico de votação que viesse suprir as necessidades do processo eleitoral e ao mesmo tempo tentar corrigir as falhas e vícios do modelo existente até então. Em 1995, o TSE criou a Comissão de Informatização das Eleições, composta por desembargadores, juízes e técnicos em informática.

---

[3] CUNHA, A. A. Portinho da. A Evolução dos Mecanismos de Transparência no Desenvolvimento do Projeto de Votação Eletrônica no Brasil: 1996-2008. Pág. 49. Porto Alegre, 2009.

> Entre as principais premissas estabelecidas pela comissão para orientar a elaboração do projeto da urna, cita: o sistema deverá estar consoante com a legislação eleitoral então existente; o voto deverá ser registrado numericamente; o eleitor terá o direito de ver a descrição de seu candidato escolhido, inclusive sua foto, antes de confirmar o voto; o equipamento para registro do voto deverá ser de uso exclusivo; o equipamento deverá ser pequeno, compacto, leve e poder ser transportado sem sofrer danos; e o eleitor poderá corrigir seu voto antes de confirmá-lo e poderá também votar em branco. (CUNHA, 2009)[4]

Cabe destacar entre as premissas para a máquina de votar brasileira, a adoção de uma solução universal, com o registro numérico do voto (exclusivamente) para partidos e candidatos, facilitando o acesso aos eleitores analfabetos e de baixa instrução, pois é muito mais fácil reconhecer números do que letras. Eliminar a possibilidade de votar no nome do candidato e exibir uma tela de confirmação com a foto do candidato após digitar o número, ajudou a reduzir a complexidade da interface com o usuário e ao mesmo tempo resolveu as questões relacionadas à homonímia, tornando o processo de escolha mais amigável. O fato do nosso sistema eleitoral se basear em votação direta em lista aberta de candidatos impede a adoção de uma solução de escolha de candidatos listados em tela, como ocorre com frequência em sistemas eletrônicos de votação de outros países, cujos sistemas eleitorais muitas vezes se baseiam em voto distrital e lista fechada com número reduzido de candidatos, o que está de acordo com outra premissa, que é a aderência do modelo à legislação vigente.

O sigilo do voto deve ser resguardado, motivo pelo qual não deve haver relação entre a lista de eleitores e a tabela de votos registrados, como veremos mais adiante. Como cada eleitor pode votar somente uma vez e nenhum eleitor pode votar por outro, deve haver um rígido controle na identificação e acesso à máquina de votar, que culminou com a identificação biométrica do eleitor, requisito que foi incorporado à urna eletrônica a partir de 2006, embora ainda não houvesse cadastramento biométrico do eleitorado à época. É importante esclarecer que o problema do sigilo do voto pode ser dividido basicamente em duas categorias:

a) o eleitor que não quer que saibam em quem ele votou;
b) o eleitor que quer um comprovante de que o voto dele foi registrado corretamente.

Aqui temos o problema da transparência *versus* sigilo do voto. É o chamado "cobertor curto": se melhorarmos muito a transparência podemos comprometer o sigilo do voto.

---

[4] CUNHA, A. A. Portinho da. A Evolução dos Mecanismos de Transparência no Desenvolvimento do Projeto de Votação Eletrônica no Brasil: 1996-2008. Pág. 54. Porto Alegre, 2009.

Com relação à votação, a urna só deve permitir a inserção de votos a partir das 8h do dia da eleição. Uma vez iniciada a votação, a urna deve guardar os resultados e o estado da votação, não sendo permitido voltar ao estado inicial, anterior ao registro do primeiro voto. A votação só poderá ser encerrada a partir das 17h, permitindo que sejam inseridos votos após esse horário em caso de fila na seção eleitoral, desde que a votação não tenha sido encerrada. Uma vez encerrada a votação, não deve ser possível inserir mais votos na urna eletrônica. A urna deve permitir a recuperação/regeração dos resultados.

Por fim, foram estabelecidas algumas premissas relacionadas à orçamento e logística[5]: o projeto deveria ser economicamente viável, em função do grande número de seções eleitorais no país; possibilidade de reaproveitar o equipamento em várias eleições, diminuindo o custo do voto; equipamento robusto, com porte e peso reduzidos, de forma a facilitar o transporte e armazenamento; utilização de bateria interna que permita o uso mesmo em locais onde houver indisponibilidade de energia elétrica

Cabe destacar aqui que a urna eletrônica tem cumprido até então com seus propósitos. Embora existam alguns pedidos de auditoria, recursos e denúncias de fraude (nada comparado à quantidade de recursos apresentados até 1994), não há nenhum registro sequer de fraude confirmada até hoje, em 20 anos de existência da urna eletrônica.

2.2 Por que outros países não utilizam a urna eletrônica?

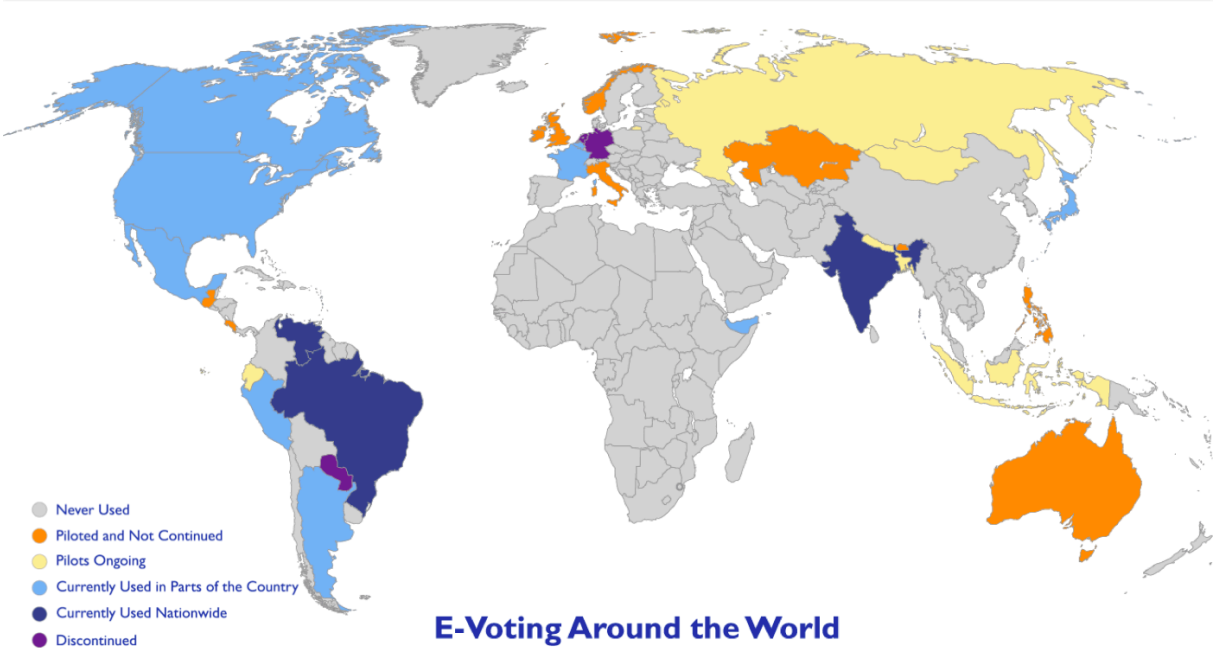
Embora muitos países tenham demonstrado interesse na urna eletrônica brasileira – o TSE chegou a firmar parcerias para o empréstimo de urnas eletrônicas a outras nações, dentre elas o Paraguai, Equador, Argentina e República Dominicana - é importante lembrar que a nossa urna foi feita para atender as necessidades e requisitos do processo eleitoral brasileiro. Além disso, muitos países já desenvolvem, conforme suas necessidades, um sistema eletrônico de votação específico para a sua realidade.

Vários países, inclusive os do chamado primeiro mundo, adotam ou tentaram adotar, ainda que parcialmente, soluções eletrônicas para o voto da população. O mapa da Figura 2.1 a seguir apresenta alguns exemplos de países que tentaram a implantação de máquinas de votar. Uma breve análise desse mapa demonstra o que podemos denominar de binômio capacidade *versus* necessidade. Alguns países tem tecnologia para implantar um modelo de

[5] Disponível em: <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/eleicoes>

votação eletrônica, mas não necessariamente tem essa necessidade. Por outro lado, muitos países tem a necessidade de implantar um modelo eletrônico, seja para atender requisitos de segurança ou eficiência no processo eleitoral, mas não tem capacidade tecnológica ou financeira para tal – o que pode facilmente explicar o vazio existente no continente africano.

Figura 2.1 – Mapa da votação eletrônica no mundo



Fonte: National Democratic Institute (2016)[6].

Para entender os motivos que levam uma nação a adotar ou desistir de um determinado modelo de votação eletrônica é preciso compreender as necessidades, os requisitos, o momento e as características culturais de cada país. Um dos casos mais emblemáticos que podemos citar para ilustrar essa questão é a Estônia e a implantação do voto pela internet:

> Precoce ao agir nos primeiros meses de desmoronamento do império soviético, a Estônia manteve a iniciativa ao estruturar suas instituições governamentais. É por este caminho que se chega à especificidade da experiência do país báltico com o voto eletrônico. Sem uma tradição governamental legitimada pela população – o Estado anterior havia sido erigido pelo invasor –, os estonianos procuraram aproximar o mais rápida e eficientemente possível a sua população das novas estruturas estatais. Para tanto, criaram um dos mais ousados sistemas de governo eletrônico do mundo.
>
> Nas eleições municipais de 2005, em mais uma fase da implementação da governança eletrônica, os estonianos puderam votar em seus candidatos através da internet. A partir deste ponto, começam a ficar mais claras as diferenças entre os vários projetos de voto eletrônico em voga no mundo. País geograficamente pequeno, com poucos habitantes e necessitando estruturar um Estado com legitimidade, a Estônia trilhou o caminho da informatização em várias esferas. O

[6] https://www.ndi.org/e-voting-guide/electronic-voting-and-counting-around-the-world

> sistema de votação foi apenas mais uma delas. De seus 1,3 milhão de habitantes, mais de 60% possuía, em 2005, um cartão de identificação digital utilizado, entre outros fins, para votação à distância. Mais da metade da população, 52%, possuía acesso à internet e nove entre dez estonianos utilizavam telefone celular no ano de 2005. (TRE-RS, 2006, pág. 80)[7]

Some-se a isso o fato de que o voto na Estônia é facultativo, com alta taxa de abstenção, acima de 50% (Estonia, 2006, pág. 28)[8] e a necessidade de aproximar a eleição da população. Dessa forma, estão criadas as condições para que se estude a adoção e implantação de um modelo de votação pela internet. Não é objeto desse trabalho analisar a segurança do modelo de votação eletrônica na Estônia. Estamos usando o caso apenas para exemplificar que, para diferentes problemas, existem distintas soluções.

Reforçando a questão de que é necessário compreender o contexto em que está inserido o panorama eleitoral de uma nação, para seja possível definir um modelo de votação específico, podemos citar o caso da Alemanha, cujos votos são apurados no próprio local de votação – após o encerramento da votação – e os resultados transmitidos por telefone para o respectivo comitê eleitoral (OSCE/ODIHR, 2009). Ao que parece, atualmente existe confiança e suficiência no processo eleitoral alemão, de forma que não há um ganho perceptível ou uma expressiva vantagem em se adotar um modelo eletrônico de votação. A apuração é bastante rápida, já que a contagem dos votos é feita pelos próprios presidentes das mesas de votação e imediatamente transmitidos os resultados por telefone. Nesse cenário, como justificar o custo exorbitante da implantação do modelo eletrônico de votação como o do Brasil?

Ainda em relação ao caso da Alemanha, há que se ressaltar que, em 2005, houve a tentativa de implantação de um modelo eletrônico de votação que, posteriormente, em 2008, foi vetado pela Corte Alemã por ser inconstitucional (OSCE/ODIHR, 2009)[9]. A decisão se baseou no argumento de que, em uma eleição em que o resultado é determinado através do processamento computacional de votos armazenados em uma memória eletrônica, a produção e divulgação dos resultados não é suficiente para atender os requisitos do escrutínio público. O uso de máquinas de votar só estaria de acordo com os princípios fundamentais da constituição alemã se os passos essenciais em uma eleição (votação, apuração e tabulação dos

---

[7] Tribunal Regional Eleitoral do Rio Grande do Sul. Voto Eletrônico. Edição comemorativa: 10 anos da urna eletrônica; 20 anos do readastramento eleitoral. 2006

[8] ESTONIA. National Electoral Comittee. Internet Voting at the Elections of Local Government Councils on October 2005. Report. 2006. Table 11, pág. 80

[9] Office for Democratic Institutions and Human Rights (OSCE/ODIHR). Federal Republic Of German - Elections To The Federal Parliament (Bundestag), sep 2009, pág 5.

resultados) pudessem ser examinados ou compreendidos pelo cidadão médio sem o auxílio de um especialista ou de qualquer conhecimento técnico.

Por fim, alterar a legislação ou a constituição de um país para atender ou possibilitar a implantação de um modelo eletrônico de votação parece ser um dos fatores que mais contribuem para o insucesso dessa experiência. Em muitos países, a exigência constitucional de um modelo de auditoria independente do software – o voto impresso, por exemplo – parece ser um fator determinante para a escolha de um determinado modelo.

2.3 Evolução do sistema de votação eletrônica do brasil

A primeira eleição com a urna eletrônica como conhecemos atualmente foi em 1996, quando tivemos eleições municipais em todo o país. Nessa eleição, a urna eletrônica foi utilizada em todas as capitais e também nos municípios com mais de 200 mil eleitores.

Embora o voto eletrônico tenha iniciado com a implantação da urna eletrônica, há que se considerar dois marcos evolutivos anteriores a esse fato, que contribuíram significativamente para esse processo: o recadastramento nacional do eleitorado em 1986 e a totalização informatizada das eleições em 1994. O recadastramento nacional permitiu que a base de eleitores cadastrados no TSE se aproximasse mais da realidade, com o cancelamento e a exclusão de títulos eleitorais de pessoas falecidas ou em duplicidade, por exemplo. A totalização informatizada permitiu que os dados de votação fossem digitados nos Tribunais Regionais Eleitorais dos estados, após o envio, por fax, dos mapas de votação com os resultados de cada município. No Rio Grande do Sul, alguns cartórios utilizavam um programa em Clipper para totalizar os boletins de urna. Em Porto Alegre, todos os boletins de urna eram digitados na Secretária de Informática do TRE, em um servidor com vários terminais.

A partir das eleições de 2000, o Brasil passou a adotar a votação totalmente eletrônica, utilizando uma solução padrão para todo o país. Ao longo dos anos, diversas modificações foram introduzidas no software e no hardware urna eletrônica, por recomendação de especialistas, para atender demandas dos partidos políticos ou para resolver questões e problemas encontrados a partir da experiências com os pleitos anteriores. Um dos conjuntos mais importantes de mudanças introduzidas e que levaram à consolidação da maturidade da nossa urna eletrônica, foram as sugestões apontadas pelo relatório apresentado por especialistas da Universidade Estadual de Campinas, em 2002, denominado Relatório

Unicamp[10], após minuciosa investigação e análise do código da urna em 2002. Esse relatório apresentou "*um conjunto de recomendações cujo objetivo é o aumento da segurança e da confiabilidade do Sistema Informatizado de Eleições, em especial de seu componente mais sensível que é a urna eletrônica"*. A seguir, listamos as recomendações apontadas, que podem ser conferidas a partir da página 37 do relatório:

a) Desenvolvimento dos aplicativos de votação baseados em blocos estáveis permanentes para todas as eleições;
b) Formalização do ciclo de desenvolvimento do software;
c) Avaliação do código-fonte do núcleo do aplicativo e seus componentes acessórios por especialistas em informática independentes do TSE;
d) Compilação e determinação de resumos criptográficos dos arquivos em sessão pública;
e) Verificação, por representantes partidários, dos resumos criptográficos dos arquivos instalados nas urnas carregadas com o software;
f) Revisão do procedimento de preparação da urna para o segundo turno;
g) Impressão do boletim de urna antes do ciframento dos resultados da votação;
h) Substituição do uso de ciframento por assinaturas digitais como forma de autenticação dos boletins de urna.

O Relatório da Unicamp aponta que "*O sistema eletrônico de votação implantado no Brasil a partir de 1996 é um sistema robusto, seguro e confiável atendendo a todos os requisitos do sistema eleitoral brasileiro*". E conclui dizendo que

> Como resultado da avaliação realizada conclui-se que o sistema eletrônico de votação analisado atende as exigências fundamentais do processo eleitoral, ou seja, o respeito a expressão do voto do eleitor e a garantia do seu sigilo. Conclui-se também que a segurança e a confiabilidade do sistema de votação eletrônico podem ainda ser aprimoradas pela adoção de procedimentos e modificações apontados (...)
>
> (...) A confiabilidade do processo eleitoral depende crucialmente do controle sobre todas as etapas de sua condução, que deve ser exercido pela sociedade por meio dos partidos políticos, dos fiscais, dos mesários, dos juízes eleitorais e dos próprios eleitores. Algumas das recomendações acima só terão seus objetivos totalmente atendidos se houver a efetiva fiscalização e acompanhamento por representantes aptos a fazê-lo. (UNICAMP, 2002, pág. 46 e 47)

Mais tarde aprofundaremos a importância do papel dos partidos políticos e da sociedade na fiscalização do processo eleitoral.

[10] UNICAMP. Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica). 2002.

Outras evoluções importantes, que serão mais detalhadas nos próximos capítulos, que podemos destacar são: a tabela de correspondências, a Cerimônia de Lacração dos Sistemas, a inspeção do código pelas partes interessadas, a assinatura digital na urna eletrônica, a votação paralela, o registro digital do voto, a publicação dos boletins de urna, a identificação biométrica e os Testes Públicos de Segurança.

A Tabela 2.1 apresenta as principais modificações e recursos introduzidos no sistema brasileiro de votação eletrônica.

Tabela 2.1 – Principais marcos evolutivos do sistema de votação eletrônica do Brasil

1986	Recadastramento nacional do eleitorado brasileiro
1994	Totalização informatizada
1996	Primeira urna eletrônica Votação eletrônica nas capitais e cidades com mais de 200.000 eleitores
1998	Votação eletrônica nos municípios com mais de 40.500 eleitores (2/3 do eleitorado do país)
2000	Votação totalmente eletrônica (solução padrão para todo o país) Fotos de candidatos inclusive para os cargos proporcionais Tabela de Correspondência
2002	Relatório UNICAMP Assinatura digital na urna eletrônica Cerimônia de Lacração dos Sistemas Publicação dos resumos digitais Entrega da Tabela de Correspondência aos partidos políticos Voto impresso - projeto piloto (Lei 10.408/2002) Implantação da Votação Paralela
2003	Definição do acompanhamento do desenvolvimento do software pelas partes interessadas (partidos políticos) nos 6 meses anteriores à eleição
2004	Registro Digital do Voto (em substituição ao voto impresso) Tabela com registro digital do voto assinada digitalmente e disponibilizada aos partidos políticos
2008	Linux em todas as urnas Início da identificação biométrica Publicação dos boletins de urna na internet
2009	1º Teste Público de Segurança
2014	Auditoria especial do PSDB (análise de integridade dos dados em mais de 1000 urnas eletrônicas no país) Batimento biométrico
2015	Regulamentação da obrigatoriedade de realização dos Testes Públicos de Segurança

Fonte: TSE – Testes Públicos de Segurança (2016).

3 MODELOS DE VOTAÇÃO ELETRÔNICA E MÁQUINAS DE VOTAR

As máquinas de votação eletrônica usadas atualmente podem ser divididas basicamente em 3 modelos, de acordo com suas características:

1. Armazenamento eletrônico direto (DRE – *Direct Recording Electronic*): Nesse modelo os votos são armazenados e contabilizados de maneira puramente eletrônica em algum arquivo da memória digital. Não há mecanismo de verificação independente do software para os resultados que permita uma recontagem dos votos, sem a necessidade de uma nova eleição. Esse é o modelo adotado no Brasil.
2. Voto impresso conferível pelo eleitor (VVPT – *Voter Verified Paper Trail*): Nesse modelo, também conhecido por IVVT – *Independent Voter Verifiable Record* (Registro Independente Conferível pelo Eleitor), os votos são impressos, ou digitalizados, e estão disponíveis para verificação independente pelo eleitor e apuração posterior, sem, no entanto, estarem disponíveis para o eleitor na forma de um comprovante de votação;
3. Verificabilidade fim-a-fim (E2E – *End-to-end Verifiability*): Existe um software independente da máquina de votação que permite ao eleitor verificar se o voto foi devidamente registrado, contabilizado corretamente e incluído no resultado final.

Em relação ao modelo DRE, as maiores salvaguardas estão relacionadas com a dificuldade de verificação do software para garantir que não há erros que possam produzir resultados indesejados. Embora alguns estudiosos insistam em afirmar que "*adulterações não detectadas no software, causam distorções indetectáveis nos resultados"* (ARANHA, 2014, pág. 119), isso não é necessariamente verdade. A Justiça Eleitoral do Brasil adota, com sucesso, um modelo de auditoria por amostragem (votação paralela), independente do software, que permite verificar distorções nos resultados. Abordaremos em detalhes esse processo de auditoria na seção 5.10. Além disso, o TSE permite amplo acesso à entidades legitimadas a inspecionar o software da urna, conforme verificaremos nas seções 5.2 e 5.3. Claro que, havendo distorções no resultado, não será possível recuperar o resultado correto sem a convocação de uma nova eleição. Entretanto, se considerarmos, no caso do Brasil, todas as barreiras de segurança implementadas, os riscos envolvidos e os custos de implementação de um modelo totalmente verificável, pode-se compreender a opção do TSE em correr o risco (remoto) da necessidade de uma nova eleição.

Com relação à dependência de software, os sistemas podem ser: dependentes do software, fracamente independentes do software e fortemente independentes do software (RIVEST, 2006). Um sistema de votação dependente do software se alicerça na confiança e correção do software. Já um sistema de votação é independente de software sempre que um erro não detectado em software pode ser detectado no resultado final da eleição. Um sistema fracamente independente do software pode identificar uma falha não detectada no software, mas não apresenta um mecanismo de recuperação do resultado correto. Já o sistema fortemente independente do software, pode identificar uma falha não detectada no software e apresenta um mecanismo que permite a recuperação do resultado correto

O modelo VVPT em que o resultado do voto impresso em papel se sobrepõe ao voto eletrônico e pode ser considerado como o resultado oficial, em caso de divergência, é considerado fortemente independente do software. Já um modelo em que a cédula impressa em papel serve apenas para identificar a divergência de resultados, mas não permite a simples recontagem para fins de divulgação do resultado oficial, é um modelo fracamente dependente do software. Aqui cabe uma reflexão: é possível confiar exclusivamente no resultado impresso em papel? Havendo divergências entre os resultados, qual é o resultado oficial? O voto impresso, que é manipulado durante a apuração de forma análoga ao que ocorria nas eleições até 1994, ou o voto eletrônico? Além disso, há que se considerar que o sistema de impressão é gerenciado pelo mesmo software da urna. Um sistema de impressão completamente independente do software não pode garantir que ambos mecanismos (impressora e software de votação) estão registrando o mesmo dado.

O modelo E2E, verificável fim-a-fim, possui um mecanismo de verificação que é totalmente independente do software. Há que se considerar, nesse modelo, se o sigilo do voto é realmente garantido, ou seja, seu registro é apenas verificável, sem revelar o conteúdo. Além disso, recaímos na mesma questão da desconfiança de uma parte do eleitorado em relação ao software da urna: O cidadão que não tem conhecimentos de criptografia e segurança, e não crê que o software da urna soma corretamente os votos, provavelmente terá a mesma desconfiança em relação ao sistema que verifica a totalização do voto.

Em todos os casos, invariavelmente, recairemos na questão da verificação e validação do software na busca contínua por correção e integridade. Por esse motivo, é imprescindível que as partes interessadas nesse processo (partidos políticos e demais representantes da sociedade) façam uso de sua prerrogativa nesse processo.

4 A URNA ELETRÔNICA BRASILEIRA

A urna eletrônica que conhecemos atualmente foi desenvolvida, a partir de 1995, com base nas especificações técnicas produzidas por uma comissão de especialistas em informática designados pelo Tribunal Superior Eleitoral. “As instituições escolhidas para colaborar com a Justiça Eleitoral representam uma amostra do que havia de melhor na área da tecnologia nacional: Instituto de Pesquisas Espaciais – INPE, Ministério da Ciência e Tecnologia, Instituto Tecnológico da Aeronáutica – ITA, Centro de Pesquisa e Desenvolvimento da Telebrás, além dos setores de tecnologia dos então ministérios militares” (TRE-RS, 2006, pág. 48)[11]

A urna eletrônica foi evoluindo de acordo com as necessidades e as experiências aprendidas a cada eleição. Já passou por trocas de sistema operacional, começando com o VirtuOS, passou por Windows CE e hoje utiliza Linux. Também é importante ressaltar as contribuições e sugestões propostas por especialistas da comunidade acadêmica, partidos políticos e até mesmo equipes de investigadores formadas para explorar vulnerabilidades da urna eletrônica, como veremos na seção que trata dos Testes Públicos de Segurança. Atualmente, todo o código dos aplicativos do ecossistema da urna eletrônica e sistemas de apoio são desenvolvidos e mantidos exclusivamente pelo TSE.

4.1 Hardware e Arquitetura da Urna Eletrônica

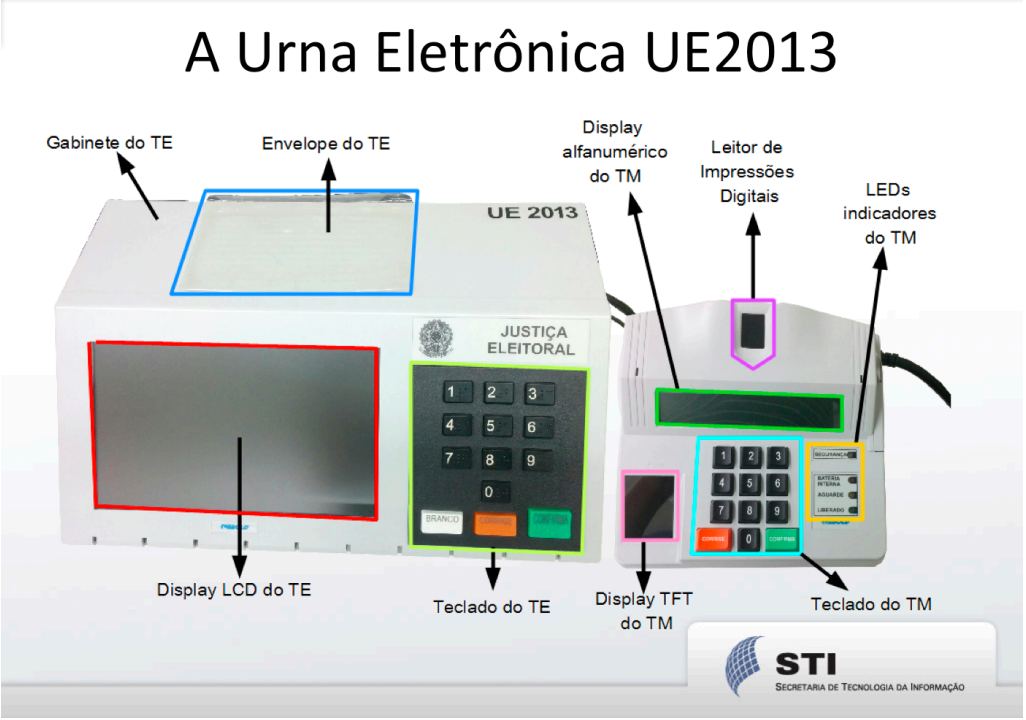
O último modelo de urna eletrônica desenvolvido até a publicação deste trabalho é a Urna Eletrônica modelo 2013 (UE2013). Basicamente é um dispositivo de coleta de votos composto de 2 módulos: um Terminal do Eleitor (TE) e um Terminal do Mesário (TM), ambos conectados por um cabo de dados. O Terminal do Mesário é o dispositivo em que o mesário ou presidente de mesa digita (habilita) o título de eleitor que comparece para votar. O Terminal do Eleitor é o dispositivo com o qual o eleitor interage para registrar o seu voto.

A figura 4.1 a seguir apresenta a face frontal de ambos os módulos da urna, que usaremos como referência para detalhar os componentes. A parte frontal do Terminal do Eleitor possui uma tela LCD (que não é sensível ao toque) e um teclado numérico (com disposição dos números equivalente ao teclado de telefone), cuja numeração das teclas conta

[11] Tribunal Regional Eleitoral do Rio Grande do Sul. Voto Eletrônico. Edição comemorativa: 10 anos da urna eletrônica; 20 anos do recadastramento eleitoral. 2006

com código braile em relevo. Além das teclas numéricas existem as teclas Branco, Corrige e Confirma. Esse teclado do TE possui a circuitaria resinada, para dificultar acesso ao circuito, um hardware de segurança denominado SCK (*Secure Ciphered Keyboard*) e possui curso das teclas com limiar de força (pressão de acionamento) especialmente especificadas para a finalidade da votação do eleitor.

Figura 4.1 – A Urna Eletrônica 2013 – Detalhamento frontal TE e TM.



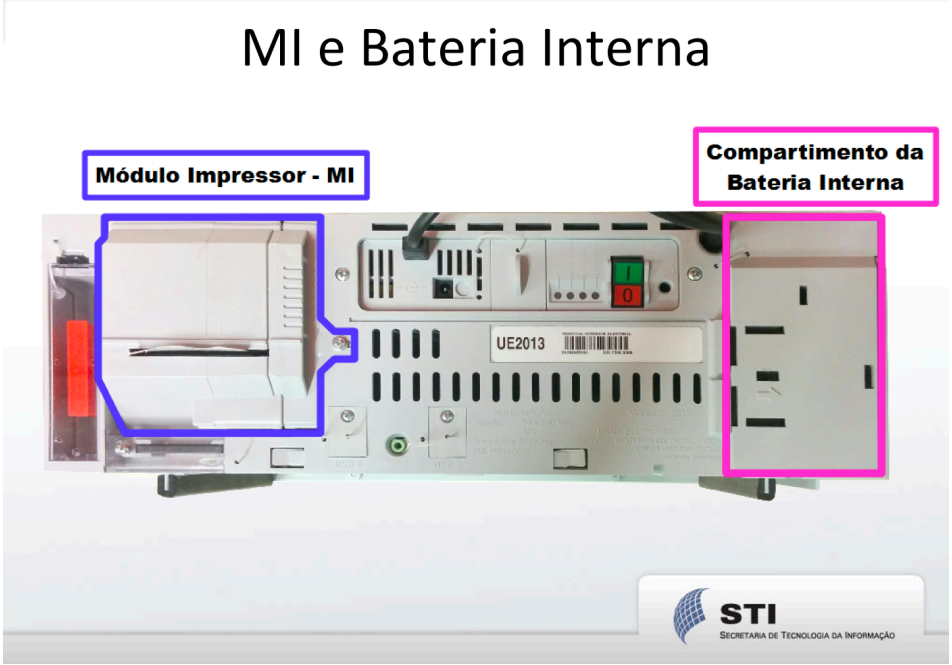
Fonte: TSE – Testes Públicos de Segurança (2016).

O Terminal do Mesário conta com teclado numérico (também conta com a disposição dos números equivalente ao teclado de telefone) além das teclas Corrige e Confirma. Além disso, o TM conta com um *display* alfanumérico de 4 linhas com 40 colunas que exibe informações relevantes ao mesário como: campo para digitar o título do eleitor ou códigos especiais (encerramento da votação, suspensão da votação, etc.), nome do eleitor, quantidade de eleitores na seção, quantidade de eleitores que já votaram, horário da urna, dentre outras informações que poderão ser citadas adiante, conforme relevância. Acima do *display* alfanumérico existe um leitor de impressões digitais (*DigitalPersona U.are.U 5301*). À esquerda do teclado numérico do TM existe um *display* TFT que futuramente deverá exibir a foto do eleitor para conferência visual do mesário. À direita do teclado numérico do TM existem 4 *leds* indicadores (Segurança, Bateria interna, Aguarde e Liberado). O Terminal do

Mesário ainda possui, em sua lateral, um leitor de *smartcard* e uma interface USB. Internamente possui um *hardware* de segurança denominado SMT (*Secure Micro Terminal*).

Além dos itens descritos anteriormente, a urna eletrônica possui, no gabinete do Terminal do Eleitor: um módulo impressor com uma impressora térmica (para impressão de relatórios e resultados da urna); dois drives para *compact flash*, que denominaremos Flash Interna (FI) e Flash Externa (FE); um drive USB para *pendrive*, que denominaremos de Memória de Resultado (MR); uma bateria removível, cuja autonomia é de aproximadamente 12 horas de duração; conectores para bateria externa; *leds* indicadores do estado de alimentação de energia; duas entradas USB; uma saída de áudio; uma saída de 12V; chave de liga/desliga, um potenciômetro para o controle de luminosidade na tela LCD. As figuras 4.2, 4.3, e 4.4 a seguir detalham o painel traseiro do gabinete do Terminal do Eleitor.

Figura 4.2 – A Urna Eletrônica 2013 – Detalhamento traseiro MI e Bateria Interna.



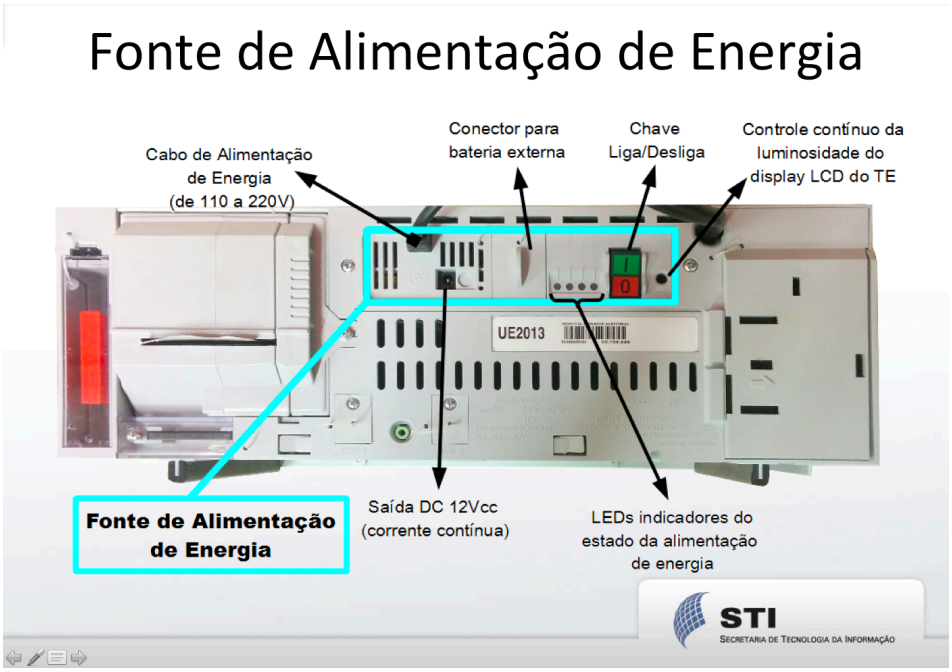
Fonte: TSE – Testes Públicos de Segurança (2016).

Segundo especificações de criptografia e segurança de hardware e software da urna eletrônica[12], as comunicações entre o terminal do eleitor, terminal do mesário e módulo impressor, com a placa-mãe da urna eletrônica, devem ser criptografadas, além de prover autenticação segura entre os dispositivos. A criptografia deve gerar um conjunto diferente dados a cada tecla pressionada, inclusive para repetição de teclas. A decifração e autenticação

[12] Processo TSE 20.038/2014 – Anexo IV

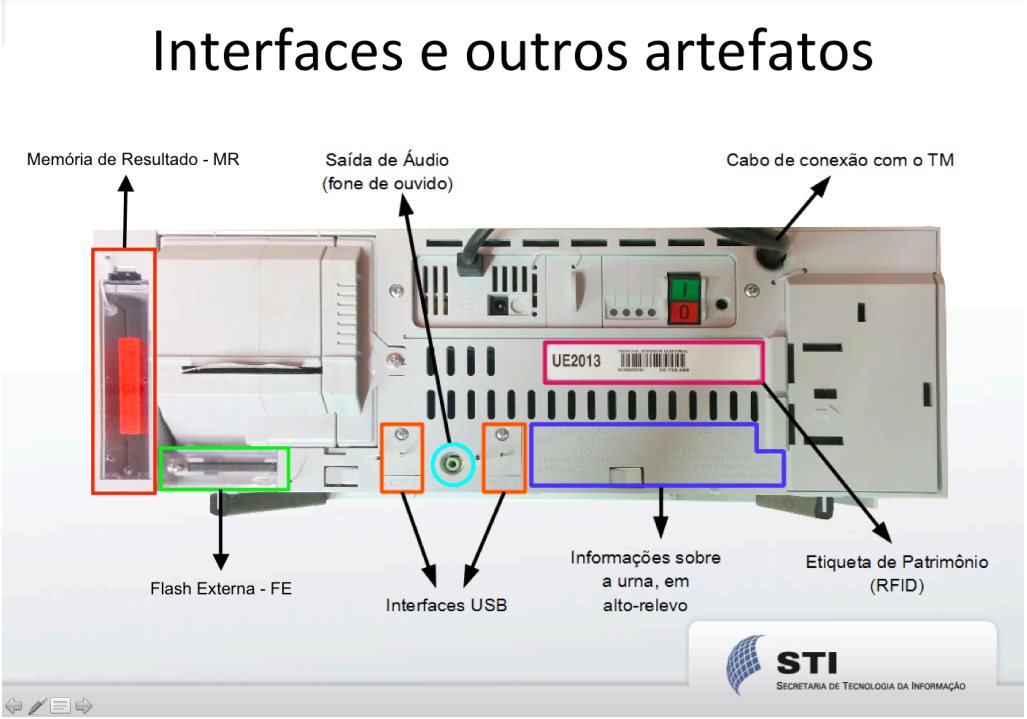
desses dados deve ser realizada por dispositivo de segurança específico em hardware na placa-mãe com chave protegida pelo dispositivo.

Figura 4.3 – A Urna Eletrônica 2013 – Fonte de Alimentação e Energia.



Fonte: TSE – Testes Públicos de Segurança (2016).

Figura 4.4 – A Urna Eletrônica 2013 – Armazenamento de Dados e Interfaces.

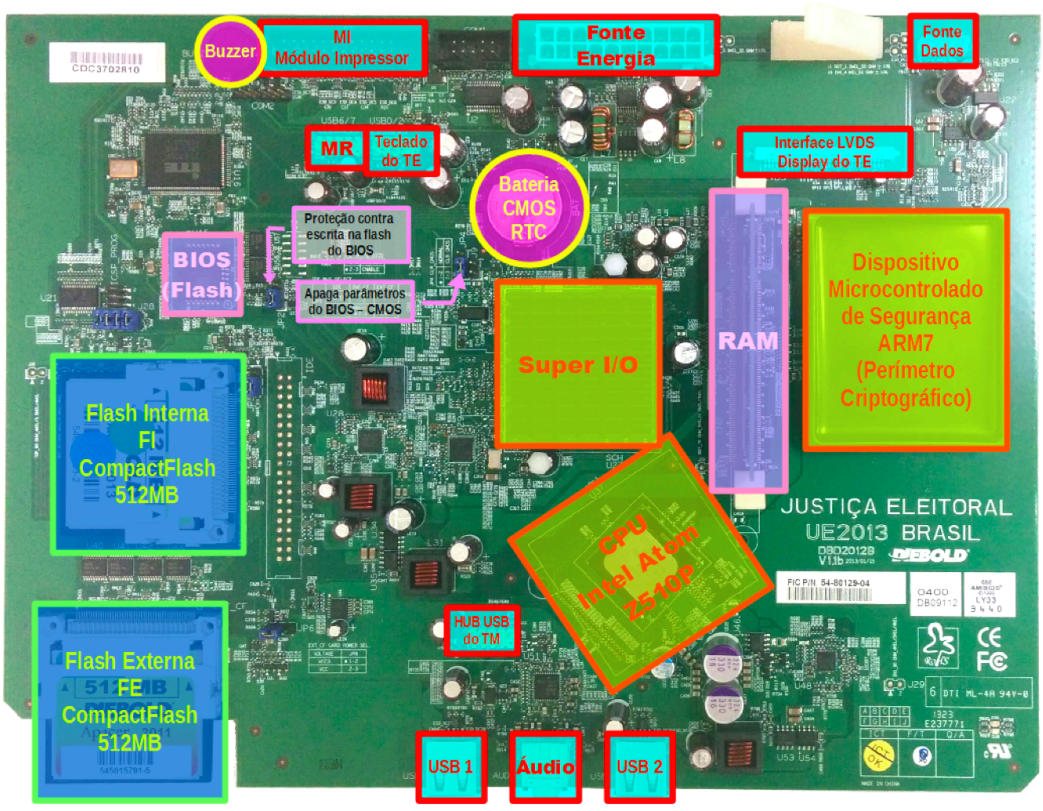


Fonte: TSE – Testes Públicos de Segurança (2016).

A Flash Externa e a Flash Interna estão fisicamente posicionadas na placa-mãe. Não há acesso à Flash Interna sem abertura do gabinete da urna e retirada da placa-mãe, enquanto que a Flash Externa está estrategicamente posicionada para acesso pela parte de trás do gabinete. A placa-mãe possui, além da CPU e do chip de BIOS, um dispositivo microcontrolado de segurança (MSD), que reside em um perímetro criptográfico (que está encapsulado, lacrado com resina para proteção) e é composto de um processador ARM7 e memória própria; um chip de *super-IO* que controla os dispositivos de entrada e saída; e um relógio de tempo real (*RTC – Real Time Clock*). Além disso, há um jumper para proteção contra escrita na *flash* BIOS e outro *jumper* que apaga os parâmetros do BIOS – CMOS conforme podemos observar na figura 4.5.

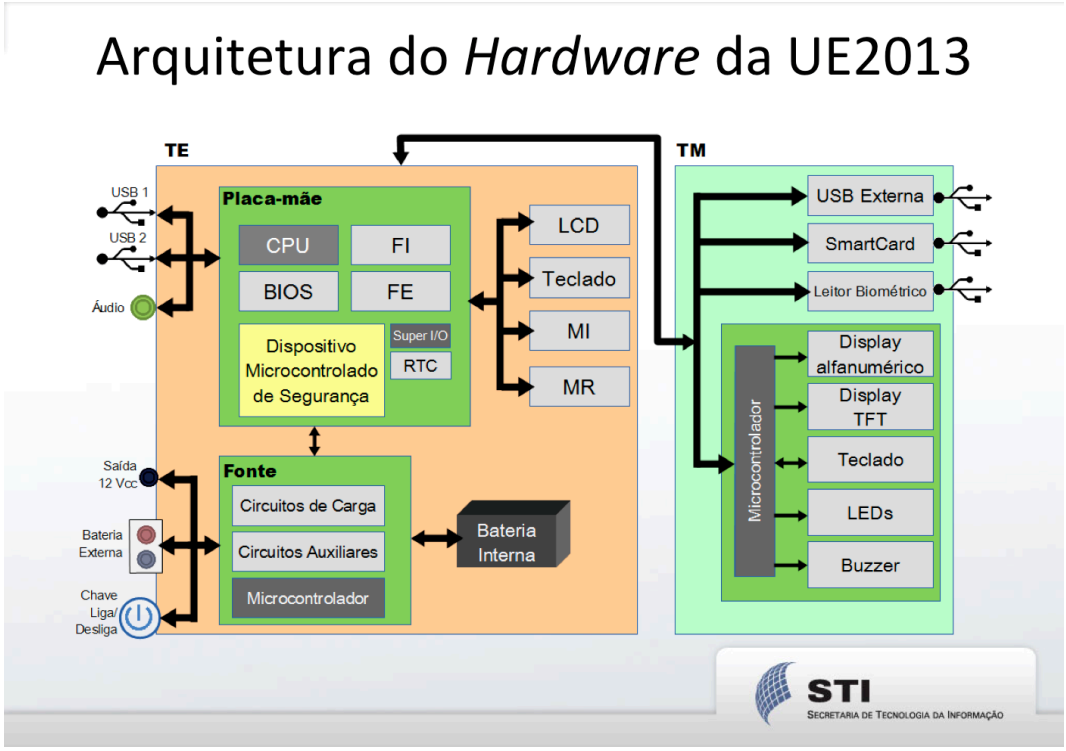
Com relação aos *leds* do Terminal do mesário cabe destacar a sinalização do indicador de segurança: Quando em amarelo piscante indica autenticação em processamento. Vermelho aceso indica processo de autenticação finalizado com sucesso mas com chave diferente da chave oficial do TSE. Vermelho piscante indica falha no processo de autenticação. Verde indica processo de autenticação finalizado com sucesso e com a chave oficial do TSE.

Figura 4.5 – A Urna Eletrônica 2013 – Componentes da placa-mãe.



Fonte: TSE – Testes Públicos de Segurança (2016).

Figura 4.6 – Hardware da Urna Eletrônica 2013



Fonte: TSE – Testes Públicos de Segurança (2016).

4.2 Software Básico da Urna Eletrônica

Os dados a seguir foram obtidos a partir da Palestra dos Testes Públicos de Segurança de 2016[13] que ocorreram na sede do TSE em Brasília. A urna eletrônica possui como software básico:

- BIOS (Sistema Básico de Entrada e Saída);
- *Bootloader* (Carregador do Sistema Operacional);
- Sistema operacional UENUX, assim como os drivers e bibliotecas do sistema;
- MSD (dispositivo microcontrolado de segurança)

O BIOS foi desenvolvido/adquirido pelo fabricante da urna eletrônica (Diebold). É gravado em memória não volátil e contém o código necessário para a comunicação com os dispositivos. Ele pode ser regravado pela própria urna. Se a urna eletrônica não tiver qualquer fonte de energia, o BIOS permanece na memória em que está gravado. Ele é assinado digitalmente pelo TSE e sua assinatura é verificada pela chave pública que foi inserida previamente na urna eletrônica.

[13] Tribunal Superior Eleitoral. **Apresentação Testes Públicos de Segurança**. Brasília, 2016.

O *Bootloader* é um pequeno código, desenvolvido e mantido pela SEVIN – Seção do Voto Informatizado do TSE, cuja função principal é carregar o Sistema Operacional (UENUX) a partir de uma memória *Compact Flash* para a memória RAM. Inicialmente a BIOS procura por um *bootloader* na Flash Externa e, caso não encontre, carrega o *bootloader* da Flash Interna – isso fará sentido quando descrevermos o procedimento de carga da urna eletrônica. Esse *bootloader* está localizado em posição específica da *CompactFlash* (no início da *flash*, de acordo com a geometria). Ele está assinado digitalmente pelo TSE e sua assinatura é verificada pela chave pública que foi inserida previamente na urna eletrônica.

O Sistema Operacional UENUX é uma distribuição Linux para uso exclusivo nas urnas eletrônicas brasileiras e é customizado e mantido pela SEVIN do TSE. Foi desenvolvido/construído a partir do *Kernel* do Linux, versão 2.6.16.62 (2008). É assinado digitalmente pelo TSE e sua assinatura é verificada pela chave pública previamente inserida na urna. Ele fica gravado na Flash Interna ou na Flash Externa e pode ser regravado pela urna eletrônica, conforme veremos no tópico que trata da carga de urna. O UENUX não possui comandos de terminal, por exemplo.

O dispositivo microcontrolado de segurança (MSD) é na verdade um hardware, mas como possui um firmware está sendo relacionado como um dos softwares básicos da urna. É um sistema computacional independente, com processador (ARM7) e memória próprios. Conforme descrito anteriormente, ele encontra-se segregado e resinado em um perímetro criptográfico na placa-mãe, para proteção. Possui ainda um circuito TRNG – *True Random Number Generator* (gerador de números realmente aleatórios). É um firmware mantido, adquirido e desenvolvido pela Diebold (fabricante da urna).

4.3 Encadeamento de Segurança Baseado em Hardware

Conforme Luís Augusto Consularo explica na edição de 2016 dos Testes Públicos de Segurança[14] a urna eletrônica, para a inicialização, possui um encadeamento de segurança baseado em hardware, que utiliza o dispositivo microcontrolado de segurança (MSD) presente no perímetro criptográfico da placa-mãe da urna eletrônica.

O MSD é o primeiro componente a ser energizado quando a urna eletrônica é ligada. O MSD faz a leitura e verifica a assinatura do BIOS com a chave pública previamente

[14] TSE. **Apresentação Testes Públicos de Segurança**. Brasília, 2016.

inserida na urna eletrônica. Se a assinatura for válida, coloca o BIOS em execução. Ao entrar em execução, o BIOS carrega o *bootloader* na memória e verifica sua assinatura utilizando o MSD. Se a assinatura for válida, coloca o *bootloader* em execução. O *bootloader* decifra o *kernel* do UENUX, verifica sua assinatura utilizando o MSD e, se assinatura for válida, coloca o UENUX em execução.

Assim que o UENUX entra em execução ocorre a validação do hardware da urna eletrônica. Um driver do sistema operacional verifica qual o modo de segurança que está em execução (Desenvolvimento, Simulado ou Oficial) e executa um desafio. Esse desafio consiste de um protocolo de desafio-resposta executado por uma aplicação no nível de usuário[15] conforme descrito a seguir:

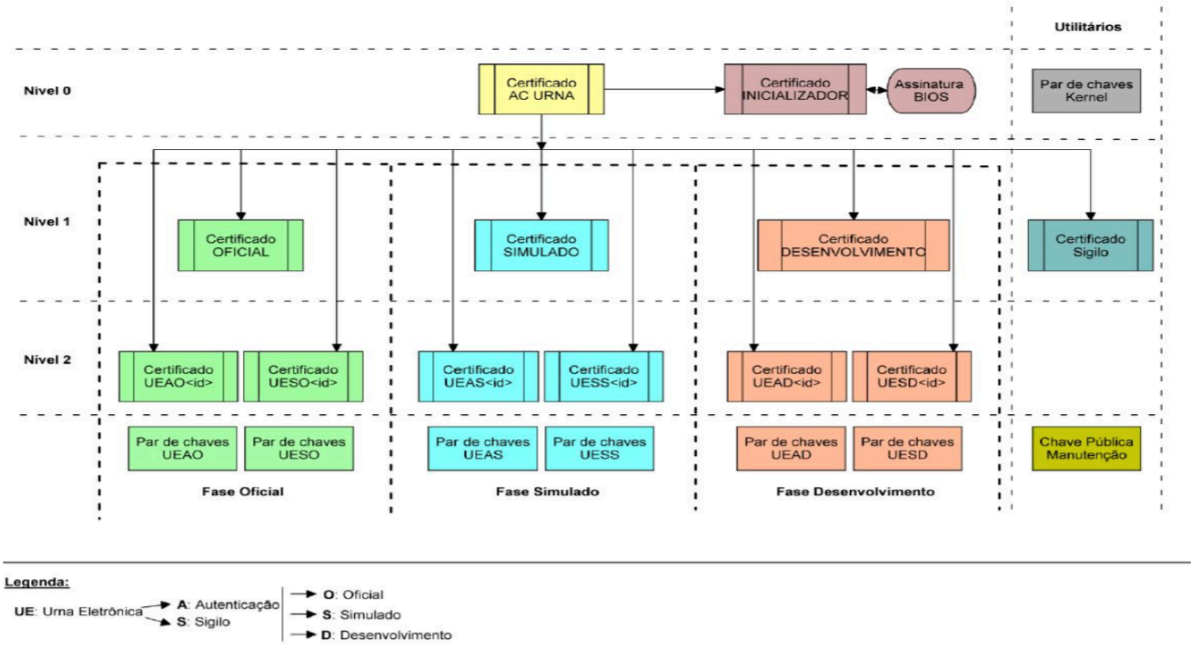
1. A aplicação autenticadora solicita os certificados da urna ao dispositivo de segurança (MSD);
2. Compara o certificado recebido com a sua cópia local do certificado AC da urna.
3. Gera 1024 bytes aleatórios e criptografa com a chave de sigilo da urna, recebida no passo 1;
4. Envia o criptograma para o dispositivo de segurança (MSD);
5. MSD decifra o criptograma, assina os dados decifrados e envia para a aplicação autenticadora;
6. Aplicação autenticadora verifica a assinatura com a cadeia de certificados enviada pelo hardware (MSD).

Se o MSD decifrar a informação, dentro de 4 min, ele sinaliza o UENUX indicando que o desafio foi resolvido. Caso ocorra o timeout após decorridos 4 min, o MSD sinaliza o UENUX de que o desafio não foi resolvido e que o hardware não é válido.

Com o hardware validado, o UENUX carrega o Gerenciador de Aplicativos da Urna (GAP) e verifica se a assinatura do GAP é válida. Se a assinatura for válida, coloca o GAP em execução. A figura 4.7 a seguir apresenta a hierarquia de certificados da urna. O certificados de nível 0 são armazenados obrigatoriamente no MSD.

[15] Processo TSE 20.038/2014 – Anexo IV

Figura 4.7 – Hierarquia de certificados e chaves da Urna Eletrônica



Fonte: TSE – Processo 20.038/2014 – Anexo IV, pág. 5

4.4 Segurança do Software

Existem 3 modos de segurança para os sistemas da urna eletrônica, sendo que cada um deles dispõe de um conjunto de chaves específicas:

- Desenvolvimento
- Simulado (para testes e treinamentos simulados).
- Oficial (utilizado exclusivamente nas eleições).

Na apresentação dos Testes Públicos de Segurança de 2016, Rodrigo Coimbra, da Seção do Voto Informatizado do Tribunal Superior Eleitoral apresentou alguns aspectos de segurança do ecossistema da urna que utilizam recursos criptográficos, os quais, em conjunto com o encadeamento de segurança baseado em hardware descrito anteriormente tem por objetivo garantir que apenas um software desenvolvido pelo TSE, e que foi submetido à Cerimônia de Assinatura Digital e Lacração dos Sistemas, será executado em modo oficial na urna eletrônica.

O sistema de arquivos (*filesystem*) dos cartões de memória da urna (ambas as *CompactFlash*) são criptografados com algoritmo AES-256, utilizando chaves diferentes para cada cartão de memória (Flash Interna e Flash Externa). O *bootloader* decifra o *kernel* do

Linux antes de colocá-lo em execução – a imagem do *kernel* do Linux é criptografada com AES-256. Todos os executáveis e bibliotecas dinâmicas tem assinatura RSA-1024 embutida no cabeçalho, que são verificadas pelo *kernel* do Linux, ou seja, o *kernel* do Linux só coloca em execução um software que contenha uma assinatura válida. Essas assinaturas são geradas na Cerimônia de Lacração dos Sistemas, como veremos mais adiante na seção 5.3. O *initje*, que é o responsável por fazer a chamada do sistema que coloca os outros softwares em execução faz verificação prévia do *hash* SHA-512 dos executáveis – esses resumos digitais (*hash*) também são gerados durante a Cerimônia de Lacração.

O sistema conta com assinatura digital que utiliza algoritmo de curvas elípticas de 256 bits – algoritmo de Estado desenvolvido pelo CEPESC/ABIN conforme estabelecido em norma específica[16]. São verificados com esse tipo de assinatura:

- todos os arquivos de dados que entram na urna (dados de candidatos, eleitores, seções, etc.)
- todos os arquivos de resultado que saem da urna
- *kernel* e todos os executáveis e bibliotecas

Os arquivos de resultado da urna recebem duas assinaturas: uma de hardware e outra de software. A assinatura de hardware, ESDC (*Elliptic Curve Digital Signature Algorithm*) de 521 bits utiliza o MSD. A assinatura de software utiliza a biblioteca desenvolvida pelo CEPESC/ABIN (ElGamal 256). O certificado digital da urna, que contém a chave pública, é anexado à assinatura digital para permitir a verificação, já que os cerificados da urna não são ICP-Brasil, pois foram gerados na autoridade certificadora do TSE.

A assinatura do QR Code do boletim de urna impresso utiliza um algoritmo de curvas elípticas, público, de código aberto (Ed25519 de 256 bits). Por ser de código aberto, qualquer pessoa pode inclusive criar seu próprio aplicativo para verificação, embora o TSE disponibilize um: Boletim na Mão, conforme será verificado mais adiante na seção 5.12.

A criptografia do RDV – Registro Digital do Voto (somente enquanto é mantido na urna) utiliza o protocolo AES-256. Por fim, as chaves privadas (do CEPESC) são gravadas como arquivos dentro da urna e são criptografadas com AES-256 (também com chaves diferentes das outras).

[16] Disponível em: <http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf>

5 PRINCIPAIS ETAPAS DE PREPARAÇÃO, PROCEDIMENTOS DE AUDITORIA E DISPOSITIVOS/BARREIRAS DE SEGURANÇA DA URNA

O objetivo da segurança no processo eleitoral é tornar a fraude inviável ou possibilitar a identificação de rastros. Para isso, são implementadas diversas barreiras de segurança, cuja função é impedir algum tipo de ação de um atacante ou pelo menos tornar essa ação cara ou demorada demais. As barreiras de segurança atuam em conjunto e devem ser analisadas dessa forma. Uma única barreira de segurança, quando analisada isoladamente, dificilmente fornecerá todos os requisitos de segurança desejáveis. Um claro exemplo que ilustra essa ideia é a utilização conjunta dos conceitos de criptografia, resumos digitais e assinatura digital para cobrir os quesitos de proteção/ocultação da informação, integridade dos dados e autenticidade. Ainda, determinadas barreiras de segurança tem simplesmente o objetivo de validar ou permitir a verificação dos resultados assim como a auditoria de determinadas etapas do processo. Também é necessário ressaltar que, por mais que um mecanismo de segurança seja importante, devemos analisar todo o contexto, com os possíveis riscos que ele pode trazer para outros aspectos como usabilidade, transparência e desempenho, não deixando de observar as premissas e requisitos para votação e conformidade com a legislação eleitoral vigente.

Neste capítulo serão apresentados algumas das barreiras de segurança mais importantes, o risco envolvido em cada etapa da eleição e como esses mecanismos atuam para garantir a lisura do processo eleitoral ou inviabilizar um possível ataque. É importante destacar que ficarão de fora dessa análise eventuais problemas com o julgamento de registro de candidatos e irregularidades na campanha por não fazerem parte do escopo desse trabalho, já que são ações de natureza jurídica e processual.

5.1 Arquitetura da Urna Eletrônica

A certificação digital das urnas eletrônicas e o encadeamento de segurança baseado em hardware com verificações de assinatura digital na BIOS, no *bootloader* e no Sistema Operacional, como vimos no capítulo 4, tem o propósito garantir que o software que está rodando na urna é autêntico – aquele que foi desenvolvido pelo TSE – ou seja, a Justiça Eleitoral precisa garantir a integridade do software rode na urna.

Para fins de segurança e transparência, há que se questionar se o software que o TSE desenvolve para o sistema faz realmente aquilo que se espera. Nesse sentido, a Justiça Eleitoral vem buscando ampliar a transparência dos processos, permitindo o acompanhamento do desenvolvimento e inspeção do código dos sistemas da urna, além da verificação e auditoria nas próprias urnas eletrônicas, como veremos a seguir.

5.2 Acompanhamento do Desenvolvimento e Análise do Código da Urna Eletrônica

Com o objetivo de aumentar a transparência no processo eleitoral e ampliar as rotinas de verificação e auditoria dos sistemas, a Justiça Eleitoral permite à diversas instituições acompanhar, nos 180 dias que antecedem a eleição, as fases de especificação e desenvolvimento dos programas que serão utilizados nas eleições[17]. Todo o processo de acompanhamento do desenvolvimento e inspeção do código dos softwares utilizados nas eleições estão previstos e regulamentados pela Lei nº 9.504/1997 (Lei das Eleições) e na Resolução TSE nº 23.458/2015 que dispõe sobre a cerimônia de assinatura digital e fiscalização do sistema eletrônico de votação, do registro digital do voto, da auditoria de funcionamento das urnas eletrônicas por meio de votação paralela e dos procedimentos de segurança dos dados dos sistemas eleitorais para o pleito de 2016.

Em relação ao acompanhamento e fiscalização do software, o artigo 1º estabelece:

> Art. 1º Aos fiscais dos partidos políticos e das coligações, à Ordem dos Advogados do Brasil, ao Ministério Público, ao Congresso Nacional, ao Supremo Tribunal Federal, à Controladoria-Geral da União, ao Departamento de Polícia Federal, à Sociedade Brasileira de Computação, ao Conselho Federal de Engenharia e Agronomia e aos departamentos de Tecnologia da Informação de universidades é garantido acesso antecipado aos programas de computador desenvolvidos pelo Tribunal Superior Eleitoral ou sob sua encomenda a serem utilizados nas eleições, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do Tribunal Superior Eleitoral.
>
> Parágrafo único. Serão fiscalizados, auditados, assinados digitalmente, lacrados e verificados todos os sistemas e programas, a saber:
>
> I - Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica;
>
> II - Preparação;
>
> III - Gerenciamento;
>
> IV - Transporte de Arquivos da Urna Eletrônica;
>
> V - JE-Connect;

[17] Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2016/Maio/desenvolvimento-dos-sistemas-da-urna-podem-ser-acompanhados-por-partidos-e-instituicoes

> VI - Receptor de Arquivos de Urna;
>
> VII - Votação, Justificativa Eleitoral, Apuração, utilitários, operacionais das urnas, de segurança;
>
> VIII - bibliotecas-padrão e especiais;
>
> IX - softwares de criptografia, inseridos nos programas utilizados nos sistemas de coleta, totalização e transmissão dos votos; e
>
> X - programas utilizados para compilação dos códigos-fontes de todos os programas desenvolvidos e utilizados no processo eleitoral[18]

O acompanhamento do desenvolvimento do software da urna eletrônica já era facultado a representantes indicados pelos partidos políticos, Ministério Público e Ordem dos Advogados do Brasil e, em 2015, foi ampliado às demais instituições relacionadas no art. 1º. A intenção do TSE, com a ampliação das entidades representativas da sociedade, é permitir maior controle e abrangência na fiscalização dos sistemas e no comportamento do software da urna eletrônica e, eventualmente, a colaboração na identificação de bugs no código. Repare que objetivo dessas ações tem caráter colaborativo e, portanto, não estamos falando na abertura do código, motivo pelo qual os representantes das entidades trabalham em um ambiente controlado no TSE e devem assinar um termo de confidencialidade em relação ao conteúdo desses códigos. A ampliação da transparência e abertura do código a mais interessados é um processo natural que deverá ocorrer com passar do tempo. O principal problema em relação à abertura do código é a descoberta de eventuais falhas ou vulnerabilidades sem o conhecimento do TSE e a oportunidade de correção imediata dos sistemas. Veremos mais sobre esses aspectos na seção que trata dos Testes Públicos de Segurança, mais adiante nesse capítulo.

Embora o prazo de aproximadamente seis meses para acompanhamento do desenvolvimento e análise seja curto para a quantidade de linhas de código envolvidas nesse processo – estamos falando de quase 12 milhões de linhas nos sistemas elencados – ele não é impossível, já que grande parte desse volume envolve o *kernel* do Linux e bibliotecas de terceiros. Além disso, o código-fonte utilizado ainda pode ser analisado após as eleições, mediante agendamento, pois são assinados digitalmente e guardados em sala cofre após a Cerimônia de Assinatura Digital e Lacração dos Sistemas, conforme veremos na próxima seção.

---

[18] Resolução TSE nº 23.458/2015. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-458-instrucao-53-765>.

5.3 Cerimônia de Assinatura Digital e Lacração dos Sistemas

Após o período do desenvolvimento e testes dos sistemas, ocorre no TSE, em até 20 antes da eleição, a Cerimônia de Assinatura Digital e Lacração dos Sistemas. Essa cerimônia está prevista na Lei nº 9.504/1997 (Lei das Eleições) e regulamentada pelos artigos 4º a 14º da Resolução do TSE nº 23.458/2015.

> Art. 4º Os programas relacionados no parágrafo único do art. 1º, após concluídos, serão apresentados, compilados, testados e assinados digitalmente pelo Tribunal Superior Eleitoral em Cerimônia de Assinatura Digital e Lacração dos Sistemas, que terá duração mínima de três dias.
>
> § 1º Os representantes dos partidos políticos, das coligações, da Ordem dos Advogados do Brasil, do Ministério Público, do Congresso Nacional, do Supremo Tribunal Federal, da Controladoria-Geral da União, do Departamento de Polícia Federal, da Sociedade Brasileira de Computação, do Conselho Federal de Engenharia e Agronomia e dos departamentos de Tecnologia da Informação de universidades que demonstrarem interesse poderão, ao final da Cerimônia, assinar digitalmente os programas relacionados no parágrafo único do art. 1º. [19]

Nessa cerimônia, os programas-fontes e executáveis são apresentados para inspeção e testes e, após a validação, são assinados digitalmente pela Justiça Eleitoral – as chaves privadas e senhas de acesso são mantidas em sigilo. Os representantes das entidades relacionadas no parágrafo 1º do artigo 4º, que tiverem interesse, também poderão assiná-los, desde que tenham manifestado interesse com antecedência e tenham apresentado seu respectivo certificado digital para conferência prévia de sua validade. Essas entidades também podem apresentar programa próprio para assinatura digital e verificação das assinaturas, que deverá ser homologado pela Secretaria de Tecnologia da Informação do TSE. Todas as assinaturas digitais de terceiros serão executadas por autoridade certificadora devidamente credenciada no Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil). Cabe observar que os programas próprios apresentados para verificação da assinatura digital não podem introduzir alterações nos sistemas, conforme descrito no art. 28:

> Art. 28. Não será permitida a gravação na urna ou nos sistemas e programas da Justiça Eleitoral de nenhum tipo de dado ou função pelos programas próprios apresentados pelos interessados para a verificação das respectivas assinaturas digitais.

[19] Resolução TSE nº 23.458/2015. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-458-instrucao-53-765>.

Esses programas também serão compilados na cerimônia de lacração e as entidades deverão assinar digitalmente os respectivos programas assim como as chaves públicas, que também serão assinados pelo representante da Justiça Eleitoral.

O artigo 8º da resolução estabelece:

> Art. 8º Após os procedimentos de compilação, assinatura digital e testes, serão gerados resumos digitais (*hash*) de todos os programas- fonte, programas-executáveis, arquivos fixos dos sistemas, arquivos de assinatura digital e chaves públicas.[20]

Todos os resumos digitais serão inseridos em um arquivo que será assinado pelo presidente do TSE e pelos representantes das entidades relacionadas no parágrafo 1º do artigo 4º que tiverem interesse. Uma cópia desse arquivo será enviado a todos os representantes das entidades e também publicada na página de internet do Tribunal Superior Eleitoral.

Após a compilação, assinatura digital e geração dos resumos digitais (*hashes*) dos arquivos, eles serão lacrados conforme descrito no artigo 10º a seguir:

> Art. 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 digital 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 da Secretaria de Tecnologia da Informação do Tribunal Superior Eleitoral.

Caso haja necessidade de alterações nos sistemas, após prévia autorização do presidente do TSE, as entidades serão comunicadas para que compareçam e os programas sejam novamente analisados, compilados, assinados digitalmente e sejam gerados novos resumos digitais.

No prazo de 5 dias após o encerramento da Cerimônia de Assinatura Digital e Lacração dos Sistemas, as entidades poderão impugnar os sistemas apresentando petição fundamentada que será analisada pelo TSE.

Como podemos observar, a sistemática de lacração dos sistemas está baseada em 3 princípios:

- **Assinatura Digital** pela Justiça Eleitoral e demais entidades garante a autenticidade dos programas, além do fato de que o TSE não vai alterar os

[20] Resolução TSE nº 23.458/2015. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-458-instrucao-53-765>.

sistemas sem a anuência das outras partes interessadas, sempre que houver pelo menos assinatura de mais uma entidade.

- **Geração de Resumos Digitais** (*hashes*) garante a integridade dos arquivos, permitindo comparar os arquivos das urnas e demais sistemas com aqueles apresentados na cerimônia de lacração, a fim de verificar se eles não foram modificados após a cerimônia
- **Lacre Físico de Mídia não Regravável** de todos os programas-fonte, resumos digitais, programas compilados e outras informações, em invólucro assinado pelos presentes e armazenado em sala cofre permite verificar, a qualquer momento, se os programas são os mesmos lacrados, além de possibilitar a inspeção do código em busca de erros.

O Partido da Social Democracia Brasileira apresentou sugestões[21] objetivando aumentar a transparência em relação a segurança do software de votação, as quais foram acatadas parcialmente pelo TSE. Dentre elas, cabe destaque nesse tópico a sugestão nº 1, que diz respeito aos sistemas que seriam fiscalizados, auditados, assinados digitalmente pelas entidades interessadas e posteriormente lacrados. Eles relacionavam, além dos sistemas que já estão previstos na resolução, a assinatura digital das entidades interessadas no software de inicialização embarcado (*firmware*) no BIOS (*Basic Input Output System*) e nos circuitos de segurança como o MSD (*Master Secure Device*), o SMT (*Secure Micro Terminal*) e o SCK (*Secure Ciphered Keyboard*).

A manifestação técnica apresentada pela Secretaria de Tecnologia da Informação solicitou a exclusão desses itens porque o procedimento de gravação da BIOS nas urnas eletrônicas exige a abertura e retirada da placa-mãe de mais de meio milhão de urnas no país, para ajuste (inversão) de um jumper que permitisse a execução de uma rotina de software. Assim, além de o período entre a cerimônia de cargas e a eleição ser extremamente exíguo para esse tipo de atividade, não se encaixaria nos custos de manutenção preventiva do contrato atual. Ainda, a atualização do firmware dos MSD, SMT e SCK, com versões assinadas digitalmente pelas entidades, exigiria um procedimento de execução do sistema de atualização que dura em média 10 min por urna, além da geração de requisição de certificados digitais, que seriam encaminhados para o TSE – os quais seriam gerados na Autoridade

[21] Voto do Relator Ministro Gilmar Mendes na instrução 537-65.2015: Páginas 34 a 49. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-458-instrucao-53-765>

Certificadora localizada na sala cofre – e, posteriormente, enviados de volta aos TREs para inoculação nas urnas eletrônicas através da execução de um sistema específico para isso. Esse processo envolveria a geração de aproximadamente 2.160.000 certificados digitais para cada ciclo eleitoral, o que, da mesma forma que o procedimento de atualização da BIOS, não seria possível de realizar em tempo hábil. Por fim, recomendava o aprofundamento dos estudos para implementação futura dessa sugestão, destacando a necessidade de ampliação da equipe responsável pela gestão dos certificados digitais – atualmente composta por 3 membros – e programação para o início das atividades imediatamente após o término de um ciclo eleitoral. Somente assim seria possível a atualização em todas as urnas do país, além dos procedimentos de testes exaustivos a fim de verificar a ocorrência de bugs – que demandaria nova atualização do firmware.

5.4 SIS – Subsistema de Instalação e Segurança

As estações de trabalho da Justiça Eleitoral que utilizam sistemas eleitorais responsáveis pelo cadastro de eleitores e geração de mídias para as urnas eletrônicas têm, obrigatoriamente, um Subsistema de Instalação e Segurança (SIS) desenvolvido dentro do Tribunal Superior Eleitoral. Esse subsistema incorpora e gerencia as funções de controle de acesso aos usuários, backup, auditoria, instalação automatizada de pacotes criptografados com os sistemas eleitorais, oficialização de sistemas eleitorais, dentre outras.

O acesso de usuários administradores do sistema é realizado por meio de contrassenhas. Assim, mesmo de posse da senha de administrador, será necessária a validação com um número de título eleitoral que identifica o usuário em questão, além de ligar para um dos Tribunais Regionais Eleitorais e solicitar uma senha de acesso temporária. Essa contrassenha só valerá para a data, horário, máquina e usuário especificado em tela no momento do acesso.

Qualquer sistema eleitoral desenvolvido pelo TSE só poderá ser instalado e acessado em máquinas com o SIS. As versões oficiais, assinadas digitalmente e lacradas no TSE, só poderão ser instaladas na versão oficial do SIS para o pleito em questão, a qual conterá os certificados digitais válidos com as chaves públicas para a conferência das assinaturas digitais dos sistemas no momento de sua instalação. A instalação dos sistemas é totalmente automatizada e é feita por meio de um usuário administrador do sistema específico para esse fim (usuário instalador). A distribuição dos arquivos de instalação é feita por meio de um

pacote seguro, criptografado. Esse pacote é selecionado por meio da aplicação de instalação segura de programas controlados, que decriptografa o pacote, verifica a assinatura digital (se for uma versão oficial) e instala o sistema no local apropriado – em uma partição segura e criptografada da máquina, no caso dos sistemas para geração das mídias da urna eletrônica ou transmissão dos arquivos de resultado. Dessa forma, mesmo que um sistema eleitoral seja interceptado, ele não poderá ser instalado em um computador externo à Justiça Eleitoral.

O acesso aos sistemas eleitorais é restrito e cada gestor de autorizações concederá aos usuários uma permissão de acesso específica de acordo com o nível de privilégios adequado. As versões oficiais dos sistemas eleitorais também são restritas e cada sistema só poderá ser utilizado em sua versão oficial após o procedimento de oficialização mediante senha específica remetida à autoridade eleitoral competente.

5.5 Cadastro Biométrico

O cadastro de eleitores da Justiça Eleitoral é o maior da América Latina. A inclusão do registro de um eleitor é feita com base no documento de identidade apresentado pelo eleitor e no comprovante de residência. Assim, era possível que uma mesma pessoa tivesse títulos eleitorais distintos em diferentes estados. Embora houvesse um esforço grande de batimento nesse cadastro em busca de duplicidade de títulos eleitorais, através do cruzamento dos dados de nome, data de nascimento e filiação, esse procedimento não era imune a fraudes e crimes de falsidade ideológica, frequentemente cometidos por estelionatários no Brasil. Para isso, bastava que um cidadão apresentasse um documento com um nome, data de nascimento e filiação sem equivalência no cadastro nacional de eleitores.

O cadastro biométrico do eleitorado começou a ser implantado na Justiça Eleitoral a partir de 2008 para corrigir essa deficiência. Em maio de 2016, o cadastro nacional do eleitorado já contava com mais de 46 milhões de eleitores com dados de biometria (coleta de foto, digital e assinatura) de acordo com os dados estatísticos no site do TSE. Além de impedir que um eleitor vote no lugar de outro, o batimento biométrico permite a identificação de duplicidade ou multiplicidade de títulos de eleitor mesmo que os nomes sejam diferentes, com base na varredura automatizada dos dados biométricos do eleitorado. Isso é garantido através do sistema IAFIS que é a sigla em inglês para Sistema Automático de Identificação de Impressões Digitais. Segundo o Secretário de Tecnologia da Informação do TSE, Giuseppe Janino, o sistema IAFIS permite comparar até 160 mil digitais por dia. Conforme os dados do

TSE, até as eleições de 2014 já havia sido realizado o batimento de 24 milhões de títulos cadastrados, identificando 5.556 casos de duplicidade e o incrível caso de um cidadão que possuía 47 títulos de eleitor[22].

Ainda segundo Janino, *"Os dados biométricos básicos que nós colhemos são as digitais de todos os dedos e a fotografia dentro de requisitos de padrão internacional, que permite fazer a análise matemática da face. Quando não há elementos suficientes para individualizar o cidadão por meio das suas digitais, recorre-se, também, à fotografia e, a partir daí, por meio de dados matemáticos, comparam-se também fotos"* havendo inclusive a possibilidade de que um papiloscopista faça uma análise minuciosa dos dados da digital de um eleitor. Como último recurso, ainda pode ser utilizada a assinatura do eleitor que não possuir elementos ou minúcias suficientes para sua identificação, já que nem todas as pessoas possuem uma digital com boa qualidade, e isso também é uma característica biométrica.

É inegável que o sistema biométrico confere mais segurança à identificação do eleitor no momento da votação, tornando praticamente inviável a fraude em que um eleitor tenta se passar por outro. Dessa forma, caminhamos para um sistema de votação cada vez mais democrático e seguro, na medida em que aumentamos a precisão e confiabilidade do cadastro nacional de eleitores.

5.6 Geração de Mídias

O procedimento de Geração de Mídias para as urnas é feito exclusivamente através de um aplicativo desenvolvido para o sistema operacional Windows, o Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE). Esse aplicativo importa todos os dados necessários para as urnas eletrônicas (dados do processo eleitoral, configuração de município, dados de eleitores, seções eleitorais, mesas de justificativa, agregações de seção, eleitores impedidos de votar, dados de candidatos, além do software da urna eletrônica).

Uma vez que o GEDAI-UE esteja configurado com todos os dados é possível proceder com a geração das seguintes mídias:

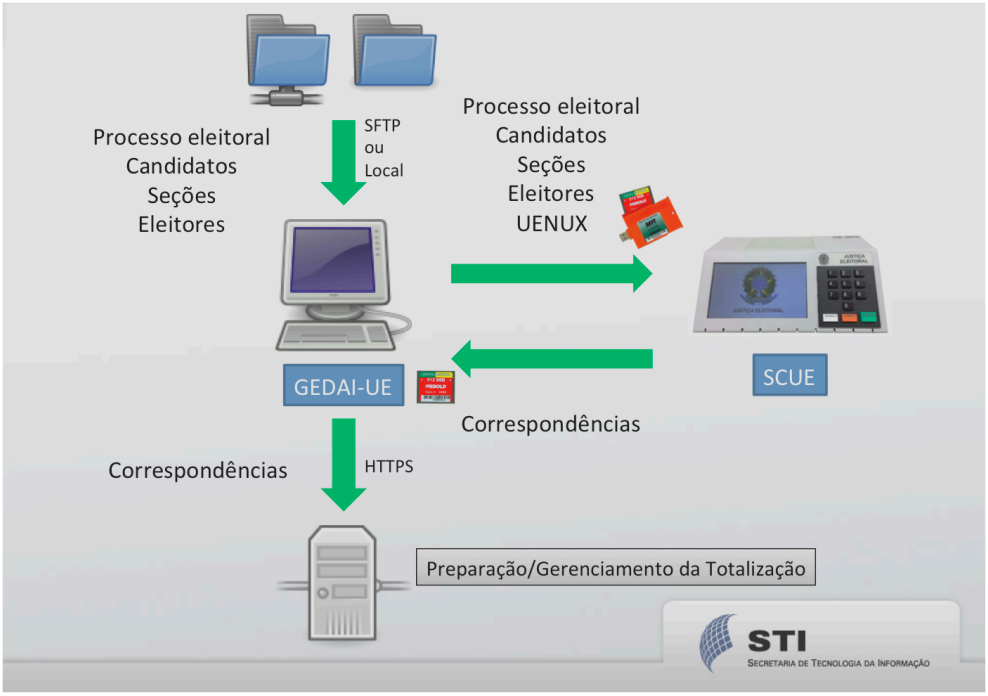
- Flash de Carga (FC) – cartão de memória do tipo *compact flash* contendo o sistema operacional da urna (UENUX), todos os aplicativos da urna, dados de

[22] http://www.tse.jus.br/imprensa/noticias-tse/2016/Janeiro/serie-urna-eletronica-sistema-de-batimento-biometrico-confere-mais-seguranca-as-eleicoes

candidatos que concorrem na eleição e dados de eleitores das seções eleitorais selecionadas.

- Flash de Votação (FV) – cartão de memória contendo as fotos dos candidatos que concorrem na eleição.
- Mídia de Resultado (MR) – *pendrive* que inicializa o aplicativo de votação (vazio) ou que contém marca de inicialização para um ou mais dos demais aplicativos da urna (recuperador de dados, sistema de apuração, ajuste de data e hora, etc.).

Figura 5.1 – Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica



Fonte: TSE – Testes Públicos de Segurança (2016).

O sistema GEDAI-UE possui registro no log com as quantidades e tipos de mídias geradas. A Flash de Carga recebe, em média, os dados de 50 seções eleitorais (eleitores). As seções geradas são excluídas da lista de seções disponíveis automaticamente para geração da próxima Flash de Carga. Assim, evita-se a geração de cartões de memória com dados de eleitores e seções duplicados. O objetivo desse mecanismo é manter o controle sobre as Flash de Carga. Em caso de necessidade (*flash* corrompida, por exemplo) ainda é possível regerar uma nova Flash de Carga com os dados de seções que já foram geradas anteriormente. É importante destacar que cada cartão de memória possui um número serial que identifica uma *flash*. Portanto, através dos relatórios de sistema é possível identificar quais seções foram geradas em cada *flash card*.

Os procedimentos relativos à Geração de Mídias estão regulamentados e descritos no Capítulo IV da Resolução 23.456/2015[23], o qual trata da preparação das urnas para a eleição. Todas as mídias devem ser geradas em cerimônia específica para esse fim (Cerimônia de Geração de Mídias), cujo edital deve ser publicado com antecedência mínima de 2 dias, dando publicidade necessária para que os fiscais dos partidos e coligações e demais partes interessadas compareçam ao evento para fins de fiscalização e auditoria dos trabalhos. Nesse momento, poderão ser verificadas as assinaturas digitais dos sistemas oficiais utilizados para a Geração de Mídias e impressos os relatórios com os registros das mídias geradas.

Após a geração das mídias e lavração da Ata de Geração de Mídias, informando a quantidade e os tipos de mídias gerados, os cartões de memória de Carga deverão ser acondicionados em envelope específico que será lacrado e guardado sob responsabilidade da autoridade eleitoral até o dia da Cerimônia de Carga das Urnas, que será abordada na próxima seção. É de extrema importância o correto controle de todos os cartões de memória (Flash de Carga e Flash de Votação), pois, de posse desses cartões de memória e das mídias de resultado será possível instalar o sistema oficial da eleição em qualquer urna certificada pela Justiça Eleitoral. Abordaremos os aspectos de segurança sobre o controle de todas as cargas de urna na seção 5.8, que trata da tabela de correspondências.

5.7 Carga das Urnas Eletrônicas

O procedimento de instalação do software oficial da eleição nas urnas eletrônicas é realizado nos Tribunais Regionais Eleitorais ou Cartórios Eleitorais durante a Cerimônia de Carga das Urnas Eletrônicas. Esses procedimentos também estão regulamentados no Capítulo IV da Resolução 23.456/2015[24] que trata dos Atos Preparatórios para as Eleições Municipais de 2016.

Para a Cerimônia de Carga das Urnas deverá ser publicado edital com antecedência mínima de dois dias, de forma a dar publicidade às entidades interessadas em acompanhar ou auditar o processo de carga das urnas eletrônicas. No dia e hora especificados no edital, e na presença dos fiscais dos partidos políticos, coligações e demais representantes das entidades

[23] Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-456-instrucao-53-680>

[24] Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-456-instrucao-53-680>

legitimadas (Ministério Público, Ordem dos Advogados do Brasil, etc.) será realizada a carga das urnas eletrônicas de seção, de mesas receptoras de justificativa e de urnas de contingência.

O procedimento de carga das urnas eletrônicas é um processo automatizado de instalação do software no qual é inserido um cartão de memória de carga (Flash de Carga) no drive da Flash Externa e a urna é ligada. A urna passa pelo processo de verificação do software, conforme descrito no Encadeamento de Segurança Baseado em Hardware da seção 4.3. Se estiver tudo correto, o Software de Carga da Urna Eletrônica (SCUE) apresentará a data e hora atuais da urna para confirmação. Em seguida, o operador da Justiça Eleitoral deverá digitar a data e hora da urna eletrônica, de acordo com o horário oficial local, e escolher o número da seção eleitoral que será carregada na urna. A urna eletrônica sempre oferece o menor número de seção disponível no cartão de memória de carga, que ainda não foi carregada. Uma vez carregada a seção a partir de um cartão de memória, ela não será oferecida novamente, a não ser que o operador escolha explicitamente dar nova carga para uma seção já carregada. Esse procedimento ajuda a evitar que uma mesma seção seja carregada mais de uma vez, acidentalmente.

Após o procedimento de configuração de data e hora e escolha da seção, o SCUE – que está rodando a partir do cartão de memória de carga presente no drive da Flash Externa – formatará o cartão de memória presente no drive da Flash Interna e instalará o sistema operacional e todos os aplicativos da urna eletrônica, além dos eleitores da seção escolhida e dos dados dos candidatos que concorrem à eleição. Concluída a instalação e cópia dos dados necessários, será gerado um relatório denominado Extrato de Carga da Urna, que conterá informações relevantes como nome do município e seção, data e hora da carga, código de identificação da urna e do cartão de memória de carga, código de identificação da carga, dentre outros. Nesse momento o SCUE solicita que sejam verificados os dados no Extrato de Carga e em seguida solicita que a urna eletrônica seja desligada, retirada a Flash de Carga e sejam inseridos a Flash de Votação e a Mídia de Resultado de Votação nos respectivos compartimentos (drive da Flash Externa e drive da Mídia de Resultado).

Na próxima etapa da carga da urna eletrônica o sistema será inicializado a partir da Flash Interna, já que não temos mais a Flash de Carga no drive da Flash Externa. O mesmo processo de validação da urna durante a inicialização ocorrerá. O SCUE identificará uma Flash de Votação não utilizada e copiará os dados de candidatos e eleitores da Flash Interna para a Flash Externa em um procedimento denominado sincronismo de *flash*. Após o sincronismo de *flash*, a urna entra em um processo de auto-teste que exigirá um pouco mais de intervenção do operador, a fim de verificar o correto funcionamento de todos os

dispositivos do equipamento. Se tudo estiver correto e a urna passar por todas as etapas de verificação, será exibida uma tela com a mensagem de que a urna só funcionará a partir das 7h do dia da eleição. Nesse momento, a urna deverá ser desligada, lacrada com lacres confeccionados pela Casa da Moeda e assinados pela autoridade eleitoral, armazenada em sua caixa e devolvida à prateleira, onde aguardará o dia da distribuição das urnas eletrônicas.

Os fiscais dos partidos políticos poderão solicitar a auditoria em até 3% das urnas eletrônicas carregadas de cada município. Nessa auditoria serão conferidas as assinaturas digitais através de programa específico do TSE, ou de programa próprio homologado na Cerimônia de Assinatura Digital e Lacração dos Sistemas. Também serão impressos os resumos digitais dos arquivos estáticos das urnas, visualizados os logs e, eventualmente, poderá ser forçada a votação através de programa específico de auditoria do TSE (VPP – Verificador Pré-Pós Eleição). Se não houver interessados em auditar as urnas eletrônicas, um servidor designado da Justiça Eleitoral deverá auditar, obrigatoriamente, pelo menos uma urna por município a fim de verificar os resumos digitais dos arquivos da urna eletrônica. Caso seja forçada a votação em uma urna através do software de Verificação Pré-Pós Eleição, essa urna deverá passar por novo procedimento de carga, a fim de que todos os dados sejam apagados para que ela esteja em condições de ser enviada para votação no dia da eleição.

Todos os relatórios e extratos de carga referentes à auditoria e carga das urnas deverão ser anexados à Ata da Cerimônia de Carga, que ficará à disposição dos partidos políticos e coligações em caso de auditoria. As informações de carga das urnas eletrônicas, presentes na Flash de Carga (veja a seção 5.8 a seguir, que trata da tabela de correspondências), deverão ser recebidas no sistema GEDAI-UE e transmitidas para o Tribunal Regional Eleitoral. Esse processo de recebimento da tabela de correspondência pode ser feito pela leitura da Flash de Carga, ou, em caso de dados corrompidos na *flash*, com digitação dos dados do Extrato de Carga, em função específica do GEDAI-UE.

É importante destacar que o procedimento de carga é quase totalmente automatizado e há muito pouca interação entre o operador responsável pela carga e o software de carga: digitação de data e hora, escolha da seção e auto teste. Ao final da carga a urna estará lacrada e o software da urna estará travado até o dia da eleição. Ligar novamente a urna eletrônica apenas levará à mesma tela de informação de que ela só funcionará a partir das 7h do dia da eleição, além de fazer os registros de todas as operações no log da urna. A possibilidade de fraudar uma urna carregada é bastante remota, pois qualquer tentativa de inserir um novo cartão de memória ou mídia de resultado passa necessariamente pelo rompimento dos lacres. Ainda que os lacres sejam rompidos, a inserção de um novo cartão de memória ou mídia de

resultado só funcionará se contiver um sistema oficial do TSE. Se for inserido um novo Flash de Carga, o aplicativo SCUE informará sobre a existência de uma carga oficial na urna. Seria possível prosseguir com a carga – procedimento que formatará a Flash Interna, dando início a um novo processo de carga. Se for inserido um Flash de Votação não utilizado, a urna passará por um novo processo de sincronização do conteúdo da Flash Interna com a Flash Externa – abordaremos esse processo com mais detalhes quando tratarmos dos procedimentos de contingência. Caso seja utilizada uma Flash de Votação com dados de seção (ou de votação) que não sejam os do sincronismo original, mesmo que seja uma Flash de Votação da mesma seção, a urna apresentará erro de sincronismo entre as flash interna e externa, fazendo registro dessa operação no log e travando a urna.

Alguns dias antes da votação, as urnas ainda passam por um processo de conferência dos dados em tela, com a ajuda de um aplicativo que lê o QR Code no *display* da urna. Esse QR Code contém as informações de carga: zona, seção, data, hora e código de identificação de carga. O aplicativo contém as informações da tabela de correspondência que foram transmitidas ao TRE, conforme veremos na próxima seção. Basicamente esse processo de conferência serve para identificar erros de digitação de data e hora de carga, urnas trocadas na caixa, problema de relógio da urna ou, ainda, divergência entre o código de identificação da carga da urna que vai para a seção e o código de identificação de carga esperado pelo sistema de totalização no TRE. A próxima seção explicará o funcionamento desses códigos de identificação de carga, que estão disponíveis na tabela de correspondências.

5.8 Tabela de Correspondências

Ao processo de carga das urnas eletrônicas está associado um mecanismo de segurança denominado tabela de correspondências. Cada carga de urna eletrônica produz um identificador único chamado de código de identificação de carga. Esse identificador é produzido por uma função que associa o código do município, número da seção eleitoral, serial da urna eletrônica, serial da Flash de Carga, data e hora da carga e um número aleatório (produzido pelo /dev/urandom) – cujo objetivo é gerar um número distinto mesmo que seja reproduzida uma nova carga na mesma urna e com os mesmos dados de entrada. Além disso, conforme Rodrigo Coimbra, da Seção do Voto Informatizado do TSE, "*é adicionada uma assinatura de comprimento reduzido (emparelhamentos bilineares) para o código de identificação da carga. O objetivo dessa assinatura é prover segurança, de modo a impedir*

que uma correspondência forjada entre no sistema. Dessa forma, somente uma correspondência gerada pelo SCUE poderá ser digitada no GEDAI-UE. A assinatura também ajuda na manutenção da integridade e autenticidade das informações da tabela de correspondências gravadas localmente no banco de dados do GEDAI-UE". Assim, a tabela de correspondências conterá, para cada seção carregada, as informações de data e hora da carga, número de série da urna, número de série da Flash de Carga utilizada para dar carga na urna, data e hora da transmissão da correspondência, o código de identificação da carga, assinatura da carga e o *status* da correspondência, que abordaremos mais adiante nessa seção.

A partir do procedimento de carga de uma urna eletrônica, o código de identificação e as demais informações da tabela de correspondência estarão presentes em vários relatórios, para fins de verificação e auditoria. Podemos citar entre eles: o extrato de carga da urna que será afixado na Ata da Cerimônia de Carga; o comprovante de carga que acompanha a urna eletrônica; a zerésima da seção, que é impressa obrigatoriamente antes da votação e é um relatório que indica a inexistência de votos na urna eletrônica; o boletim de urna da seção, que é impresso ao final da votação e possui o extrato da votação daquela seção eleitoral; o relatório de carga das urnas eletrônicas, no sistema GEDAI-UE; a tabela de correspondências esperadas que é publicada no site da internet do Tribunal Superior Eleitoral e disponibilizada aos partidos políticos e coligações para fins de auditoria, até a véspera da eleição.

Observa-se portanto, que toda a carga de urna eletrônica será registrada na tabela de correspondência, o que vai ao encontro de um dos objetivos dessa tabela: as urnas eletrônicas devem ser carregadas estritamente dentro do prazo previsto no edital da Cerimônia de Carga da Urnas, que é publicado com dois dias de antecedência, permitindo aos fiscais e representantes dos partidos comparecer à cerimônia para fins de auditoria e fiscalização dos trabalhos.

Quando o resultado de votação de uma seção é transmitido ao TRE, o sistema verifica qual o código de identificação de carga da urna que gerou o resultado e compara com o código de identificação de carga na tabela de correspondências esperadas pelo sistema. Esse resultado só será aceito pelo sistema, ou seja, será computado na totalização, se houver essa correspondência. Caso contrário, o resultado dessa seção entrará em pendência, exigindo uma intervenção da autoridade eleitoral competente: o juiz eleitoral, em eleições municipais, ou o presidente do Tribunal Regional Eleitoral, nas eleições gerais.

As intervenções possíveis para o tratamento de uma pendência são o processamento ou a exclusão. O processamento é o ato de validar a pendência, autorizando a entrada do resultado da seção no sistema de totalização. Ele deve ser bem fundamentado, com uma

explicação detalhada do motivo pelo qual ocorreu a pendência. Um exemplo didático para entender a ocorrência de uma pendência é uma nova carga de urna no dia eleição antes do início da votação. A tabela de correspondência deve ser transmitida até a véspera da eleição para dar publicidade aos partidos políticos de todas as correspondências esperadas. Se, ao tentar iniciar a votação na seção, a urna eletrônica apresentar um problema crítico que não seja possível recuperá-la, nem mesmo através dos procedimentos de contingência, o juiz eleitoral pode autorizar, mediante consulta à Secretaria de Tecnologia da Informação do TRE, uma nova carga de urna para essa seção eleitoral, que gerará um novo código de identificação de carga, ocasionando a divergência de correspondência no sistema quando do recebimento do resultado. Já a exclusão da pendência é o ato de apagar o resultado da seção no sistema, que também deve ser justificado pela autoridade eleitoral. O resultado da seção nesse caso, continuará pendente de recebimento, aguardando uma transmissão com o resultado correto.

As situações possíveis para o *status* de uma carga de urna na tabela de correspondência são:

- Atual: É a correspondência que está valendo para fins de recebimento no sistema de totalização.
- Sobreposta: É uma correspondência de uma carga de urna que não existe mais, pois ela foi sobreposta por uma carga de urna mais recente. O *status* sobreposta está associado a uma nova carga na mesma urna. A carga de urna não existe mais porque a urna foi formatada para a nova carga, que pode ou não ser para a mesma seção. O objetivo aqui é manter um histórico que permita fazer um rastreamento de todas as cargas que foram realizadas na urna eletrônica e registrar na tabela de correspondências cargas de urna que não são mais válidas para fins de recebimento no sistema.
- Anterior: É uma carga de urna que deixou de ser válida pois foi realizada uma nova carga para a seção em outra urna eletrônica. Esse procedimento pode ocorrer sempre que uma urna eletrônica apresenta pane após a carga, não sendo possível recuperá-la. A solução nesse caso, é dar uma nova carga para essa seção em uma urna eletrônica plenamente funcional.

Cabe destacar que cada Flash de Carga possui a sua tabela de correspondências, e essa tabela deve ser obrigatoriamente recebida no sistema GEDAI-UE e transmitida aos Tribunais Regionais Eleitorais, caso contrário, o resultado da seção não entrará no sistema de totalização. Assim, toda tentativa de clonagem de uma urna eletrônica será detectada por meio da tabela de correspondência, que deverá garantir que o resultado de seção que está entrando

no sistema de totalização veio de uma carga oficial de urna, que estava sujeita a auditoria pelos partido políticos e cuja correspondência foi transmitida para o TRE e publicada na internet para fins de conferência e auditoria. Os códigos de identificação de carga no boletim de urna para cada seção deverão ser os mesmos relacionados na tabela de correspondências esperadas, que está disponível no site da internet do Tribunal Superior Eleitoral. Trataremos com mais detalhes do Boletim de Urna nas próximas seções.

5.9 Votação

5.9.1 Zerésima

A partir das 07 horas da manhã do dia da votação, a tela da urna passa a exibir mensagem para confirmação de emissão da zerésima, que é um comprovante que indica que não há registros de votos na urna eletrônica. Esse documento é obrigatório para a ata da seção. Em seu cabeçalho existem informações sobre a seção, data e hora de carga, horário de emissão, além do código de identificação de carga. Também existe a relação de todos os candidatos aptos com o quantitativo de votos zerado. Caso necessário, é possível reemitir a zerésima desligando e religando a urna eletrônica, desde que nenhum eleitor tenha votado.

5.9.2 Habilitação do Eleitor

Quando o relógio da urna atingir a marca de 8 horas da manhã, o terminal do mesário e o terminal de eleitor entram em modo de espera de habilitação de título para início da votação. O eleitor apresenta um documento com foto ao mesário, que irá procurar pelo nome na folha de votação. Encontrando o eleitor e constatando que ele está apto a votar, pronunciará em voz alta o nº do título ao presidente de mesa, que o digitará no terminal do mesário. A urna verifica se o título digitado existe no arquivo de eleitores, e exibe, no terminal do mesário, uma mensagem de confirmação com o nome do eleitor. Nesse momento do processo de habilitação do eleitor, cabe uma observação relevante em relação à votação sem biometria e com biometria:

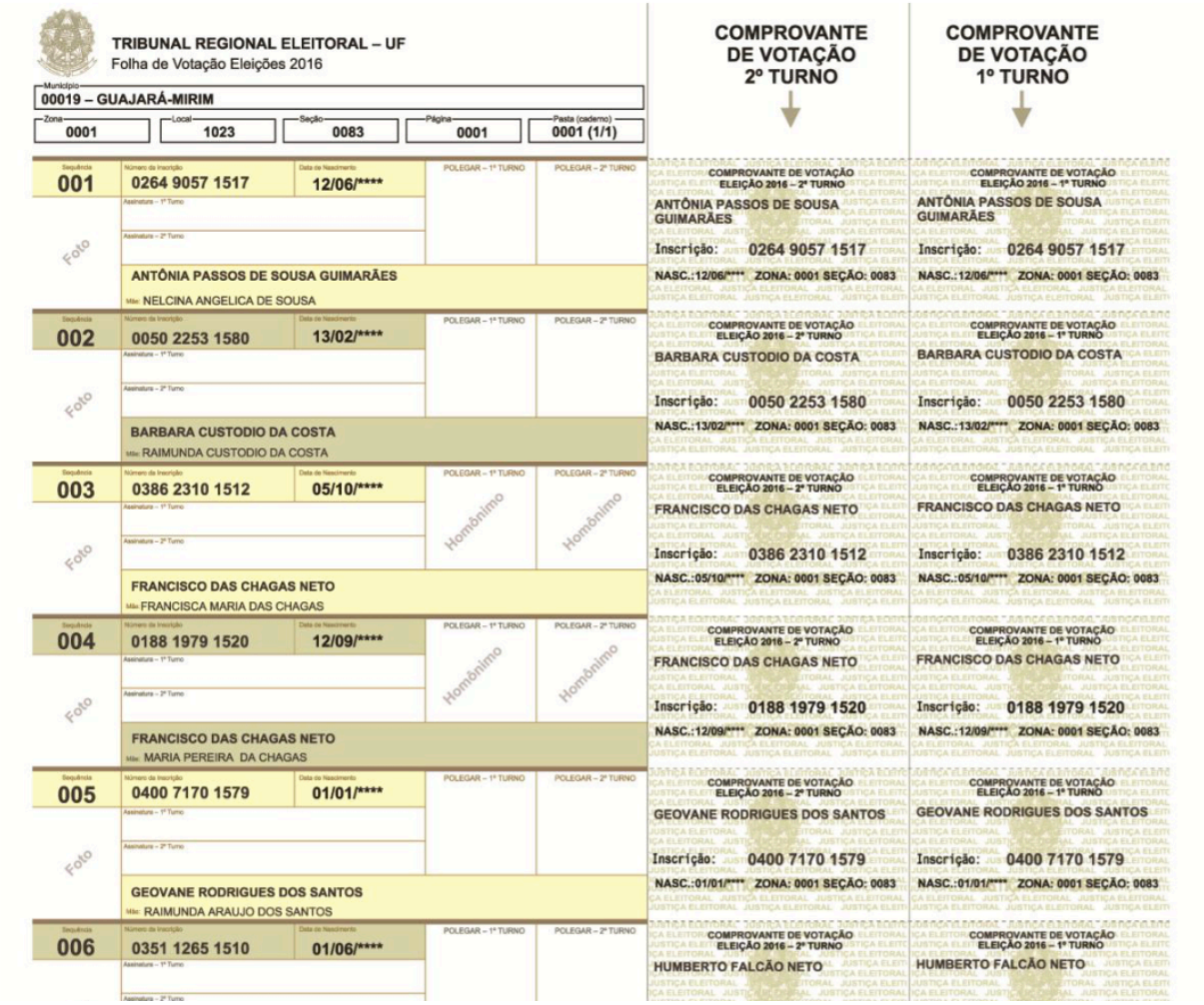
a) Na votação sem biometria, o mesário confirma o nome do eleitor exibido no *display*, e o eleitor se dirige à cabina de votação, para votar no terminal do eleitor. Repare que o controle de quem se apresenta e quem está se dirigindo à cabina de

votação é feito exclusivamente pelos componentes da mesa (presidente de mesa e mesários). Isso dá margem a alguns problemas que ocorrem eventualmente, como por exemplo, o de eleitores que votam indevidamente no lugar de outro, fruto de desatenção do mesário. Explico: a lista de eleitores no caderno de votação é ordenada alfabeticamente e pode acontecer de ter nomes muito semelhantes em posições contíguas – veja posições 3 e 4 na figura 5.2 a seguir, que tem uma imagem parcial de um caderno de votação, para referência. Se o mesário não estiver atento ele pode habilitar para votação o número de título errado, que está na posição imediatamente acima ou abaixo na folha do caderno de votação.

b) Na votação com biometria, após exibir o nome do eleitor para confirmação, a urna solicita que o eleitor posicione um dedo para identificação biométrica – pode ser o polegar ou o indicador de qualquer uma das mãos. Caso falhe o processo de comparação entre a digital armazenada na urna e a digital posicionada no sensor, a urna solicitará que o eleitor posicione novamente o dedo. Se em quatro tentativas não houver correspondências, o que é possível, já que nem todos os eleitores possuem em sua digital a quantidade de minúcias necessária para a identificação, a urna solicita um código para habilitação (de conhecimento do presidente de mesa) e também que seja digitado o ano de nascimento do eleitor. Como essa informação do ano de nascimento não existe no caderno de votação, reduzimos significativamente o risco de o mesário habilitar para votação um eleitor que não seja aquele que está presente na seção. Além disso, antes de liberar o eleitor para votação, a urna solicita a digital do mesário que está habilitando esse eleitor, cuja digital não foi reconhecida, para votar.

Atualmente, como o cadastro biométrico do eleitorado ainda está sendo implantado, alguns municípios tem votação totalmente biométrica, aplicando-se exclusivamente o procedimento descrito no item “b”, votação sem biometria, com o procedimento descrito no item “a”, e votação híbrida (ou mista), aplicando-se ambos os procedimentos, dependendo da existência do arquivo de biometria do eleitor na urna. De qualquer forma, o registro de habilitação de eleitor, no log da urna, informa como foi feita a habilitação, se houve erro no reconhecimento ou se o mesário digitou código de liberação. Essas informações de reconhecimento das digitais, além do log das urnas, são transmitidas ao TSE, junto com arquivos de resultado, para que posteriormente sejam analisadas por ferramentas de *Business Inteligence*.

Figura 5.2 – Imagem parcial de folha de um caderno de votação com a relação de eleitores



Fonte: TSE – Resolução 23.456/15, anexo pág. 83.

5.9.3 Ordem dos cargos para votação

O software de votação exibe na tela da urna (terminal do eleitor) o cargo para o qual deve ser registrado o voto, com um campo indicando a quantidade de dígitos que devem ser digitados. Ao registrar o voto na urna, o eleitor deve observar a ordem dos cargos para votação:

- Voto para vereador e depois voto para prefeito, nas eleições municipais;
- Voto para deputado estadual, depois deputado federal, senador(es), governador e, por fim, presidente, nas eleições gerais.

Nos cargos proporcionais (vereador, deputado estadual e deputado federal) ao digitar os primeiros dois números, a urna exibe uma mensagem de voto na legenda do partido (caso o

número corresponda ao de um partido em situação regular). Se, ao completar o número, o software não encontrar um candidato apto para aquele cargo e o eleitor confirmar o voto, o sistema registrará o voto para a legenda. Encontrando um candidato apto com o número correspondente, o sistema exibe em tela a foto e os dados desse candidato para conferência do eleitor. Nesse momento o eleitor poderá confirmar o voto. A qualquer momento antes da confirmação do voto para um determinado cargo, o eleitor, constatando erro de digitação, poderá apertar a tecla Corrige e reiniciar a votação para o cargo em tela. Uma vez confirmado o voto, não é possível retornar àquele cargo para corrigi-lo. Também é possível votar nulo, desde que os dois primeiros dígitos não correspondam ao de um partido em situação regular. Para o voto em branco basta pressionar a tecla Branco na urna eletrônica. Enquanto houver cargos para a votação o processo se repete.

Se o eleitor não respeitar a ordem de votação, e, por exemplo, votar primeiro para prefeito na tela de voto para o cargo de vereador, o voto será registrado para a legenda do partido do vereador. Na sequência, ele não encontrará candidato correspondente ao cargo de vereador, pois o cargo em tela na urna será o de prefeito. Erros de procedimento do eleitor são relativamente comuns, já que muitos eleitores são instruídos, equivocadamente, a "digitar o número do candidato e confirmar". Repare que, se o eleitor proceder dessa forma, o voto estará registrado na memória da urna, sem chance de confirmação visual. De fato, em todas as eleições os cartórios recebem reclamações de eleitores que não visualizaram a foto do seu candidato, o que frequentemente dá origem a suspeitas sobre a correção do software. Uma das soluções aqui seria a inclusão de uma segunda confirmação, para cada cargo, o que carece de estudos de usabilidade. O mais fácil seria intensificar o treinamento do eleitor para que ele adote o procedimento correto: Observar o cargo em tela, digitar o número completo, verificar se o candidato ou mensagem em tela estão corretos, e, só então, pressionar a tecla Confirma – ou Corrige, caso seja constatado erro de digitação.

Durante a sequência de votação, os votos confirmados para os cargos são armazenados em memória volátil. O voto só é registrado em ambos no cartões de memória após a confirmação de votos de todos os cargos em disputa, momento em que aparece na tela da uma barra de progresso, seguida de sinal sonoro característico e mensagem "FIM". Isso significa que, se ocorrer uma pane na urna eletrônica antes de concluir a votação em todos os cargos, o eleitor deve permanecer na seção até resolverem o problema, para que ele possa reiniciar a votação para todos os cargos.

Caso um eleitor desista de votar ou tenha dificuldades, a votação pode ser suspensa, desde que ele não tenha confirmado o voto para nenhum dos cargos – o mesário dispõe de

código específico para esse procedimento. Nesse caso, o eleitor pode retornar em outro momento para votar. Se o eleitor já registrou o voto para pelo menos um cargo e desistir de votar, o mesário deve orientá-lo a retornar à cabine de votação para concluir o voto, ou alertá-lo de que os votos para os cargos restantes serão anulados pelo sistema. Nesse caso, o eleitor não poderá retornar para concluir a votação. O terminal do mesário apresenta mensagens específicas para os procedimentos em cada caso.

5.9.4 Justificativa Eleitoral

O eleitor que, no dia da votação, não se encontrar no seu domicílio eleitoral – o município em que ele vota – poderá comparecer em qualquer seção eleitoral para justificar o seu voto. O eleitor deve apresentar ao mesário o seu documento de identidade e título eleitoral, informando que quer justificar a ausência. O presidente de mesa digitará o número do título no terminal do mesário e o software da urna fará a validação do título. Em seguida, o software procura no arquivo de eleitores da urna pelo título correspondente. Como esse título não deve existir naquela seção, será exibida mensagem no terminal do mesário informando o registro de uma justificativa de ausência às urnas, com opção para confirmar ou cancelar o procedimento. Se o presidente de mesa confirmar, o software registra a justificativa na urna e exibe um código de autenticação, que deverá ser anotado em um formulário de justificativa como comprovante do registro da operação para o eleitor.

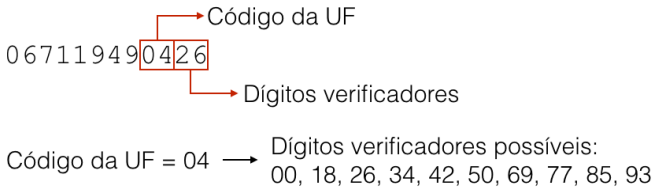
Teoricamente, um eleitor que justificou ausência às urnas em um município não poderia estar votando em outro município. A partir dessa premissa, em 2014 foi feito um cruzamento entre os registros de justificativas e o de eleitores que efetivamente compareceram às urnas para votação em seu domicílio eleitoral, e foram encontrados mais de 40 mil casos no 1º turno e outros 37 mil no segundo turno que recaíram nessa situação[25]. Em uma análise superficial parece tratar-se de fraude eleitoral. Na prática, pode acontecer de um eleitor, em viagem, justificar sua ausência em um município, mas chegar a tempo de votar em sua cidade. Imagine um eleitor que resolve passar o final de semana no litoral, decidido a não votar nas eleições. Esse eleitor, no dia da eleição, se dirige na primeira hora da manhã a uma seção eleitoral para justificar o voto. Após o almoço, começa a chover e o eleitor resolve

[25] Disponível em: http://g1.globo.com/politica/noticia/2016/06/tse-manda-apurar-40-mil-casos-de-voto-de-eleitor-que-justificou-ausencia.html

antecipar a volta para casa, chegando a tempo de votar. Podem não ser muitos casos, mas é perfeitamente possível que essa situação ocorra.

Outra situação possível, que deve corresponder à grande maioria dos casos identificados nesse cruzamento, diz respeito às regras de formação do número do título do eleitor e do código verificador. Observe a figura 5.3 abaixo:

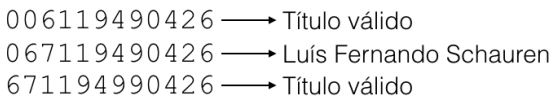
Figura 5.3 – Exemplo do formação do dígito verificador no título de eleitor



Fonte: Autor.

Um número de título possui 12 dígitos, dentre os quais, os dois últimos são para validação. O cálculo desses dois dígitos é feito de forma que, para um determinado código de unidade da federação, só existam 10 possibilidades, em vez de 99. Isso implica no fato de que, quando um número de título é digitado erroneamente (suprimindo ou duplicando um dígito, por exemplo) existe uma boa probabilidade de que um deles corresponda a um título válido. Assim, é possível que um presidente de mesa, ao digitar um título errado, possa acidentalmente incluir uma justificativa para um eleitor que votou em outro local no país. Observe o exemplo da figura 5.4 abaixo:

Figura 5.4 – Exemplo de números de título de eleitor válidos



Fonte: Autor.

Claro que uma parte dos casos em que houve essa coincidência pode realmente corresponder à fraude dos mesários. Nesse caso, deve-se verificar, para cada seção eleitoral, quantos casos desses ocorreram. Havendo mais de um ou dois casos em uma mesma seção, há motivos para suspeita. É importante ressaltar que esses problemas originam-se por uma falha de procedimento. Assim, é plausível que, dentre as 8.231.993[26] justificativas no 1º turno de 2014, tenha 40 mil justificativas (0,48%) por erro de digitação do mesário.

[26] TSE. Estatísticas de Justificativa Eleitoral – Origem e Destino. Disponível em: http://www.tse.jus.br/eleitor/estatisticas-de-eleitorado/origem-e-destino

5.9.5 Encerramento da Votação

A partir das 17h o software da urna permite o encerramento da votação, mediante a digitação de um código específico no terminal do mesário. Após o presidente de mesa digitar o código de encerramento, o sistema automaticamente imprime a 1ª via do Boletim de Urna (BU). Esse documento contém a lista, separada por cargo e partido, com o quantitativo de votos de todos os candidatos e legendas que receberam pelos menos um voto na urna eletrônica, além da relação de votos nulos e brancos. Estando esse documento legível e confirmada a qualidade da impressão, o sistema gravará a Mídia de Resultado – com todos os arquivos necessários à apuração, registro digital do voto, logs, faltosos, dentre outros – e imprimirá mais cópias do BU – obrigatoriamente mais 4 vias e até 15 adicionais.

Todas as vias dos BUs deverão ser assinadas pelo presidente de mesa, 1º secretário e fiscais presentes. Duas vias devem ser remetidas ao cartório eleitoral ou à junta apuradora; uma cópia deve ficar em poder do presidente de mesa, para posterior conferência com o resultado por seção divulgado na internet; uma cópia deve ser afixada em local visível da seção; as demais cópias serão distribuídas aos fiscais presentes. A partir desse momento, o resultado da seção é público e poderá ser conferido com o resultado por seção divulgado no site de internet do Tribunal Superior Eleitoral, após a totalização dos resultados.

A mídia de resultado deverá ser encaminhada à junta eleitoral, existindo ainda a possibilidade de transmiti-la previamente a partir de um ponto de transmissão remoto, conforme verificaremos na seção 5.14 quando trataremos da transmissão dos dados.

5.10 Auditoria de Funcionamento das Urnas Eletrônicas por meio de Votação Paralela

A auditoria de funcionamento das urnas por meio de votação paralela, que, por conveniência denominaremos apenas de votação paralela, é um procedimento de auditoria por amostragem, cujo objetivo é comprovar o correto funcionamento das urnas testando a segurança na captação dos votos e na contabilização dos resultados. Esse mecanismo de auditoria foi implantado em 2002 e ocorre em todos os turnos das eleições, em todos os estados.

Com a informatização das eleições e a introdução do voto eletrônico, surgiu o desafio de encontrar uma maneira simples que pudesse demonstrar à sociedade que a urna eletrônica

efetivamente soma corretamente os votos. Inicialmente, a impressão do voto seria uma opção de auditoria independente, na qual o resultado proveniente do escrutínio manual das cédulas impressas poderia ser confrontado com o resultado eletrônico contabilizado pela urna. No entanto, esse procedimento trouxe uma série de problemas que serão abordados na seção 5.20, ao analisarmos a impressão do voto. Uma solução mais simples, de menor custo, e que não traz nenhum impacto em segurança, confiabilidade, usabilidade e eficiência no processo normal de votação eletrônica é a votação paralela. Assim, qualquer pessoa pode aferir o correto funcionamento da urna, com o procedimento simples de anotar em uma planilha os votos que estão sendo digitados na urna eletrônica que está sendo auditada. Ao final da votação é possível comparar esse resultado com o resultado emitido pela urna eletrônica. Claro que o ônus dessa conferência não pode ser repassado ao eleitor presente na cerimônia. Esse processo de auditoria, que é regulamentado pela Resolução TSE 23.458/2015 e auditado por empresa independente, na realidade, é bem mais complexo e explicaremos todas as particularidades em maior profundidade.

5.10.1 Sorteio da Votação Paralela

Na véspera e antevéspera da eleição todas as urnas eletrônicas carregadas são enviadas para os respectivos locais de votação, de forma que, por volta das 9h da véspera, praticamente todas as urnas já estão instaladas e testadas em suas seções eleitorais. A partir das 9h do sábado de véspera da eleição, nas sedes dos Tribunais Regionais Eleitorais, ocorre uma cerimônia pública para o sorteio da votação paralela.

De acordo com o número de seções eleitorais em cada estado são sorteadas de 3 a 5 seções, sendo uma obrigatoriamente da capital do estado. Esse sorteio ocorre de forma manual, visando reduzir suspeitas sobre o método do sorteio. Ele é realizado com base na tabela de correspondências que foram transmitidas, de forma que todas as seções tenham a mesma probabilidade de serem sorteadas. Existe ainda o Sistema de Apoio à votação paralela (SAVP) cujo objetivo, nessa fase, é agilizar o processo de identificação da seção sorteada, além de eliminar possibilidades de sorteio que não levem a uma seção existente, já que o número é sorteado a partir da unidade, depois a dezena e, por fim, a centena. Assim, o SAVP vai indicando as possibilidades de formação válidas para zona e seção, permitindo que sejam retirados do sorteio números desnecessários.

Assim que uma seção é sorteada no estado, o cartório eleitoral é informado para que inicie os procedimentos para recolher a urna do local de votação e preparação de uma nova

urna para substituí-la. O Tribunal Regional Eleitoral designa uma equipe para trazer essa urna para a capital. A urna recolhida do local de votação será armazenada em ambiente controlado e fiscalizado, até que seja enviada ao local onde ocorrerá a cerimônia da votação paralela, no dia da eleição.

Sabendo-se de qual município foi sorteada a seção, é possível obter a lista de candidatos que concorrem à eleição. Com base nessa lista, fiscais de entidades representativas da sociedade e partidos políticos estão aptos a preencher, aleatoriamente, cédulas de papel com números dos candidatos, além de votos brancos e nulos. Ao final do preenchimento dessas cédulas elas são lacradas em uma urna de lona que também será armazenada em local seguro, controlado e sob fiscalização.

5.10.2 A Votação Paralela

No dia da eleição, a partir das 7 horas da manhã, as urnas das seções sorteadas podem ser ligadas dando início aos procedimentos para votação, que iniciará às 8 horas, podendo-se emitir, a qualquer momento, a zerésima da seção, além de abrir os lacres das urnas de lona que contém as cédulas preenchidas aleatoriamente no dia anterior. A partir da zerésima pode-se conferir a seção, a data e hora de carga e o código de identificação de carga, que devem corresponder àqueles que haviam sido transmitidos anteriormente e constavam inicialmente na tabela de correspondências – isso garantirá que não foi preparada uma urna especial para enviar à auditoria. A partir das 8h, os títulos dos eleitores aptos a votar começam a ser habilitados, de forma aleatória, e as cédulas de papel começam a ser sorteadas nas respectivas urnas de lona.

Cada cédula sorteada é numerada sequencialmente, seu conteúdo é lido em voz alta e apresentado aos fiscais presentes e auditores, que anotarão o voto em uma planilha, além de ser apresentado na filmagem. Esse voto então será digitado na tela da urna, que é constantemente filmada, e também será registrado com o número de sequência e horário no SAVP, que está rodando em um computador isolado. Isso permitirá que, em caso de divergências no resultado ao final da votação, seja possível identificar qual voto originou a divergência e retornar a gravação da filmagem para identificar possível erro de digitação na urna eletrônica. Esse processo ocorre ao longo do dia com equipes que se revezam nos procedimentos em cada urna. Também existe a possibilidade de inserir justificativas eleitorais e o art. 56 inciso II da Resolução 23.458/15 estabelece que o número de votos fique entre

75% e 82% dos eleitores aptos da seção, de forma a representar a realidade de uma seção eleitoral.

5.10.2 Encerramento da Votação Paralela

A partir das 17h é possível encerrar a votação nas urnas sorteadas, sendo facultado a inserção de mais alguns votos antes do encerramento para simular uma situação de fila na seção, caso a Comissão da Votação Paralela entenda pertinente. Após o encerramento da votação, a urna emitirá um Boletim de Urna, cujos resultados deverão ser confrontados com o resultado do relatório Espelho do BU, emitido pelo SAVP e com os resultados das planilhas dos auditores. Esse resultado pode ser conferido manualmente com o resultado do Boletim de Urna emitido pela urna eletrônica ou de forma automatizada através da leitura do *pendrive* com resultados da urna no SAVP.

Até hoje nunca houve um caso sequer no país que tenha apresentado resultados divergentes, mas se ocorresse, é possível emitir, no Sistema de Apoio à Votação Paralela, o Relatório de Resultados Divergentes. Identificada divergência na votação entre candidatos, votos de legenda, nulos ou brancos, é possível emitir o relatório Votos por Candidato do SAVP, que conterá os horários de digitação de cada cédula para o número do candidato em questão. Assim, é possível retornar a gravação da filmagem para o momento exato em que foram digitados os votos na urna em busca de possíveis erros de digitação.

Ao final dos procedimentos, a urna deverá ser auditada por meio da mídia de resultado VPP (Verificação Pré e Pós Eleição) emitindo os relatórios com os resumos digitais dos arquivos de sistema da urna e se necessário o log da urna eletrônica. Concluídos os trabalhos, a Comissão da Votação Paralela deverá terminar de preencher a ata da cerimônia e encaminhá-la à presidência do Tribunal Regional Eleitoral.

5.11 Contingências

Sempre que uma urna eletrônica apresentar algum defeito, uma equipe técnica é acionada para resolver o problema. O suporte pode ser realizado através de contato telefônico, para problemas mais simples, ou então mediante suporte presencial, havendo necessidade de troca ou intervenção na urna eletrônica que enseje a remoção dos lacres.

O primeiro procedimento é sempre desligar e ligar a urna eletrônica. No momento da inicialização, ocorrendo algum erro, a urna deverá exibir mensagem específica informando o problema e indicando qual procedimento deverá ser realizado: troca da urna eletrônica, que vamos tratar por contingência de urna; ou troca do cartão de memória da flash externa, que vamos denominar contingência de flash. Existe ainda a possibilidade do simples desacoplamento do módulo impressor e reinserção desse módulo, em caso de mal contato.

A contingência de urna é realizada sempre que há um defeito físico no hardware da urna eletrônica ou na integridade dos arquivos da flash interna. É importante esclarecer que todos os eventos da urna eletrônica são gravados simultaneamente na flash interna e na flash externa (logs e dados de votação). Assim, num procedimento de contingência de urna, será retirada a flash de votação do drive da flash externa, juntamente com a mídia de resultado, e serão inseridas em uma urna de contingência (urna reserva). A urna de contingência não possui flash de votação na flash interna e nem mídia de resultado no compartimento do *pendrive*, ainda que estes compartimentos estejam lacrados desde a Cerimônia de Carga. Ela possui apenas a flash interna, que contém, nesse momento, apenas o sistema operacional e os aplicativos da urna. Repare que não há dados de candidatos e nem dados de eleitores, tampouco dados de votação. Após a inicialização do sistema, na urna de contingência, com todas as validações do encadeamento de segurança, o software de votação identificará que a flash interna não possui dados de eleitores, candidatos ou votação. Nesse momento ocorre o sincronismo entre as flashes, procedimento que vai copiar todos os dados necessários (logs, dados de eleitores, de candidatos e de votação) da flash de votação – que foi inserida na flash externa – para dentro da flash interna. Ocorrendo o sincronismo com sucesso, a urna entra em modo de votação novamente, devendo ser lacrada com lacres de reposição, que devem ser assinados pelos componentes da mesa e pelos fiscais presentes. A urna original, que apresentou defeito, também deverá ser lacrada com lacres de reposição (assinados da mesma forma) e deve retornar ao local designado pela Justiça Eleitoral.

Existe a possibilidade de que o problema esteja relacionado à leitura ou integridade dos arquivos da flash de votação, que está no drive da flash externa. Nesse caso, o primeiro

procedimento de contingência será desligar a urna, romper os lacres da flash externa, remover a flash de votação, reinserí-la e religar a urna eletrônica. Caso o problema não seja resolvido com esse procedimento, deve-se fazer a contingência de flash, que consiste na troca da flash de votação por uma flash de votação reserva - que ainda não foi utilizada em nenhuma urna, portanto contém somente as fotos dos candidatos, e está lacrada em envelope específico desde a Cerimônia de Geração de Mídias. Assim, após a inicialização do sistema, o software de votação identificará uma flash externa sem dados de eleitores, de candidatos (exceto as fotos) e de votação, e dará início ao sincronismo de flash, só que dessa vez, copiará os dados da flash interna – que contém todos os dados necessários – para a flash de votação que está no drive da flash externa. Assim que a urna entrar em modo de votação novamente, o compartimento da flash externa deverá ser lacrado com lacre de reposição, que será assinado pelos componentes da mesa e pelos fiscais presentes, e a flash de votação com defeito deverá ser lacrada em envelope específico e remetida ao local designado pela Justiça Eleitoral.

Não sendo possível recuperar a urna eletrônica através dos procedimentos de contingência de flash ou contingência de urna, a votação na seção será feita em cédulas de papel que serão depositadas em urna de lona previamente lacrada pela junta eleitoral.

Todos os procedimentos de contingência deverão constar na ata da seção e também registrados em sistema eletrônico de ocorrências específico da Justiça Eleitoral, para fins de controle dos Tribunais Regionais Eleitorais.

5.12 Boletim de Urna

Ao longo de 20 anos da Urna Eletrônica a Justiça Eleitoral sempre se preocupou em desenvolver novos mecanismos e aprimorar os processos visando aumentar a transparência, facilitando a fiscalização e garantindo a segurança do processo eleitoral. Uma das formas mais simples de fiscalização, e que está acessível a todos os cidadãos, é o Boletim de Urna.

Ao final da votação a urna apura os votos e imprime um relatório com o resultado oficial da votação daquela seção. Esse documento é público e deve ser afixado em local visível, além de ter cópias distribuídas aos fiscais interessados. Dessa forma, qualquer cidadão pode fazer a sua própria conferência com o resultado de seção divulgado na internet no site do TSE. De fato, em municípios menores, em eleições municipais, muitos partidos e coligações já fazem a sua própria totalização e já tem o resultado antes mesmo que o TRE divulgue de forma oficial o resultado final da totalização.

O artigo 110 da Resolução 23.456/15, que dispõe sobre os atos preparatórios para as eleições 2016, estabelece que:

> Art. 110. O boletim de urna fará prova do resultado apurado, podendo ser apresentado recurso à própria Junta Eleitoral, caso o número de votos constantes do resultado da apuração não coincida com os nele consignados.
>
> § 1º Ao final da apuração dos votos pela urna eletrônica e a respectiva emissão do boletim de urna, poderá ser atestada, por qualquer eleitor, a coincidência entre o número de votos do boletim de urna e o número de votos consignado no resultado da apuração disponível na Internet, nos termos do art. 154, por meio da leitura do código de barras bidimensional (Código QR) constante do boletim de urna.
>
> § 2º O Tribunal Superior Eleitoral disponibilizará aplicativo para a leitura do código de barras bidimensional (Código QR) sem prejuízo da utilização de outros aplicativos desenvolvidos para esse fim. [27]

Com o crescente interesse da população surgiu a necessidade de facilitar a conferência e fiscalização desses resultados – entre o BU impresso e aquele divulgado após a totalização dos resultados. Assim, o TSE implementou um código de barras bidimensional do tipo *Quick Response Code* (QR Code) no final de cada BU e disponibilizou gratuitamente um aplicativo para dispositivos móveis chamado "Boletim Na Mão". De posse desse aplicativo é possível capturar/digitalizar os QR Codes de quantos Boletins de Urna desejar. O aplicativo se encarrega de tornar a informação do QR Code legível montando os dados na tela do dispositivo no mesmo formato exibido no boletim de urna impresso.

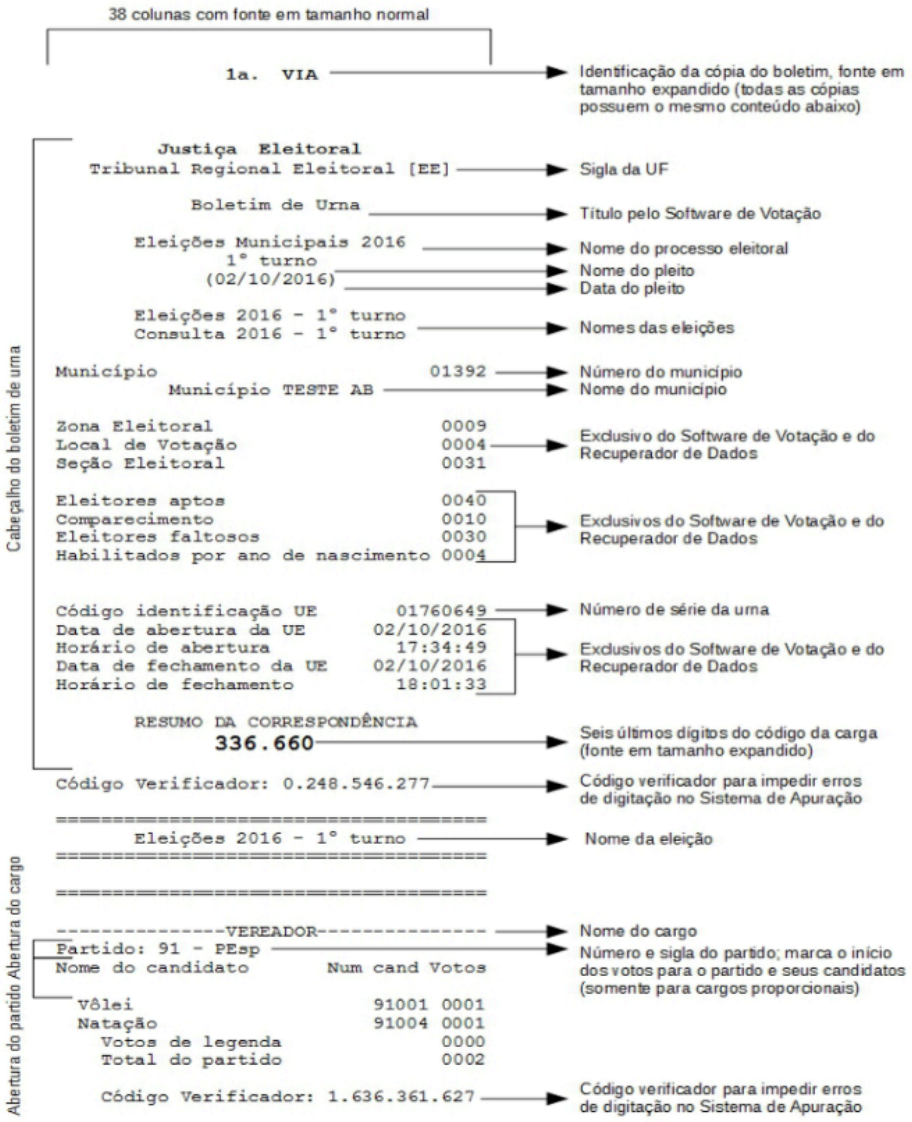
A Justiça Eleitoral também fornece um manual com informações para que terceiros possam criar o seu próprio aplicativo para leitura dos QR Codes dos Bus. O conteúdo do boletim de urna codificado por esse QR Code é assinado digitalmente por um algoritmo de chave pública Ed25519 com configuração EdDSA. Segundo informações do manual do TSE é um algoritmo de curvas elípticas, moderno, de alto desempenho, elevado nível de segurança e que possui implementações resistentes a ataques do tipo *side-channel*. O algoritmo é de domínio público e possui várias implementações de código aberto para diferentes linguagens de programação, o que facilita a implementação, sendo um dos motivos pelos quais foi escolhido. *O software da urna utiliza a biblioteca libsodium[28] para a geração de assinatura e de pares de chaves. Devido às limitações de espaço do QR Code e à sua aplicação em dispositivos móveis, um benefício importante do Ed25519 é o tamanho de chave (256 bits) e*

[27] Resolução TSE 23.456/15. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-456-instrucao-53-680>

[28] Disponível em <https://github.com/jedisct1/libsodium>.

de assinatura reduzidos (512 bits). As chaves públicas para validação da assinatura do conteúdo do QR Code estão disponíveis no site de internet do TSE[29].

Figura 5.5 – Cabeçalho de um boletim de urna com identificação dos elementos



Fonte: TSE. QR Code no Boletim de Urna

É importante ressaltar que, embora, o conteúdo do boletim de urna codificado no QR Code utilize um algoritmo de código aberto de domínio público, a assinatura digital empregada no arquivo de resultado que será verificada no sistema de totalização, para fins de

[29] Disponível em: <http://qrcodenobu.tse.jus.br/qrcode-bu/chavesqrcodeoficial.zip>

validação do arquivo recebido, utiliza algoritmo de Estado conforme estabelecido em norma específica[30].

Figura 5.6 – Parte final de um boletim de urna com identificação dos elementos

Fonte: TSE. QR Code no Boletim de Urna

A partir da compreensão da importância do boletim de urna, percebe-se que o argumento de que os resultados da eleição são alterados durante a transmissão ou totalização dos resultados é o mais fácil de ser contestado, pois sua verificação é elementar, bastando apresentar um único boletim de urna que seja divergente daquilo que é divulgado.

[30] Disponível em: <http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf>

Por fim, cabe destacar que os BUs possuem alguns elementos de controle muito importantes, como o código de identificação da carga, que permitirá rastreá-lo e até mesmo verificar se não foi forjado, além dos códigos verificadores da votação, que são utilizados no sistema de apuração para identificar erros de digitação. As figuras 5.5 e 5.6 podem ser utilizadas como referência para identificar esses elementos.

5.13 Registro Digital do Voto

A Lei 10.740 de 1º de outubro de 2003 alterou o artigo 59 da Lei 9504/97 (Lei das Eleições) instituindo o Registro Digital do Voto - em substituição à obrigatoriedade do voto impresso. Os parágrafos 4º a 6º do art. 59 passaram a vigorar com a seguinte redação:

> § 4º A urna eletrônica disporá de recursos que, mediante assinatura digital, permitam o registro digital de cada voto e a identificação da urna em que foi registrado, resguardado o anonimato do eleitor.
>
> § 5º Caberá à Justiça Eleitoral definir a chave de segurança e a identificação da urna eletrônica de que trata o § 4º.
>
> § 6º Ao final da eleição, a urna eletrônica procederá à assinatura digital do arquivo de votos, com aplicação do registro de horário e do arquivo do boletim de urna, de maneira a impedir a substituição de votos e a alteração dos registros dos termos de início e término da votação.[31]

Para cada voto inserido na urna eletrônica é feito um registro digital correspondente em uma posição aleatória de uma tabela, o Registro Digital do Voto (RDV). Não há qualquer vinculação desse registro com o eleitor depositário do voto, de forma a preservar o sigilo da escolha do eleitor. Essa tabela do RDV possui tamanho igual à quantidade de eleitores da seção e é reassinada digitalmente, mediante a aplicação de sistema de criptografia com chaves assimétricas, após a inserção de cada voto, para preservar a sua integridade e impedir que um voto seja substituído ou removido do RDV. [32]

Ao final da votação, a contabilização dos votos para a geração e impressão do boletim de urna é feita a partir das informações da tabela com o registro digital dos votos.

---

[31] Lei 10.740/2003 Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.740.htm#art2>

[32] TSE: Registro Digital do Voto. Disponível em: <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/registro-digital-do-voto>

Em relação ao sigilo do voto, cabe destacar que a informação de quais eleitores votaram na urna eletrônica é registrada em uma tabela distinta do RDV. Também não há registro do horário em que cada eleitor votou. Quando o mesário habilita um eleitor no terminal do mesário, é adicionado um registro no log da urna indicando o horário do evento e a informação de que houve habilitação de eleitor, em seguida novo registro de evento com horário e a informação de que um eleitor está votando, mas não há qualquer registro de que eleitor é esse.

A figura 5.7 abaixo demonstra um exemplo de como ocorre esse registro. Após concluída a votação o sistema faz um registro indicando que o eleitor que estava habilitado concluiu a votação. Em outra tabela separada ocorre o que chamamos de embaralhamento dos votos, ou seja, são sorteadas posições aleatórias para cada cargo nas quais são inseridos os registros de cada voto.

Figura 5.7 – Tabela de eleitores que votaram x Tabela do RDV

Eleitor	Votou?
Eleitor 1	✓
Eleitor 2	
Eleitor 3	
Eleitor 4	✓
Eleitor 5	✓

Vereador	Tipo	Prefeito	Tipo
<Branco>	Branco	92	Nominal
90123	Nominal	91	Nominal
92	Legenda		
		99	Nulo

Fonte: TSE – Testes Públicos de Segurança (2012).

Nos Testes Públicos de Segurança de 2012, uma equipe de investigadores coordenada pelo professor Dr. Diego Aranha, especialista na área de Criptografia em Segurança Computacional, identificou uma vulnerabilidade relacionada ao RDV que colocava em risco o sigilo do voto do eleitor [33]. Basicamente o algoritmo de embaralhamento utilizado até então para escolher uma posição na tabela não possuía qualidade criptográfica e não atingia o nível de aleatoriedade necessário para garantir a segurança e o sigilo dos votos registrados por dois motivos: a escolha inadequada de um gerador, pois a implementação utilizava um gerador de números pseudo aleatórios; e a escolha inadequada da semente, que deveria ser escolhida de forma verdadeiramente imprevisível, mas consistia de uma simples tomada de tempo com

[33] ARANHA, D. F. et al. **(In)segurança do voto eletrônico no Brasil**. Fundação Konrad Adenauer, p. 117–133, 2014. Disponível em: <http://www.kas.de/wf/doc/13775-1442-5-30.pdf>.

precisão de segundos, a partir do horário de emissão da zerésima. Assim, após exame do código-fonte e de posse do horário de emissão da zerésima foi possível reproduzir, com a reversão do algoritmo de embaralhamento, *a ordem de armazenamento de até 950 votos com exatidão e eficiência, sem probabilidades de erro ou alto custo computacional*.

O TSE se baseava na premissa de que, mesmo reconstruindo a ordem de registro dos votos, não seria possível conhecer a ordem em que os eleitores votaram, pois não existe registro dessa informação no sistema. Assim, supostamente, não haveria como fazer essa associação a fim de quebrar o sigilo do voto. O argumento utilizado pelos investigadores foi o de que se houvesse um controle (externo ao software) sobre a ordem da fila de eleitores – coagindo o mesário a fornecer esses dados, por exemplo – poderia ser feita facilmente essa associação, já que a fonte de entropia (coleta de informação imprevisível) para geração de aleatórios utilizava uma medida de tempo em resolução de segundos, e todos os dados necessários estavam disponíveis no log da urna, que é um documento público que pode ser solicitado por qualquer partido político.

O TSE reconheceu a necessidade de melhorias e implementou a geração de aleatórios para semente do RDV a partir do /dev/urandom, ainda para aquela eleição. A sugestão proposta por Aranha para esse caso foi: "*Para satisfazer o critério de aleatoriedade verdadeira, recomenda-se utilizar um gerador em hardware baseado em efeito físico bem estudado. Segundo especificação da urna eletrônica modelo 2009, dois geradores com estas características já estão disponíveis no equipamento*". De fato, o hardware da urna possui um relógio de tempo real e um gerador de números realmente aleatórios.

É importante ressaltar nesse caso, que não foi possível adicionar, subtrair ou trocar qualquer voto registrado no teste. O problema estava relacionado exclusivamente ao sigilo do voto, pois, não só foi possível recontar todos os votos a partir do RDV, como foi possível reconstruir a ordem exata em que foram inseridos no sistema. Embora resolvida a questão de segurança relacionada ao sigilo do voto, as entidades interessadas na inspeção do código devem prestar especial à implementação do RDV, pois é um importante elemento para auditoria dos resultados.

5.14 Transmissão dos Dados

Todos os cartórios eleitorais possuem conexão de dados privada com os Tribunais Regionais Eleitorais, utilizando principalmente MPLS (*Multi-Protocol Label Switching*) sobre

circuitos *frame relay* ou VPN (*Virtual Private Network*) sobre conexões ADSL (*Assymetrical Digital Subscriber Line*), ou ainda alguma tecnologia semelhante, conforme disponibilidade das operadoras locais.

Todos os dados de resultados produzidos pela urna eletrônica são transmitidos exclusivamente a partir do sistema Transportador, que é uma aplicação desktop que só pode ser instalada em computadores da Justiça Eleitoral, pois necessita da versão oficial do SIS – Subsistema de Instalação e Segurança, que contém os certificados digitais necessários para sua instalação. Além disso, existe uma versão especial do Transportador para o kit *JE Connect* como veremos mais adiante.

O sistema transportador é oficializado automaticamente no primeiro acesso, após as 12h, dia da eleição. Ao iniciar a execução em um computador da Justiça Eleitoral, o sistema Transportador verifica as assinaturas dos arquivos. Verificadas as assinaturas é estabelecida uma conexão *https* com o servidor responsável pela recepção dos arquivos, que está localizado no *datacenter* do Tribunal Regional Eleitoral. Estabelecida a conexão, antes de proceder com a leitura de qualquer arquivo de resultado, o operador do sistema deve emitir o relatório "Espelho dos Diretórios" que deverá indicar a inexistências de arquivos de resultados nos diretórios da aplicação. Esse relatório é emitido em todos os micros que possuem uma cópia do Transportador e faz parte da ata da Eleição. Após a emissão do relatório pode-se proceder com a leitura das Mídias de Resultado provenientes das urnas eletrônicas, que são entregues em mãos, nas juntas de apuração, pelo presidente de mesa da seção. Durante a leitura das MRs o sistema transportador verifica as assinaturas digitais dos arquivos. Após a leitura das MRs é possível transmitir os arquivos lidos para o TRE.

O sistema Transportador também recupera relatórios com o resultado das transmissões. Caso um arquivo não tenha sido transmitido, o sistema tenta enviar novamente na próxima transmissão. Também é possível forçar a retransmissão de arquivos, desde que seja selecionada opção para isso.

5.14.1 JE Connect

Uma das maiores questões relacionadas ao tempo de apuração e totalização das eleições é a distância entre os locais de votação e os cartórios eleitorais, já que a mídia de resultado que é gravada pela urna é levada em mãos pelo presidente de mesa da seção até uma junta apuradora. Em um país de dimensões continentais é bastante comum que existam locais de votação que estão a 4 horas ou mais de distância do cartório eleitoral. Há muitos anos os

Tribunais Regionais Eleitorais vem pensando em alternativas para reduzir esse tempo. Em 2012 um grupo de trabalho formado por servidores da área de TI de vários Tribunais Regionais Eleitorais criou uma solução para transmissão remota dos arquivos de resultado das urnas eletrônicas: o JE Connect. A ideia original era iniciar uma máquina virtual padrão da justiça eleitoral, com o transportador instalado, a partir de um *pendrive* inicializável com o sistema Linux. Essa solução usaria apenas o hardware de uma máquina e uma conexão VPN utilizando o acesso à internet do local de transmissão remota.

A solução, que foi aperfeiçoada nas últimas eleições, consiste atualmente de um par de *pendrives* que denominamos kit JE Connect. O sistema operacional Linux roda a partir de um *pendrive* denominado Mídia de Sistema Embarcado (MSE) que pode ser plugado em qualquer microcomputador ou notebook, para usar apenas o hardware da máquina. O segundo *pendrive*, denominado de Mídia Chave (MC), serve para decriptografar a partição raiz onde se encontra o Sistema Operacional JE Connect na MSE, através de uma senha (PIN).

Um sistema denominado JEC Gerador é responsável por toda a parte de geração do sistema, geração de chave e criptografia da partição onde está o sistema operacional. Esse sistema JEC Gerador tem acesso restrito e é gerenciado por servidores da área de TI do Tribunais Regionais Eleitorais. A MSE está dividida em 3 partições (FAT, Boot e a Raiz do Sistema Operacional).

Ao selecionar o *pendrive* como dispositivo de boot, ocorre a seguinte sequência de eventos:

1. A partição de *boot* é decriptografada com informações de hardware do próprio *pendrive*;
2. Após decriptografar a partição de boot, o *bootloader* solicita a senha (PIN) da Mídia Chave para decriptografar a partição raiz do SO. A chave de criptografia está divida em 3 partes: A mídia chave (MC) contém uma parte da chave de criptografia do Sistema Operacional, o código PIN é outra parte e a identificação do hardware (número de série) do *pendrive* MSE é a outra parte;
3. Após a validação da senha, será decriptografada a partição raiz do Sistema Operacional;
4. Inicia o Sistema JE Connect apresentando a tela com as opções de conexão;
5. Sistema fecha a conexão com o servidor de VPN do TRE;
6. Somente após fechar a conexão VPN é liberada a inicialização do Sistema Transportador;

7. O sistema Transportador verifica as assinaturas digitais dos executáveis, entra em operação e fecha conexão *https* com o servidor responsável pela recepção dos arquivos no datacenter do Tribunal Regional Eleitoral.

Os demais procedimentos ocorrem como descrito anteriormente, de acordo com a operação normal do sistema Transportador, com a diferença de que o relatório "Espelho dos Diretórios" poderá ser salvo no partição FAT do *pendrive* para posterior impressão em cartório e anexação à ata da eleição.

Devido aos requisitos de segurança adicionais implantados (partição criptografada, ativação por mídia chave e senha), pode-se considerar que esse sistema é bem mais seguro que o sistema Transportador instalado nos micros padrão da Justiça Eleitoral. A ideia do TSE é utilizar o kit JE-Connect como solução padrão para transmissão dos resultados a partir das eleições de 2018.

5.15 Recuperação de Dados

O Sistema Recuperador de Dados (RED) é utilizado sempre que não for possível efetuar a leitura de uma Mídia de Resultado no sistema Transportador. Os motivos que levam a essa situação são erros estruturais na formação dos arquivos de resultado, que podem estar corrompidos. Ainda existe a possibilidade de que o *pendrive* da MR possa estar efetivamente vazio, ou por ter sido retirado pelo mesário antes que urna gravasse o resultado, ou não ter encerrado a votação.

A situação mais comum de utilização do RED é a de regerar o resultado em uma urna cuja votação foi encerrada normalmente, mas não teve a Mídia de Resultado gravada corretamente. Para isso, basta aguardar o recebimento da urna e proceder com a recuperação. Existe ainda a possibilidade de que o presidente de mesa não tenha conseguido encerrar a votação corretamente, embora todos os eleitores que compareceram na seção tenham votado normalmente. Assim, o RED oferece a opção para encerrar a votação e gravar a Mídia de Resultado para o Totalizador. A outra situação é a geração de um resultado parcial em uma urna que teve pane e não foi possível fazer a contingência, ou seja, tem uma parte dos votos na urna eletrônica e outra parte dos votos em cédulas de papel – veremos como resolver essa situação quando tratarmos do Sistema de Apuração na seção 5.16.

Pode acontecer de o drive do *pendrive* estar com defeito, impedindo a geração de resultado na urna original. Nesse caso é possível fazer a recuperação dos dados em uma urna de contingência. Para isso retira-se a *flash* de votação do drive da Flash Externa da urna e insere-se essa Flash de Votação juntamente com a MR RED em uma urna de contingência. O resultado será extraído dos dados contidos na FV.

O aplicativo Recuperador de Dados da urna sempre tenta, por padrão, recuperar o resultado da FV que está na Flash Externa. Supondo-se uma situação em que essa Flash de Votação esteja corrompida, será possível recuperar o resultado na urna original, que veio da seção, removendo-se a FV da Flash Externa e ligando a urna apenas com a MR RED. Assim, ao detectar ausência da Flash Externa, o RED vai recuperar os dados de votação a partir da Flash Interna.

5.16 Sistema de Apuração

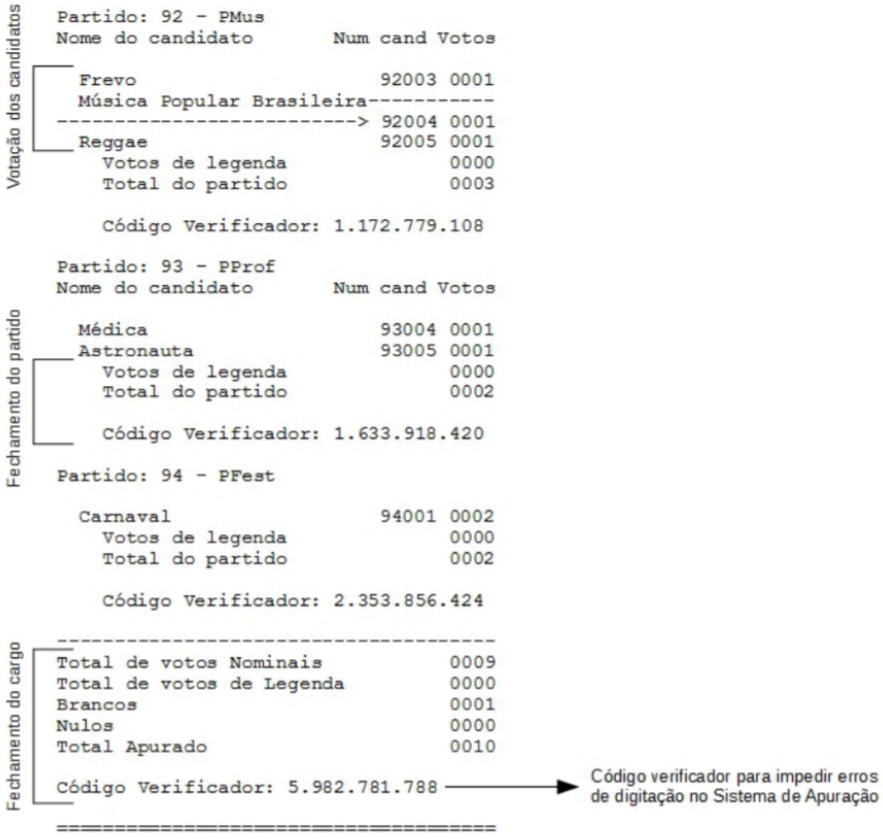
Todo o resultado de seção só poderá ser transmitido ao TRE a partir da leitura, no sistema Transportador, de uma MR gerada pela urna eletrônica. Existem 3 situações, no entanto, em que não dispomos dos resultado digital completo gerado pela urna:

1. Existe pelo menos uma via do Boletim de Urna impresso, mas não foi possível ler a MR com o resultado, nem recuperá-la com a MR RED, por problemas em ambos os cartões de memória (FE e FI), ou ainda, por indisponibilidade da urna eletrônica da seção.
2. Existe votação mista, ou seja, parte eletrônica, parte em cédulas de papel. Isso pode ocorrer quando, após transcorrido o início da votação eletrônica, a urna apresenta pane e nenhum dos procedimentos de contingência resolve o problema, obrigando a passar a votação para o método manual, utilizando uma urna de lona e cédulas de papel.
3. A votação ocorre totalmente manual. Em nenhum momento foi possível iniciar a votação eletrônica.

O Sistema de Apuração prevê solução alternativa a todas essas possibilidades. Em caso de votação totalmente manual, a junta apuradora deverá fazer o escrutínio das cédulas, que serão separadas por cargo, numeradas, apresentadas uma a uma aos fiscais presentes e lida em voz alta para o operador do Sistema de Apuração, que digitará o respectivo voto na

urna eletrônica. Ao final do processo, a urna emitirá um BU com cabeçalho indicando que foi gerado pelo Sistema de Apuração, e fará a gravação do resultado na MR, cujo arquivo de resultado será gerado com assinatura da urna usada pelo SA, seu número de série e indicativo de origem do BU a partir do SA. Os procedimentos relativos à apuração de cédulas com o SA estão descritas no Capítulo III da Resolução 23.456 que trata dos atos preparatórios para as eleições de 2016.

Figura 5.8 – Imagem parcial de um Boletim de Urna com código verificador para partidos e cargo



Fonte: TSE – QR Code no Boletim de Urna

No caso de votação totalmente eletrônica, existindo apenas a cópia do BU, esse BU será digitado no SA em opção específica do sistema. Após digitação dos dados do cabeçalho do BU, os votos serão inseridos (digitados) primeiro por cargo, em ordem de partido e número dos candidatos que possuem voto na urna. Cada grupo de votos de um partido possui um código verificador de 10 dígitos, para evitar erros de digitação nos votos dos candidatos.

Após a digitação de todos os candidatos (que receberam votos) de um partido, serão digitados os votos de legenda e o código verificador de fechamento do partido. Quando

encerrar a digitação dos candidatos de todos os partidos para um determinado cargo, deverá ser digitado o quantitativo de votos brancos e nulos e o código verificador de fechamento do cargo, e assim por diante até que encerre a digitação de todos os candidatos para todos os cargos. A figura 5.8 exibe um trecho de um BU com os códigos verificadores para fechamento de partido e para fechamento de cargo. Os demais códigos verificadores podem ser observados nas figuras 5.5 e 5.6.

No caso de votação mista, além do procedimento de escrutínio das cédulas de papel conforme descrito, há duas possibilidades de inserir o resultado eletrônico: por digitação do BU parcial (com os códigos verificadores) ou com a leitura da MR com resultado parcial gerado pelo RED.

5.17 Totalização e Divulgação dos Resultados

Já havíamos visto que o sistema Transportador é o responsável pela leitura das MRs com os resultados da votação e envio dos arquivos para os TREs. Após a transmissão dos resultados, esses arquivos são recebidos em uma aplicação Java, o RecArquivos. Ele tem a função de receber, verificar, decifrar e validar todos os arquivos de urna: resultado (BU), RDV, faltosos, justificativa, log, etc. Se o arquivo de resultado (BU) estiver íntegro, ele é enviado para o RecBU, que tratará de totalizar, ou seja, somar esses votos ao resultado da eleição no banco de dados.

Os BUs que estiverem íntegros e de acordo com a correspondência esperada pelo sistema, entram no sistema de totalização com *status* recebido. De tempos em tempos, eles passam automaticamente para o *status* totalizado, que significa que seus votos já foram somados ao resultado. Esse tempo geralmente é configurado entre 2 e 5 minutos, dependendo da capacidade do banco de dados de consumir os dados que são recebidos pelo RecBU.

Para minimizar o risco de ataques externos, o acesso a internet dos cartórios eleitorais, Tribunais Regionais Eleitorais e Tribunal Superior Eleitoral é bloqueado, desde a véspera da eleição até o final da totalização. De acordo com Giuseppe Janino, Secretário de Tecnologia da Informação do TSE, a rede da Justiça Eleitoral, às vésperas da eleição, chega a sofrer 200 mil tentativas de ataque por segundo[34]. A cada totalização dos dados, são gerados arquivos

[34] BRIGIDO, Carolina. Sistema da justiça eleitoral sofre 200 mil ataques de hackers por segundo – O Globo. Online. Disponível em: http://oglobo.globo.com/brasil/sistema-da-justica-eleitoral-sofre-200-mil-ataques-de-hackers-por-segundo-20213300

com dados de divulgação que são enviados para servidores específicos. A infraestrutura de divulgação de resultados utilizada pelo TSE possui sistema de proteção contra ataques. Esse sistema de proteção bloqueia por 10 minutos os endereços IP que realizam mais de 300 acessos por segundo. Assim, os parceiros que desenvolvem aplicativo próprio para divulgação devem configurar seus sistemas para que não ultrapassem esse limite.

Com relação à totalização, é necessário esclarecer que o resultado de votação dos candidatos na urna não será, necessariamente, o mesmo na totalização, ou seja, aquele exibido na divulgação. Isso pode ocorrer em função da situação dos candidatos. Candidatos que foram julgados irregulares, mas que entraram com recurso contra a decisão, recebem voto na urna eletrônica, mas a sua votação no sistema de totalização será anulada, até que a decisão seja reformada por uma instância superior. Nesse caso, deverá ser calculado um novo resultado da totalização, que converterá os votos anulados em votos nominais ao candidato e procederá com o recálculo do quociente eleitoral e partidário, em caso de cargos proporcionais, realizando nova distribuição de vagas.

5.18 Auditoria Pré e Pós-Eleição

Os partidos políticos e demais entidades legitimadas estão aptos a fiscalizar todo o processo eleitoral desde os seis meses anteriores a eleição, a partir do acompanhamento do desenvolvimento dos sistemas e depois, na Cerimônia de Assinatura Digital e Lacração dos Sistemas, na sede do Tribunal Superior Eleitoral. Nos Tribunais Regionais Eleitorais e cartórios eleitorais é possível fiscalizar a Cerimônia de Geração de Mídias e a Cerimônia de Carga das Urnas. Nessas cerimônias os sistemas e urnas eletrônicas estão sujeitos à auditoria para verificar assinaturas digitais dos programas e arquivos, além dos resumos digitais dos arquivos de acordo com o que foi gerado na cerimônia do TSE. Os logs dos sistemas utilizados nas estações de trabalho também estão à disposição dos partidos políticos. Antes da eleição é facultado ao partidos políticos auditar até 3% das urnas de cada município, sendo no mínimo uma por município e inclusive forçar a votação nessas urnas por meio da mídia de resultado VPP (Verificação Pré e Pós Eleição) durante o período de carga das urnas previsto em edital publicado em cartório.

Após a eleição, eventualmente podem surgir suspeitas a partir de relatos de eleitores, que levam os partidos a solicitar esclarecimentos ou solicitar auditoria nos cartórios eleitorais. Inicialmente, é preciso analisar criteriosamente cada situação, para que seja possível

identificar o que é erro de procedimento do eleitor e o que é tentativa de fraude. Por isso, sugere-se que, sempre que for recebida uma denúncia de fraude, o Juiz Eleitoral convoque os eleitores envolvidos para prestar um depoimento a fim de esclarecer minuciosamente o que ocorreu. O comportamento da urna durante a votação é exatamente o mesmo em qualquer seção eleitoral do país, já que se trata do mesmo sistema instalado em todas as urnas. No entanto, a maneira com que cada eleitor interage com o equipamento pode ser diferente, e muitas vezes, não corresponde ao comportamento esperado pelo sistema de votação.

Não havendo a constatação de erro de procedimento do eleitor, resta investigar a urna eletrônica. Por meio de auditoria, é possível verificar:

- Assinaturas Digitais: Deve-se verificar se os arquivos da urna estão assinados digitalmente pelas entidades legitimadas para esse procedimento na Cerimônia de Assinaturas Digitais e Lacração dos Sistemas no TSE. Esse procedimento é realizado através da Mídia de Auditoria (Verificador) do TSE ou do MP. Em tese, os partidos políticos poderiam apresentar o seu próprio programa de verificação das assinaturas, no entanto, nenhum deles teve interesse em comparecer na cerimônia realizada em 2016.
- Resumos Digitais: Deve-se verificar se os resumos digitais de todos os arquivos da urna correspondem aos resumos digitais que foram divulgados pelo TSE na Cerimônia de Lacração e publicados na internet. Esse procedimento é feito através da Mídia de Resultado VPP (Verificação Pré e Pós Eleição). Os arquivos publicados na internet estão no site do TSE, em Eleições > Eleições 2016 > Resumos digitais (*hashes*).
- Logs da urna eletrônica: É possível verificar todo o comportamento da urna eletrônica, passo-a-passo, desde o momento em que foi instalado o software oficial da eleição até o momento da auditoria através dos logs. São registrados em um arquivo a data, o horário e a descrição de cada evento ocorrido. Esses arquivos de log são enviados ao TRE juntamente com o resultado da votação, durante a transmissão dos resultados. Eles podem ser obtidos através da Mídia de Resultado VPP (Verificação Pré e Pós Eleição) ou junto ao TRE, evitando procedimentos urna a urna durante a noventena (período pós eleição em que as urnas devem permanecer lacradas). Os partidos políticos podem solicitar os logs de todas as seções, mas só podem obtê-los mediante auditoria com o VPP em um percentual determinado das urnas eletrônicas, conforme descrito na Resolução TSE nº

23.456/15. Ainda, o programa que faz a leitura desses arquivos de logs pode ser obtido no site do TSE, em Eleições > Eleições 2016 > Visualizador de log da urna.

- Visualização dos candidatos: É possível verificar as informações (foto, nome e número) de todos os candidatos que estavam concorrendo na urna eletrônica. Esse procedimento é feito através da Mídia de Resultado VPP (Verificação Pré e Pós Eleição).
- Resultados da urna eletrônica: Caso haja interesse ou necessidade, é possível regerar os arquivos de resultado da urna eletrônica - Mídia de Resultado da Votação, reimprimir Boletim de Urna ou Boletim de Urna de Justificativa. Esse procedimento é feito através da Mídia de Resultado VPP (Verificação Pré e Pós Eleição). O Boletim de Urna emitido com a MR do VPP pode ser comparado com:
    a. O Boletim de Urna proveniente da seção no dia da eleição, que está assinado pelo presidente de mesa e fiscais dos partidos políticos presentes no encerramento da votação, o qual encontra-se disponível no cartório;
    b. O Boletim de Urna publicado na internet no site do TSE em Eleições > Eleições 2016 > Boletim de urna na Web – Resultados por seção eleitoral;
    c. O resultado gerado por meio da leitura do QR Code pelo aplicativo Boletim na Mão com qualquer smartphone que tenha o aplicativo instalado;
    d. O Resultado por Seção, publicado na página da internet dos Tribunais Regionais Eleitorais, no qual é possível verificar a votação de um determinado candidato em cada seção e somar esses votos para comparar com o resultado final divulgado pelo TSE na sua página da internet em Eleições > Eleições 2016 > Resultados das Eleições 2016;
    e. O Registro Digital do Voto que pode ser disponibilizado aos partidos políticos.
- Registro Digital do Voto (RDV): Esse arquivo fornece uma relação de todos os votos que foram digitados na urna eletrônica, separados por cargo. É importante esclarecer que não são os votos na ordem em que foram digitados na urna ao longo da eleição, pois, se assim fosse, o sigilo do voto do eleitor estaria sendo violado. Esses arquivo contém o registro de todos os votos, embaralhados em uma listagem, como se fosse sorteada uma posição aleatória da lista para inserir cada um dos votos. O arquivo do RDV pode ser impresso pela urna através da Mídia de Resultado VPP (Verificação Pré e Pós Eleição), ou solicitado ao TRE, uma vez

que esse registro digital do voto também é enviado, juntamente com o resultado da urna, durante a transmissão dos dados ao Tribunal.

- Tabela de Correspondências: Esse relatório contém o código de identificação de carga de cada seção eleitoral, indicando a data e horário da instalação do software na urna, o código da urna da seção, o código do cartão de memória que instalou o sistema no equipamento e o resumo da correspondência. No site do TSE é possível obter a lista das correspondências esperadas (os códigos de identificação de carga de cada seção) que foram enviadas ao TRE pelos cartórios eleitorais, indicando quais urnas foram efetivamente preparadas para as seções eleitorais - ou seja, aquelas que receberam uma carga oficial, com edital publicado em cartório e sujeita a auditoria dos partidos -, além da lista das correspondências efetivadas, relação com os códigos de identificação de carga das urnas que efetivamente enviaram os resultados para o totalizador no TRE. De posse desses documentos, é possível fazer o cruzamento entre as urnas que foram carregadas na cerimônia de carga (registradas ata da cerimônia de carga), as urnas que foram para a seção eleitoral (zerésima de seção, boletim de urna da seção, trocas de urna registradas na ata da seção), log da urna e o relatório de correspondências esperadas e correspondências efetivadas do TSE. Esses relatórios podem ser obtidos no site do TSE, em Eleições > Eleições 2016 > Tabela de correspondência esperadas - 1o Turno.
- Votação forçada: Após a eleição, por requisitos de segurança do sistema, não é mais possível executar esse procedimento na urna, visto que a votação já foi encerrada. Entretanto, em hipóteses excepcionais, se o Juiz Eleitoral considerar necessário, o cartório pode solicitar à presidência do TRE autorização para dar nova carga de seção em uma urna eletrônica do cartório que não tenha sido utilizada na eleição, com a data da eleição que já passou, utilizando o mesmo cartão de memória utilizado na Cerimônia de Carga, para que o representante do pedido de auditoria acompanhe o processo de carga e posteriormente seja forçada a votação nessa urna através da Mídia de Resultado VPP (Verificação Pré e Pós Eleição).
- Atas da Eleição: Os interessados podem solicitar acesso ou cópias das atas da eleição (ata da Cerimônia de Geração de Mídias, ata da Cerimônia de Carga da Urnas, ata da Junta Eleitoral, Resultado da Totalização, etc.) para averiguações.

- Inspeção dos códigos-fontes armazenados em mídia não regravável que estão em envelope lacrado na sala-cofre do Tribunal Superior Eleitoral.

5.19 Testes Públicos de Segurança

O Brasil é o único país do mundo que submete seu sistema eletrônico de votação à prova de especialistas, equipes de investigadores e até mesmo *hackers* para testar eventuais vulnerabilidades no software e hardware da urna eletrônica. Até hoje foram realizados três eventos nesse sentido, denominados Testes Públicos de Segurança (TPS). O primeiro ocorreu em 2009, o segundo em 2012 e o terceiro em 2016, quando passou a ser obrigatório antes de cada eleição. A Resolução TSE nº 23.444/15[35] dispõe sobre a realização periódica dos Testes Públicos de Segurança (TPS) nos sistemas eleitorais que especifica.

As equipes interessadas se inscrevem para participar dos testes públicos e apresentam um plano de ataque, que será analisado por equipe técnica do TSE. A ideia é descartar planos de ataque que não agreguem em nada para evolução e melhoria do sistema. Além disso, o TPS tem caráter colaborativo: encontrada uma vulnerabilidade, o TSE deve poder identificá-la para proceder com a correção, inclusive ouvindo sugestões das equipes que participam dos testes.

As descobertas mais significativas ocorreram em 2012 e 2016. Em 2012 foi encontrada a vulnerabilidade relacionada ao algoritmo de embaralhamento do votos[36] [37], que era metade do caminho para quebra do sigilo do voto, conforme já foi descrito em detalhes na seção 5.13, que trata do Registro Digital do Voto.

Em 2016, dos 11 ataques aprovados, propostos por 4 equipes e mais um investigador independente, tiveram sucesso apenas três ataques, sendo que duas vulnerabilidades são

---

[35] Disponível em: <http://www.tse.jus.br/legislacao-tse/res/2015/RES234442015.htm>

[36] Avaliação sobre o Teste Público de Segurança 2012. Disponível em : <http://www.justicaeleitoral.jus.br/arquivos/tse-aspectos-tecnicos-da-seguranca-do-sistema-eletronico-de-votacao>

[37] ARANHA, D. F. et al. **(In)segurança do voto eletrônico no Brasil**. Fundação Konrad Adenauer, p. 117–133, 2014. Disponível em: <http://www.kas.de/wf/doc/13775-1442-5-30.pdf>.

bastantes relevantes: uma relacionada ao código verificador do BU[38], que é utilizado no Sistema de Apuração, e outra relacionada ao sistema de áudio para pessoas com necessidades especiais[39]. A terceira vulnerabilidade dizia respeito à invasão de uma seção em meio a votação, abertura física do gabinete da urna para retirada dos cartões de memória, dentre outros procedimentos que teriam que contar com a conivência dos componentes da mesa da seção (presidente de mesa e mesários), dos fiscais e eleitores presentes, além do óbvio rompimento dos lacres da urna, o que por si só ensejaria a anulação do resultado da seção. Detalharemos as duas descobertas mais importantes a seguir.

A vulnerabilidade relacionada ao código verificador no Sistema de Apuração, proposta pelo Grupo 1, consistia na utilização de um Boletim de Urna impresso, com votação falsa, mas com código verificador verdadeiro. Em uma situação de apuração totalmente eletrônica, ou seja, digitação de um BU completo no Sistema de Apuração, o BU original seria interceptado e trocado pelo BU falso e submetido à junta apuradora para que fosse digitado no SA. No TPS 2016, o Sistema de Apuração gerou uma mídia de resultado que poderia ser encaminhada ao sistema Transportador, o que indica a possibilidade de fraude alterando o resultado da votação. O teste foi bem sucedido para uma situação específica: votação para somente 2 cargos em disputa (2º turno, por exemplo) ou plebiscito. Nesse caso, um atacante teria que inviabilizar a geração de uma Mídia de Resultado, mesmo nos procedimentos de recuperação de dados, para forçar a necessidade de digitação de BU no SA.

Essa vulnerabilidade ocorreu devido à quantidade de dígitos do código verificador: apenas 5, ou seja 10^5 possibilidades diferentes para o código. As sugestões de mudanças propostas, que foram implementadas pelo TSE ainda antes da eleição, para correção da vulnerabilidade foram a geração de uma assinatura digital no BU, de forma a evitar sua falsificação e a ampliação da quantidade de dígitos do código verificador, que passou para 10 dígitos, de forma que não fosse possível gerar o mesmo código a partir de um número de votos factível. Ainda, segundo informações do TSE, em 2014 houve apenas 17 casos em todo o país que passaram por esse procedimento de digitação integral de um boletim de urna em 2º turno, ou seja 0,0037% das quase 460 mil seções.

---

[38] Teste Público de Segurança 2016 – Compêndio, pág 51-56, 109-112. Disponível em: <http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/teste-publico-de-seguranca-2016-compendio.pdf>

[39] Teste Público de Segurança 2016 – Compêndio, pág 51-56, 123-127. Disponível em: <http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/teste-publico-de-seguranca-2016-compendio.pdf>

A outra vulnerabilidade, proposta pelo Grupo 5, consistia na quebra do sigilo do voto através da gravação do áudio habilitado para pessoas com deficiência visual. Existem seções com muitos deficientes visuais em que o áudio da urna é habilitado por padrão para todos os eleitores. Em outras seções, o áudio não vem habilitado por padrão, mas pode ser habilitado mediante digitação de código específico no terminal do mesário. Em ambos os casos, o eleitor recebe um fone de ouvido, que é conectado à saída de áudio no painel traseiro da urna eletrônica. No TPS 2016, o grupo conectou um arduíno (*Raspberry Pi*) à saída de áudio da urna, que gravou o áudio da votação e transmitiu esse arquivo de áudio para um microcomputador, quebrando o sigilo do voto do eleitor.

Repare que esse procedimento teria que contar com o auxílio e a conivência dos componentes da mesa de votação e, eventualmente, até mesmo dos fiscais da seção, já que a parte traseira da urna fica exposta pela cabine de votação. Além disso, era necessário registrar a ordem de votação dos eleitores na seção, para que pudesse ser feito o mapeamento dos votos com os eleitores. A solução proposta, e que foi corrigida pelo TSE ainda antes da eleição, foi exibir uma mensagem na tela da urna, durante a votação, informando que o áudio está habilitado, para que o eleitor que está votando possa questionar o presidente de mesa.

5.20 Voto Impresso

Nas eleições gerais de 2002 tivemos uma experiência com o voto impresso em 150 municípios (abrangendo 6,18% do eleitorado nacional), com 19.373 seções das 320.185 seções eleitorais do país[40]. O estado do Sergipe e mais o Distrito Federal contaram com voto impresso em 100% das seções eleitorais. Nos outros estados brasileiros ficou a critério dos TREs definir quais municípios teriam o voto impresso. No estado do Rio Grande do Sul municípios escolhidos foram Esteio, Sapucaia do Sul e São Leopoldo.

A Lei nº 10.408 de 4 de janeiro de 2002, em seu artigo 1º estabelecia que:

> O art. 59 da Lei nº 9.504, de 30 de setembro de 1997, passa a vigorar acrescido dos §§ 4º a 8º, com a seguinte redação:
>
> "Art. 59 .....

[40] Relatório Eleições 2002. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-relarorio-resultado-eleicoes-2002>

> § 4º A urna eletrônica disporá de mecanismo que permita a impressão do voto, sua conferência visual e depósito automático, sem contato manual, em local previamente lacrado, após conferência pelo eleitor.
>
> § 5º Se, ao conferir o voto impresso, o eleitor não concordar com os dados nele registrados, poderá cancelá-lo e repetir a votação pelo sistema eletrônico. Caso reitere a discordância entre os dados da tela da urna eletrônica e o voto impresso, seu voto será colhido em separado e apurado na forma que for regulamentada pelo Tribunal Superior Eleitoral, observado, no que couber, o disposto no art. 82 desta Lei.
>
> § 6º Na véspera do dia da votação, o juiz eleitoral, em audiência pública, sorteará três por cento das urnas de cada zona eleitoral, respeitado o limite mínimo de três urnas por Município, que deverão ter seus votos impressos contados e conferidos com os resultados apresentados pelo respectivo boletim de urna.
>
> § 7º A diferença entre o resultado apresentado no boletim de urna e o da contagem dos votos impressos será resolvida pelo juiz eleitoral, que também decidirá sobre a conferência de outras urnas.[41]

Ainda, em seu artigo 4º, a lei estabelecia

> Art. 4º O Tribunal Superior Eleitoral definirá as regras de implantação progressiva do sistema de impressão do voto, inclusive para as eleições de 2002, obedecidas suas possibilidades orçamentárias.

O modelo de votação com o voto impresso consistia de uma urna eletrônica que contava com um Módulo Impressor Externo (MIE), conforme pode ser observado na figura 5.9 a seguir. O eleitor digitava na urna toda a sequência de votos (6 cargos em disputa naquela eleição). Após o eleitor preencher a sua intenção de voto para todos os cargos, a urna exibia em tela o resumo dos votos e imprimia esse mesmo resumo, exibindo o voto impresso para conferência do eleitor através de um *display* de acrílico. O eleitor, que não tinha contato com a cédula, deveria apenas comparar ambos os resumos e confirmar o voto, ou apertar a tecla corrige para reiniciar a sua votação, caso discordasse daquilo que estava sendo exibido ou comparado.

Caso o eleitor confirmasse o voto, a urna imprimia uma marca de voto válido na cédula impressa e depositava esse voto em um compartimento inviolável. Se o eleitor discordasse, apertando a tecla corrige, a cédula impressa recebia uma marca de voto cancelado, era depositada no mesmo compartimento inviolável e o ciclo de votação era reiniciado para que o eleitor escolhesse novamente seus candidatos. O processo de discordância daquilo que era apresentado ao eleitor poderia se repetir por, no máximo, 3 vezes, quando então o eleitor deveria votar em cédulas de papel e depositá-las em uma urna

[41] Lei 10.408/2002.

de lona separada, cujos votos seriam apurados ao final da eleição, no ambiente da junta eleitoral, por equipe designada pelo Juiz Eleitoral.

Figura 5.9 – A Urna Eletrônica 2002, com Módulo Impressor Externo (MIE).

Fonte: Biblioteca Digital do TSE.

Em uma breve análise desse modelo podemos apontar alguns problemas:

a) se apenas 1 eleitor passasse pelo procedimento de votação manual, no momento do escrutínio das cédulas, o sigilo do voto desse eleitor estaria comprometido. Mesmo que alguns poucos eleitores votassem dessa forma, as chances de quebra do sigilo do voto seriam grandes, bastando que todos (ou quase todos) escolhessem um mesmo candidato para algum dos cargos em disputa.
b) O escrutínio das cédulas de papel estaria sujeito aos mesmos problemas de manipulação dos resultados que já foram citados na seção 2.1 e que levaram a implantação do voto eletrônico
c) O processo de votação nesse modelo estaria sujeito a um ataque de negação de serviço, o que de fato ocorreu nos 3 municípios do RS. Alguns candidatos, inconformados com o resultado das eleições municipais do ano de 2000, fizeram intensa campanha nessas cidades orientando os eleitores a adotarem o procedimento de discordar da votação eletrônica, forçando o registro do voto

> manual em cédulas de papel para que fossem apuradas pelo método antigo de escrutínio.

Com relação ao item "c", se analisarmos os dados do TSE constantes no Relatório das Eleições Gerais 2002[42] é possível observar que, somente no estado do Rio Grande do Sul, das 789 seções dos 3 municípios que utilizaram urnas eletrônicas com o módulo impressor externo, ou seja, as seções com o voto impresso, tivemos apuração manual de cédulas de papel, utilizando o Sistema de Apuração (antigo Sistema de Voto Cantado) em 209 seções. Isso é equivalente a 26,49% do total de seções desses 3 municípios. Esse número é preocupante se observarmos que, no resto do estado que não utilizou o modulo impressor externo, tivemos apuração manual em cédulas de papel em apenas 0,26% das seções. A título de curiosidade, a última eleição em que tivemos a apuração de cédulas de papel em decorrência de votação manual, no estado do Rio Grande do Sul, foi a eleição de 2012, em apenas uma única seção. A eleição de 2002 foi a única, em 20 anos de urna eletrônica, que a Justiça Eleitoral enfrentou o que podemos considerar um ataque de negação de serviço à urna eletrônica que tenha sido bem sucedido.

O relatório do TSE vai além. Na página 20 são elencadas uma série de problemas:

> 40. A experiência demonstrou vários inconvenientes na utilização do denominado módulo impressor externo.
>
> 41. Sua introdução no processo de votação nada agregou em termos de segurança ou transparência. Por outro lado, criou problemas.
>
> 42. Nas seções eleitorais com voto impresso foi:
>
> a) maior o tamanho das filas;
> b) maior o número de votos nulos e brancos;
> c) maior o percentual de urnas com votação por cédula – com todo o risco decorrente desse procedimento;
> d) maior o percentual de urnas que apresentaram defeito, além das falhas verificadas apenas no módulo impressor.
>
> 43. Houve incidência de casos de enredamento de papel, possivelmente devido a umidade e dificuldades de manutenção do módulo impressor, seu armazenamento em espaços que já eram poucos para acomodar as urnas, quantidade adicional de lacres, que é grande, além de outros pertinentes ao custo do transporte.
>
> 44. No Rio de Janeiro, por exemplo, observou-se que cerca de 60% dos eleitores não examinaram o espelho do voto na impressora, o que sugere sua desnecessidade.
>
> 45. Na Bahia, por problemas de imperícia, o eleitor não conseguia finalizar sua votação, sendo-lhe então facultado votar em cédula de papel, na urna de lona.

[42] Relatório Eleições 2002. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-relarorio-resultado-eleicoes-2002>

> 46. Na análise feita na reunião conjunta do Colégio de Presidentes e do Colégio de Corregedores da Justiça Eleitoral, realizada em Florianópolis/SC, em 28 e 29 de novembro do ano passado, concluiu-se ser imperativa a eliminação do voto impresso no processo de votação.
>
> 47. Em seu lugar, com vantagens inquestionáveis sobre o modelo do voto impresso, dever-se-á introduzir o registro eletrônico do voto (cédula eletrônica), que espelha a composição do voto do eleitor, sem identificá-lo, e pode ser recuperado e impresso para atender a eventual pedido de verificação ou auditoria.
>
> 48. No Documento nº 1 estão reproduzidas planilhas estatísticas que comprovam os problemas relatados nos itens precedentes, contendo as quantidades e percentuais das urnas eletrônicas e módulos impressores externos substituídos em cada unidade da Federação, nos dois turnos das eleições, destacando-se os resultados verificados em Sergipe e no Distrito Federal, onde a impressão do voto foi adotada em todos as seções eleitorais.
>
> 49. Para que se possa aquilatar, nas eleições do Distrito Federal, no primeiro turno, o índice de quebra de urna eletrônica foi de 5,30%, enquanto a média nacional, mesmo majorada por essa elevada marca, foi de apenas 1,41%.
>
> 50. O percentual de seções que, em decorrência dessas quebras, passaram para votação manual foi de mais de 1% no Distrito Federal e em Sergipe, enquanto a média nacional ficou em apenas 0,20%. Em números absolutos, isto equivale a dizer que, das 299 seções eleitorais que passaram para votação manual, em todo o país, 66 delas estavam localizadas nessas duas unidades da Federação.
>
> 51. Outro dado que impressiona – e muito preocupa –, também ilustrado em planilha do Documento nº1, é o fato de, nas seções com voto impresso, 30,20% delas terem utilizado o sistema de voto cantado, enquanto nas seções que utilizaram urna eletrônica, sem voto impresso, o percentual foi de apenas 0,68%.
>
> 52. O voto cantado fragiliza o processo de votação e apuração, na medida em que possibilita a interferência da ação humana, com todas as suas conseqüências.
>
> 53. Pelos inconvenientes e riscos demonstrados na utilização do denominado módulo impressor externo e em vista de sua desnecessidade, a posição firmada na reunião conjunta do Colégio de Presidentes e do Colégio de Corregedores da Justiça Eleitoral, já referida, é no sentido da revogação da Lei nº 10.408/2002.
>
> 54. Cumpre observar que nas eleições gerais, em que foram realizados os testes, as ocorrências desfavoráveis não tiveram impacto no resultado do pleito.
>
> 55. Mas o voto impresso pode ter efeito desastroso em eleições municipais, muitas vezes decididas com diferença de poucas dezenas ou centenas de votos.[43]

Tendo em vista todos os problemas apontados, a Lei 10.740 de 1º de outubro de 2003 revogou o artigo 4º da Lei 10.408/2002 que obrigava a implantação do voto impresso no país, e instituiu o Registro Digital do Voto.

É evidente que a adoção do voto impresso como recurso de auditoria independente do resultado eletrônico traz uma camada a mais de transparência no processo. Entretanto, a

[43] Relatório Eleições 2002. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-relarorio-resultado-eleicoes-2002>

adoção de uma camada adicional de transparência não pode colocar em risco o que já foi conquistado com a adoção de outras barreiras de segurança. Além disso, deve-se considerar se o ganho em transparência e segurança é suficiente para compensar os prejuízos com usabilidade, eficiência e confiabilidade decorrentes da implementação do novo recurso. Ao analisarmos o caso real de 2002, percebe-se um aparente ganho de segurança percebido pela população, com mero efeito tranquilizador, ao custo de perdas reais em usabilidade, segurança e eficiência na votação e apuração.

Ao contrário do que se pode imaginar, a reintrodução do voto em papel – ainda que sobre o pretexto de uma verificação independente que permita uma recontagem paralela ao resultado eletrônico – apenas enfraquece o processo. A manipulação dos votos em papel é um fator crítico de vulnerabilidade, que já havia sido eliminado anteriormente, e não faz sentido reintroduzi-lo no processo pelos seguintes motivos:

a) O Registro Digital do Voto está disponível aos partidos políticos e permite a recontagem voto a voto;
b) A Votação Paralela, ainda que por amostragem, já demonstra a integridade dos resultados produzidos pelas urnas eletrônicas, comprovando que os votos aleatórios inseridos na urna correspondem fielmente àquilo que é impresso no boletim de urna ao final da votação;
c) Embora o voto impresso permita uma recontagem paralela ao resultado eletrônico, a impressão do voto continua dependendo da validação do software instalado na urna, o qual gerencia a impressão dos votos;
d) Havendo divergência entre o resultado eletrônico e o das cédulas de papel, em qual confiar? O eletrônico, produzido pela máquina, cujo software está disponível para análise e pode ser auditado; ou o resultado em papel, que pode ser manipulado, depende de intensa fiscalização e pressupõe a idoneidade absoluta de todos os envolvidos no processo?
e) Ao contrário do que os defensores do voto impresso insistem em argumentar, os modelos de urna eletrônica VVPT não são imunes à fraudes. Estudos já identificaram mais de 40 potenciais ataques a urnas eletrônicas com voto impresso[44] (Brennan, 2006, pág. 61).

[44] Brennan Center Of Justice. The Machinery of Democracy: Protecting Elections in an Electronic World. Disponível em: <http://www.brennancenter.org/sites/default/files/legacy/d/download_file_36343.pdf>

f) O voto impresso produz meramente um efeito tranquilizador no eleitor, passando uma falsa sensação de segurança, visto que ele ignora os riscos envolvidos no processo de escrutínio das cédulas de papel – uma realidade distante, praticamente perdida no passado, há quase 20 anos. O eleitor simplesmente acredita que o voto será corretamente apurado, o que não é necessariamente uma verdade absoluta. Além disso, caso a impressora trave durante a impressão e necessite de troca ou manutenção, o sigilo do voto do eleitor que acabou de votar estaria comprometido, pois estará visível no *display* do módulo impressor.

g) Os eleitores nem sempre verificam o voto impresso. Estudos feitos no MIT testando máquinas de votar do tipo VVPAT identificaram que, em um teste com 36 pessoas testando o sistema, de 108 casos em que o voto impresso foi gerado diferente daquilo que o eleitor digitou na urna, apenas 3 casos foram identificados/percebidos pelo eleitor[45].

h) A impressora é controlada pelo software da urna, o qual invariavelmente deve ser analisado. Seria muito mais fácil e lógico empreender esforços na análise do código em busca do nível de transparência desejado.

i) Com relação a apuração manual dos votos em papel pelas circunstâncias já descritas anteriormente, não é possível garantir o sigilo do voto e tampouco garantir o correto escrutínio dessas cédulas. Não são poucos os casos em que foi necessário recorrer a esse procedimento conforme observado no relatório das Eleições Gerais de 2002.

j) De acordo com o princípio da condução do voto (Camargo, 2004)[46] seria *possível a produção de pelo menos um voto distinguível de todos os demais a partir de um conjunto enumerável de votos*. O princípio se baseia no fato de que, com vários cargos em disputa, um grupo determinado de candidatos, pelo meio da fraude de compra de votos, atribuiria uma combinação específica de votação em candidatos da mesma legenda ou coligação, garantindo a eleição dos candidatos da chapa majoritária e a formação dos votos necessários à legenda. Para exemplificar,

---

[45] Brennan Center Of Justice. The Machinery of Democracy: Protecting Elections in an Electronic World. Pág 66. Disponível em: <http://www.brennancenter.org/sites/default/files/legacy/d/download_file_36343.pdf>

[46] CAMARGO, Carlos Rogério. REGISTRO DIGITAL DO VOTO. Disponível em: <http://www.tre-sc.jus.br/site/resenha-eleitoral/revista-tecnica/edicoes-impressas/integra/2012/06/registro-digital-do-voto/index7d5a.html?no_cache=1&cHash=84a3e14af2869094df5cac794bb61eb6>

> vamos imaginar um conjunto de 1 governador, 7 deputados federais e 10 deputados estaduais. Assim, 1*7*10 = 70 combinações de votos distinguíveis. Se cada combinação desses votos for distribuída a 3 eleitores, teríamos 210 votos em uma única seção eleitoral – o que representa mais da metade dos votos de muitas seções pelo país. O voto impresso permitiria essa conferência. Já o Registro Digital do Voto, pela sua característica de desassociação dos votos entre cargos distintos, não permite essa inferência.

A adoção do voto impresso trata-se de um retrocesso, pois o paradigma agora é eletrônico. É preciso pensar em soluções dentro desse contexto, tal qual o Registro Digital do Voto, a Votação Paralela e soluções para uma análise profunda e eficiente do código da urna. Na contramão do que poderia ser uma evolução nesse sentido, o Congresso Nacional mais uma vez aprova uma lei[47] tornando obrigatório o voto impresso. A Lei 13.165 de 29 de setembro de 2015 torna obrigatória a impressão do voto a partir das eleições gerais de 2018.

Os partidos políticos abrem mão da prerrogativa (e dos custos) de indicar técnicos especializados para inspecionar o software do ecossistema da urna enquanto o Congresso Nacional transfere os custos de implantação do voto impresso para a população: Os grupos de trabalho do TSE que estudam a implantação do voto impresso estimam que o custo de aquisições e implantação para todas as urnas eletrônicas do país é próximo a 1,5 Bilhão de Reais[48], sendo 17,6 Milhões de Reais somente em bobinas de papel para cada eleição, além de outros 10 Milhões de Reais em logística.

Partindo-se do pressuposto de que é inevitável a implantação do voto impresso, há que se pensar em soluções para minimizar os riscos decorrentes dessa alteração:

A auditoria pela recontagem dos votos deve ser feita apenas por amostragem, nos mesmos moldes em que ocorre a votação paralela, em ambiente controlado, filmado e fiscalizado por partidos políticos e empresa independente de auditoria. Dessa forma evita-se custos exorbitantes com a instalação de juntas apuradoras e concentra-se esforços em garantir a integridade das seções auditadas.

As cédulas impressas devem ser cortadas, ou seja, separadas da bobina de papel após a impressão, de forma a impedir inferências sobre a ordem de votação, preservando assim, o

---

[47] Disponível em: http://www12.senado.leg.br/noticias/materias/2015/12/28/eleicoes-terao-voto-impresso-a-partir-de-2018

[48] Disponível em: <http://www.gazetadopovo.com.br/vida-publica/tse-conclui-urna-eletronica-nao-errou-nos-votos-de-2014-foi-falha-humana-753dv3nms6npqgwjfjpvzfv7w>

sigilo do eleitor. Cada urna eletrônica deve gravar nas cédulas impressas um código único, que associe a cédula ao hardware que produziu essa impressão. Esse mecanismo teria objetivo de impedir que, durante o escrutínio, se misturassem cédulas de diferentes seções. Além disso, seria interessante a impressão de um código, o qual não pudesse ser visualizado pelo eleitor, que associasse a cédula impressa ao registro digital do voto, para fins de auditoria.

5.21 Resumo dos principais mecanismos

A Figura 5.10 abaixo apresenta de forma visual uma relação dos requisitos de verificação e validação, controle, segurança, transparência e recuperação do processo eleitoral e quais mecanismos existentes que contribuem para atender esses requisitos.

Figura 5.10 – Principais mecanismos do Sistema Brasileiro de Votação Eletrônica.

	Verificação / Validação	Segurança	Controle	Transparência	Recuperação
Assinaturas Digitais	x	x	x		
Auditoria Pré e Pós Eleição	x		x	x	
Boletim de Urna	x		x	x	x
Cadastro Biométrico	x	x	x		
Carga das Urnas		x	x	x	
Contingências	x				x
Geração de Mídias		x	x	x	
Hardware da Urna	x	x	x		
Inspeção do Código	x			x	
Lacração dos Sistemas		x	x	x	
Recuperação de Dados		x			x
Registro Digital do Voto	x	x	x	x	
Resumos Digitais	x	x	x	x	
SIS	x	x	x		
Sistema de Apuração	x	x	x	x	x
Tabela de Correspondências	x		x	x	
Testes Públicos de Segurança	x			x	
Totalização e Divulgação	x	x	x	x	
Transmissão de Dados	x	x	x		
Votação Paralela	x			x	
Voto Impresso	x			x	x
Zerésima			x	x	

Fonte: Autor.

6 CONCLUSÃO

A definição de qual modelo de máquina de votar escolher deve levar em consideração os problemas a serem resolvidos, as características culturais, o contexto local em que se encontra o eleitorado e a legislação eleitoral vigente. A partir dos requisitos identificados será possível estabelecer as premissas mais adequadas para um modelo eletrônico de votação. Algumas máquinas de votar já existentes poderão estar em maior ou menor conformidade com essas premissas. É possível adaptar um determinado modelo a cada realidade, mas, na maioria dos casos pode ser melhor especificar um projeto do início, totalmente focado nos aspectos necessários e que atenda plenamente os requisitos. Para cada realidade existe uma solução que melhor atende às necessidades. Se olharmos isoladamente o modelo da urna eletrônica brasileira ele provavelmente não atende as necessidades de muitos países, mas tem servido muito bem ao Brasil.

Evidente que ainda há margem para melhorias no sistema brasileiro de votação eletrônica, com a introdução de novas tecnologias, mecanismos de auditabilidade e inspeção do código, visando ampliar a transparência e a segurança do sistema. Os testes públicos de segurança têm demonstrado isso. Na medida do possível, o sistema atual tenta atender às necessidades de um modelo DRE. O acompanhamento do desenvolvimento dos sistemas, a possibilidade de inspeção do código, a lacração dos sistemas e os testes públicos de segurança visam atender as salvaguardas relacionadas à integridade e correção do software. O encadeamento de segurança baseado em hardware, a autenticação do software da urna mediante protocolos criptográficos e assinaturas digitais, são barreiras indispensáveis para garantir a autenticidade e integridade do código. Os processos de auditoria, de verificação de assinaturas e resumos digitais, o acompanhamento da geração de mídias e carga de urnas, a disponibilização de tabelas de correspondências, a publicação dos boletins de urna para conferência e a votação paralela, trazem mais transparência, confiabilidade e proporcionam a ampla participação dos partidos políticos e da sociedade em geral.

Para fins de verificação da correção do software, a análise do código, embora de maior complexidade técnica, é um instrumento que apresenta menor risco e menores custos do que a impressão do voto, por exemplo. Além disso, a logística para implementação e auditoria do voto impresso se demonstrou um verdadeiro tormento para a Justiça Eleitoral no passado. Esse processo (da impressão do voto) demandará muito estudo e planejamento para a implantação e certamente terá um longo caminho até atingir a maturidade desejável, já que para suprir um único requisito ensejará uma série de novas barreiras de segurança e processos

de auditoria. Ademais, entendo dispensável a adoção do voto impresso, tendo em vista os efeitos negativos já abordados no presente estudo.

Por fim, é fundamental destacar que todos os mecanismos previstos no sistema brasileiro de votação eletrônica só terão seus objetivos atendidos com a efetiva participação da sociedade, dos partidos políticos e das entidades legitimadas nos processos de auditora e verificação. Assim, cabe à Justiça Eleitoral e aos partidos políticos promoverem o acesso da sociedade em geral, divulgando os mecanismos de segurança e aproximando os eleitores dos conceitos, para que se alcance a necessária confiança no processo eleitoral. Somente assim, teremos a democracia, em seu sentido mais amplo, plenamente atendida.

REFERÊNCIAS

ARANHA, D. F. et al. **(In)segurança do voto eletrônico no Brasil**. Fundação Konrad Adenauer, p. 117–133, 2014. Available from Internet: <http://www.kas.de/wf/doc/13775-1442-5-30.pdf>. Acesso em: 19 nov 2016

BRASIL, Senado Federal. Agência Senado. **Eleições terão voto impresso a partir de 2018**. Brasília, 2015. Disponível em: <http://www12.senado.leg.br/noticias/materias/2015/12/28/eleicoes-terao-voto-impresso-a-partir-de-2018>. Acesso em: 11 nov. 2016.

BRASIL. Tribunal Superior Eleitoral. Apresentação da Palestra dos Testes Públicos de Segurança. Testes Públicos de Segurança. TSE: Brasília, março 2016.

BRASIL. Tribunal Superior Eleitoral. **Avaliação dos Testes Públicos de Segurança**. TSE: Brasília, março de 2012. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-avaliacoes-sobre-o-teste-de-seguranca-da-urna-eletronica> Acesso em: 19 nov. 2016.

BRASIL. Tribunal Superior Eleitoral. **Desenvolvimento dos sistemas da urna pode ser acompanhado por partidos e instituições**. TSE: Brasília, maio de 2016. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2016/Maio/desenvolvimento-dos-sistemas-da-urna-podem-ser-acompanhados-por-partidos-e-instituicoes> Acesso em: 15 nov. 2016.

BRASIL. Tribunal Superior Eleitoral – **Eleições Seguras: assinatura digital e lacração garantem autenticidade e integridade dos sistemas eleitorais**. Brasília: Imprensa, TSE, 2016. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2016/Agosto/eleicoes-seguras-assinatura-digital-e-lacracao-asseguram-autenticidade-e-integridade-dos-sistemas-eleitorais >. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral – Estatísticas de Justificativa Eleitoral – Origem e Destino. Brasília: TSE. Online. Disponível em: <http://www.tse.jus.br/eleitor/estatisticas-de-eleitorado/origem-e-destino>. Acesso em: 25 nov. 2016

BRASIL. Tribunal Superior Eleitoral – **Informatização do Voto: Histórico**. Brasília: TSE, 2016. Disponível em: <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/eleicoes>. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral – Processo TSE 20.038/2014 – Anexo IV – Especificações de Criptografia e Segurança de Hardware e Software. Urnas Eletrônicas – UE2015, Brasília: TSE, 2014.

BRASIL. Tribunal Superior Eleitoral – **QR Code no boletim de urna:** Manual para criação de aplicativos de leitura. Brasília: TSE, 2016. 60 p. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-manual-para-a-criacao-de-aplicativos-de-leitura>. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral – **Relatório das Eleições 2002**, Brasília: TSE, 2003. 274 p. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-relarorio-resultado-eleicoes-2002>. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral. **Resolução 23.444/2015**. Dispõe sobre a realização periódica do Teste Público de Segurança – TPS nos sistemas que especifica. Disponível em: <http://www.tse.jus.br/legislacao-tse/res/2015/RES234442015.htm>. Acesso em: 21 nov. 2016

BRASIL. Tribunal Superior Eleitoral. **Resolução 23.456/2015**. Dispõe sobre os atos preparatórios para as eleições de 2016. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-456-instrucao-53-680>. Acesso em: 12 nov. 2016

BRASIL. Tribunal Superior Eleitoral. **Resolução 23.458/2015**. Dispõe sobre a cerimônia de assinatura digital e fiscalização do sistema eletrônico de votação, do registro digital do voto, da auditoria de funcionamento das urnas eletrônicas por meio de votação paralela e dos procedimentos de segurança dos dados dos sistemas eleitorais para o pleito de 2016. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-resolucao-23-458-instrucao-53-765>. Acesso em: 12 nov. 2016

BRASIL. Tribunal Superior Eleitoral – **Serie Urna Eletrônica: biometria garante registro único de cada eleitor**. Brasília: Imprensa, TSE, 2016. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2016/Janeiro/serie-urna-eletronica-biometria-garante-registro-unico-de-cada-eleitor >. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral – **Serie Urna Eletrônica: sistema de batimento biométrico confere mais segurança às eleições**. Brasília: Imprensa, TSE, 2016. Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2016/Janeiro/serie-urna-eletronica-sistema-de-batimento-biometrico-confere-mais-seguranca-as-eleicoes >. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral – **Sistema Eletrônico de Votação:** perguntas mais frequentes. 2ª ed. Brasília: TSE, 2015. 34 p. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-perguntas-mais-frequentes-sistema-eletronico-de-votacao>. Acesso em: 11 nov. 2016

BRASIL. Tribunal Superior Eleitoral. **Testes Públicos de Segurança: Aspectos Técnicos da Segurança do Sistema Eletrônico de Votação**. TSE: Brasília, março de 2012. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-aspectos-tecnicos-da-seguranca-do-sistema-eletronico-de-votacao> Acesso em: 19 nov. 2016.

BRASIL. Tribunal Superior Eleitoral. **Teste Público de Segurança 2016 do sistema público de votação: compêndio**. Brasília: Tribunal Superior Eleitoral, 2016. 157 pág. Disponível em: <http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/teste-publico-de-seguranca-2016-compendio.pdf> Acesso em: 22 nov. 2016.

BRENNAN. **The Machinery Of Democracy: Protecting elections in an electronic world**. Brennan Center Task Force on Voting System Security, Lawrence D. Norden, Chair. Brennan Center of Justice: NYU School Of Law, New York, NY, 2006

BRIGIDO, Carolina. Sistema da justiça eleitoral sofre 200 mil ataques por segundo – O Globo. Online. Out 2016. Disponível em: <http://oglobo.globo.com/brasil/sistema-da-justica-eleitoral-sofre-200-mil-ataques-de-hackers-por-segundo-20213300>. Acesso em: 25 nov 2016

CAMARGO, Carlos Rogério. **REGISTRO DIGITAL DO VOTO**. RESENHA ELEITORAL - Nova Série, v. 11, n. 2 (jul./dez. 2004). Disponível em: <http://www.tre-sc.jus.br/site/resenha-eleitoral/revista-tecnica/edicoes-impressas/integra/2012/06/registro-digital-do-voto/index7d5a.html?no_cache=1&cHash=84a3e14af2869094df5cac794bb61eb6> Acesso em: 19 nov 2016

CUNHA, A. A. Portinho da. **A Evolução dos Mecanismos de Transparência no Desenvolvimento do Projeto de Votação Eletrônica no Brasil: 1996-2008**. Trabalho de Conclusão de Curso de Especialização. Pós-Graduação em Administração. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2009

ESTONIA. National Electoral Comittee. **Internet Voting at the Elections of Local Government Councils on October 2005.** Report. 2006. Disponível em: <http://www.vvk.ee/public/dok/report2006.pdf>. Acesso em: 06 nov 2016.

NATIONAL DEMOCRATIC INSTITUTE. **Electronic Voting and Counting Around The World**. Disponível em: <https://www.ndi.org/e-voting-guide/electronic-voting-and-counting-around-the-world>. Acesso em: 04 nov 2016.

OFFICE FOR DEMOCRATIC INSTITUTIONS AND HUMAN RIGHTS (OSCE/ODIHR). **Federal Republic Of German - Elections To The Federal Parliament (Bundestag)**. 27 Sep 2009. Disponível em: <http://www.osce.org/odihr/elections/germany/40879?download=true>. Acesso em: 06 nov 2016.

RIO GRANDE DO SUL. Tribunal Regional Eleitoral. **Votação Paralela**. Auditoria para verificação do funcionamento das urnas sob condições normais de uso. Folder. Porto Alegre: TRE-RS, 2016. Disponível em: <http://www.tre-rs.jus.br/upload/27/Folder_Votacao_Paralela_2016.pdf> Acesso em: 19 nov 2006

RIO GRANDE DO SUL. Tribunal Regional Eleitoral. **Votação Paralela**. Auditoria para verificação do funcionamento das urnas sob condições normais de uso. Folder. Porto Alegre: TRE-RS, 2016. Disponível em: <http://www.tre-ce.jus.br/arquivos/faq-votacao-paralela-2016/at_download/file> Acesso em: 19 nov 2006

RIO GRANDE DO SUL. Tribunal Regional Eleitoral. **Voto Eletrônico**. Edição comemorativa: 10 anos da urna eletrônica; 20 anos do readastramento eleitoral. Porto Alegre: TRE-RS / Centro de Memória da Justiça Eleitoral, 2006

RIVEST, Ronald L; WACK, John P. **On The Notion Of Software Independence in voting systems**. Massachusetts Institute of Technology: Cambridge. Jul, 2006. Disponível em: <http://people.csail.mit.edu/rivest/pubs/RW06.pdf> Acesso em: 25 nov 2006

UNICAMP. Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica). UNICAMP: Maio 2002. Disponível em: <http://www.tse.jus.br/eleicoes/biometria-e-urna-eletronica/relatorio-da-unicamp-urnas-eletronicas>. Acesso em: 06 nov 2016.

GLOSSÁRIO

Carga de Urnas: Nomenclatura utilizada pela Justiça Eleitoral para o processo de instalação do software da Justiça Eleitoral nas urnas eletrônicas.

Voto Cantado: Era o antigo nome do atual Sistema de Apuração. Eles possuem praticamente as mesmas funções. A troca de nome se deu para representar melhor a função deste sistema.