Instituto Serzedello Corrêa

Auditoria da votação eletrônica: possibilidades de atuação do controle externo

Paulo Vinícius Menezes da Silveira

Orientador: Tiago Modesto Carneiro Costa

Coletânea de Pós-Graduação, v.2 n.17

Auditoria do Setor Público

TRIBUNAL DE CONTAS DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL

TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

José Mucio Monteiro (Presidente)
Ana Arraes (Vice-presidente)
Walton Alencar Rodrigues
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz de Oliveira
Raimundo Carreiro
Bruno Dantas
Vital do Rêgo

MINISTROS-SUBSTITUTOS

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho
Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Cristina Machado da Costa e Silva (Procuradora-Geral)
Lucas Rocha Furtado (Subprocurador-geral)
Paulo Soares Bugarin (Subprocurador-geral)
Marinus Eduardo de Vries Marsico (Procurador)
Júlio Marcelo de Oliveira (Procurador)
Sérgio Ricardo Costa Caribé (Procurador)
Rodrigo Medeiros de Lima (Procurador)

Instituto Serzedello Corrêa
Escola Superior do Tribunal de Contas da União

PROJETO GRÁFICO E CAPA
Núcleo de Comunicação - NCOM/ISC

Instituto Serzedello Corrêa
Escola Superior do Tribunal de Contas da União

PÓS-GRADUAÇÃO EM AUDITORIA FINANCEIRA

Auditoria da votação eletrônica: possibilidades de atuação do controle externo

Paulo Vinícius Menezes da Silveira

Orientador(a):
Tiago Modesto Carneiro Costa

Brasília | 2019

Dedicatória

Dedico esse trabalho à minha esposa, Beatriz e a meus filhos João Pedro e Lígia, por serem absolutamente especiais e terem dado um apoio especial nesta etapa de minha vida e a meus pais, por sempre terem acreditado e investido em mim.

Agradecimentos

Agradeço inicialmente ao meu orientador, Tiago Costa, por me guiar na etapa final deste curso.

Agradeço também aos professores e à equipe do ISC, que tanto nos apoiaram nesta jornada, bem como aos vários amigos que fiz durante as aulas.

Por fim, agradeço à Ana Paula Silva da Silva e a Secretaria de Controle Externo da Administração do Estado pelas iniciativas e apoio em capacitar os auditores da unidade técnica.

Resumo

A cada eleição surgem críticas ao uso de urnas eletrônicas e à falta de auditoria no pleito. Frequentemente são feitas associações entre o uso de urnas eletrônicas e a potencial ocorrência de fraudes nas eleições brasileiras. A sociedade delegou à Justiça Eleitoral a organização das eleições, entretanto os cidadãos têm na própria Justiça Eleitoral a fonte de informações sobre a lisura da votação eletrônica. O objetivo deste trabalho é analisar boas práticas internacionais relacionadas à votação eletrônica e compará-las com as normas da Justiça Eleitoral, com a finalidade de colecionar tipos e técnicas de auditoria a serem utilizadas em auditorias externas que avaliem se o processo de votação brasileiro em urnas eletrônicas garante o devido registro e totalização dos votos dos eleitores, identificando e avaliando o risco de fraudes. Os objetivos específicos foram: descrever boas práticas internacionais relacionadas à votação eletrônica; descrever processos de trabalhos da justiça eleitoral nos quais poderiam ser executados procedimentos de auditoria, buscar identificar e avaliar os riscos de fraude; relacionar métodos e ferramentas de auditoria que possam ser aplicados ao processo de votação; e sugerir calendário de auditorias em sintonia com o processo eleitoral. Esta é uma pesquisa aplicada, qualitativa e exploratória, que se utilizou de pesquisa bibliográfica documental. Foram analisadas diretrizes europeias e americanas sobre a votação eletrônica e as normas da Justiça Eleitoral. Constatou-se haver lacunas em diretrizes sobre transparência e observação, bem como em *accountability*, notadamente pela ausência de uma certificação do *hardware* e *software* e de uma avaliação independente da votação eletrônica, em que pese o acompanhamento do processo de votação eletrônica ser franqueado aos partidos políticos, à Ordem dos Advogados do Brasil, ao Ministério Público e a outras entidades. A partir desse entendimento sugeriu-se quatro auditorias a serem realizadas no ano em que houver eleições gerais, que juntas iriam, por meio de evidências suficientes e apropriadas, formar uma convicção que asseguraria a lisura da votação eletrônica e da totalização dos votos. Haveria uma auditoria no *hardware* e no *software* para assegurar que as urnas eletrônicas sigam as especificações requeridas pelo Tribunal Superior Eleitoral (TSE), que os programas garantam a segurança do sistema e funcionem de forma que os votos sejam coletados e gravados conforme a vontade do eleitor. As segunda e terceira auditorias seriam realizadas após cada pleito para certificar a exatidão da totalização de votos realizada pela Justiça Eleitoral. Por fim, uma quarta auditoria utilizaria amostragem probabilística para selecionar urnas nas quais seriam verificadas a integridade física e lógica, bem como se os arquivos obtidos nas outras auditorias seriam os mesmos armazenados nas urnas. Considera-se haver uma assimetria de informações entre o TSE e a sociedade, à medida que o órgão recebe poderes e recursos para realizar o processo eleitoral e a sociedade passa a depender unicamente da Justiça Eleitoral para obter informações sobre o processo. Isso poderia ser mitigado pela atuação de um órgão externo e independente na avaliação da votação eletrônica.

Palavras-chave: Urna Eletrônica; Votação Eletrônica; Auditoria nas Eleições; Eleições.

Lista de Figuras

Lista de Tabelas

Lista de Gráficos

Lista de Siglas

ABR - Auditoria baseada em risco

BU - Boletim de urna

CF - Constituição Federal

CoE - *Council of Europe*

DRE - *Direct-recording electronic*

DVR - Diagrama de verificação de riscos

EAC - *U.S. Election Assistance Commission*

EUA - Estados Unidos da América

Fiscam - *Federal Information System Controls Audit Manual*

GAO - *U.S. Government Accountability Office*

IIDEA - *International Institute for Democracy and Electoral Assistance*

IN - Instrução Normativa

Intosai - Organização Internacional de Entidades Fiscalizadoras Superiores

ISSAI - Normas Internacionais das Entidades Fiscalizadoras Superiores

JE - Justiça Eleitoral

NAT - Normas de Auditoria do Tribunal de Contas da União

RDV - Registro digital de voto

RDV-CE - Registro digital de voto criptografado pelo controle externo

TCE - Tribunal de Contas do Estado

TCM - Tribunal de Contas do Município

TCU - Tribunal de Contas da União

TPM - Teste Público de Segurança

TRE - Tribunal Regional Eleitoral

TSE - Tribunal Superior do Eleitoral

UT - Unidade Técnica

VAP - Verificador de Autenticação de Programas

VPP - Verificação Pré-Pós Eleição

VVSG - *Voluntary Voting System Guidelines*

Sumário

1. Introdução

A cada eleição surgem críticas ao uso de urnas eletrônicas e a falta de auditoria no pleito. Frequentemente são feitas associações entre o uso de urnas eletrônicas e a potencial ocorrência de fraudes nas eleições brasileiras.

As eleições são de responsabilidade da Justiça Eleitoral (JE), que é composta pelo Tribunal Superior Eleitoral (TSE), por 27 tribunais regionais eleitorais (TRE), pelas juntas eleitorais e pelos juízes eleitorais. Nas eleições de 2018 existiram mais de 450.000 seções eleitorais, cada uma delas utilizando uma urna eletrônica para a votação.

Conforme van de Graaf (2018, p. 32), o uso da urna eletrônica traz uma sensação de caixa preta tendo o eleitor uma dificuldade em entender o que acontece com o voto sendo processado pelo equipamento. O sistema é fechado e o eleitor tem que confiar cegamente no sistema eleitoral, fica dependente da corretude do software do equipamento para que o voto seja computado e totalizado pela JE.

A desconfiança com o processo eleitoral encontra-se aderente à teoria da agência e o conflito da agência. Segundo Hoque (2006), um relacionamento de agência aparece quando uma parte (o principal) contrata outra (o agente) para executar uma tarefa, o que envolve o agente tomar decisões em nome do principal.

De acordo com Neto (2017), o agente recebe e aceita uma delegação de recursos e poderes e, por dever dessa delegação, precisa gerenciar tais recursos e exercer tais poderes mediante estratégias e ações que permitam alcançar os objetivos e cumprir a missão que lhe foi incumbida, bem como informar sobre como ela está sendo cumprida (transparência e prestação de contas). Na esfera pública, verifica-se o problema de agência na relação entre principal, representado pela sociedade, e o agente, intrínseco ao Estado. O agente no caso das eleições é a Justiça Eleitoral, representada pelo TSE e pelos Tribunais Regionais Eleitorais (TRE).

Dessa relação surge o conceito de accountability, que envolve pelo menos duas partes, uma que delega responsabilidades e outra que aceita cumpri-las, surgindo aí a necessidade de prestação de contas. É também aí que surge a necessidade de uma terceira parte para fornecer asseguração, que mitigue a assimetria de informação e o conflito de agência, que é a auditoria (NETO, 2017).

No caso das eleições a sociedade (principal) delegou à JE (agente) a organização das eleições, que é realizada pela votação eletrônica. Assim, pode surgir uma assimetria de informações sobre o uso das urnas eletrônicas, com a JE afirmando sua confiança no sistema de votação e a sociedade levantando dúvidas sobre o uso do equipamento eletrônico. Uma das formas de reduzir essa assimetria é pela atuação de auditoria externa.

A confiança dos eleitores é um pré-requisito fundamental para uma ampla adoção da votação eletrônica. Essa confiança se origina de diversos aspectos, entre eles a garantia do correto comportamento dos sistemas. Embora não seja o mais importante do ponto de vista conceitual, ainda é considerado absolutamente necessário (PRANDINI e RAMILLI, 2012, p. 44).

No presente trabalho, serão discutidas formas de como o controle externo pode atuar na votação eletrônica, com objetivo de trazer uma asseguração de que o sistema eletrônico de votação garanta os resultados da vontade da sociedade em eleger os seus representantes.

1.1 Delimitação do tema

O presente trabalho propõe apresentar uma possível estratégia de atuação do controle externo para alcançar uma asseguração razoável dos resultados das eleições brasileiras.

1.2 Questão problema

Com base no exposto, elaborou-se a seguinte questão problema: Quais ações um órgão independente poderia realizar na votação eletrônica para assegurar que os votos dos eleitores são devidamente registrados e totalizados pela Justiça Eleitoral?

1.3 Hipóteses

São hipóteses para esta pesquisa:

- Assimetria de informações ente a Justiça Eleitoral e a sociedade;
- Existência de diretrizes internacionais que possam ser utilizadas como parâmetros para avaliar a votação eletrônica realizada no Brasil.

1.4 Objetivo geral

Analisar boas práticas internacionais relacionadas à votação eletrônica e compará-las com normas da Justiça Eleitoral brasileira, com o objetivo de colecionar tipos e técnicas de auditoria que possam ser utilizadas em auditorias externas que avaliem se o processo de votação brasileiro em urnas eletrônicas garante o devido registro e totalização dos votos dos eleitores, identificando e avaliando o risco de fraudes.

1.5 Objetivos específicos

Os objetivos específicos deste trabalho são:

- descrever boas práticas internacionais que possam fornecer subsídios em auditorias relacionadas à votação eletrônica;
- descrever processos de trabalhos da justiça eleitoral nos quais possam ser executados procedimentos de auditoria, buscando identificar e avaliar os riscos de fraude;
- relacionar métodos e ferramentas de auditoria que possam ser aplicados ao processo de votação brasileiro;
- sugerir um eventual calendário de auditorias em sintonia com o processo eleitoral brasileiro, indicando tipos de fiscalizações, como levantamentos, auditorias de conformidade ou operacionais que possam ser realizadas.

1.6 Justificativa

Antecedente: o processo eleitoral no Brasil evoluiu para o uso do voto eletrônico iniciando em 1996 o uso de urnas eletrônicas. Embora, segundo o TSE, nunca tenha sido constatada nenhuma fraude nas eleições decorrentes do voto eletrônico, os procedimentos de controle interno da Justiça Eleitoral não têm sido suficientes para que as partes interessadas tenham segurança de que os objetivos do processo eleitoral estejam sendo cumpridos. Esses objetivos consistem, em grande parte, na disponibilização de informações a partidos políticos e setores da sociedade, como OAB, MP, Universidades e pesquisadores, na realização da votação paralela e verificação do software em uma quantidade reduzida de urnas, bem como dos testes públicos de segurança.

Justificativa: o TCU tem competência constitucional para realizar auditorias visando avaliar, do ponto de vista do desempenho operacional, as atividades e os sistemas, bem como a organização e o funcionamento dos órgãos e entidades do setor público federal. Nas eleições, o Tribunal atuou basicamente em processos sobre licitações para a aquisição de urnas eletrônicas e, mais recentemente, sobre a implantação do voto impresso. Não há trabalhos do TCU sobre o acompanhamento do processo eleitoral e nem sobre a segurança no uso das urnas eletrônicas.

1.7 Estrutura

Além deste capítulo introdutório, a presente monografia é dividida em outros cinco capítulos.

O capítulo 2 apresenta o referencial teórico. Nele está exposta a revisão bibliográfica acerca dos assuntos correlacionados ao tema central. O capítulo é subdividido em seções, de modo a englobar os seguintes tópicos: votação eletrônica; diretrizes internacionais para o uso da votação eletrônica, normas brasileiras para a votação eletrônica e normas e orientações para fiscalizações.

O capítulo 3 traz a metodologia utilizada na pesquisa.

O capítulo 4 concentra a discussão dos resultados e é dividido em quatro seções. Elas tratam das possíveis fiscalizações que poderiam trazer uma asseguração razoável de que o resultado da votação eletrônica retrata a vontade dos eleitores.

Por fim, o capítulo 5 traz as considerações finais da monografia, a resposta à questãoproblema e sugestões para estudos futuros.

2. Referencial teórico

Para uma melhor compreensão do trabalho, realizou-se revisão bibliográfica acerca dos assuntos que circundam o tema principal. Foram estudados materiais sobre o direito eleitoral (devido à regulamentação da utilização da votação eletrônica e dos processos de trabalho relacionados ao tema), as normas internacionais e votação eletrônica (devido à necessidade de conhecer parâmetros que possam ser comparados com a eleição eletrônica no Brasil) e a auditoria do setor público (devido as estratégias do controle externo sobre o tema).

O presente capítulo apresenta os resultados da revisão bibliográfica e é dividido em quatro seções, as quais tratam dos seguintes temas: votação eletrônica, diretrizes internacionais para o uso da votação eletrônica, votação eletrônica no Brasil e normas e orientação sobre auditoria.

2.1 Votação eletrônica

No Glossário Eleitoral consta como voto eletrônico o voto composto e registrado em meio de armazenamento eletroeletrônico. No Brasil, este equipamento é denominado urna eletrônica, que é definido como equipamento de processamento de dados que, junto com o seu software (programas), permite a coleta de votos em uma eleição, de forma ergonômica, rápida e segura (BRASIL. TRIBUNAL SUPERIOR ELEITORAL, 2018a).

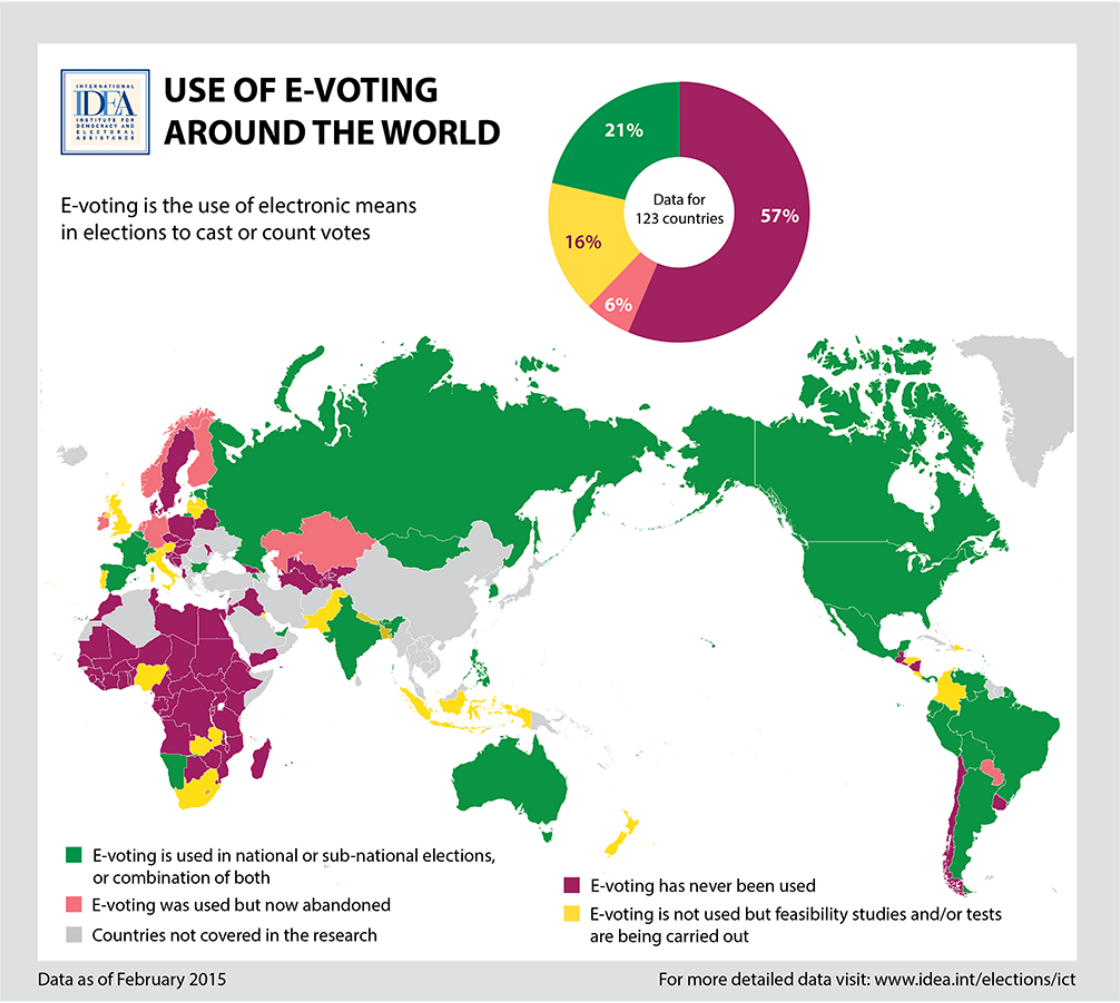
Segundo Goldsmith e Ruthrauff (2013, p. 23), em uma votação eletrônica um dispositivo eletrônico é usado pelo eleitor para fazer e gravar seu voto. O Conselho da Europa

(2017a, p. 6) define votação eletrônica como o uso de meios eletrônicos para coletar e/ou contar o voto.

A urna eletrônica utilizada no Brasil é definida como um sistema eletrônico de gravação direta (DRE). O equipamento colhe o voto do eleitor e armazena de forma eletrônica o voto na memória da urna (VAN DE GRAAF, 2018; ARANHA et Al., 2018; GOLDSMITH e RUTHRAUFF, 2013).

Segundo o Instituto Internacional para a Democracia e Apoio Eleitoral (International Institute for Democracy and Electoral Assistance – IIDEA, 2015), de 123 países pesquisados pelo instituto em 2015, 23% deles usavam o voto eletrônico em algum nível (nacional ou regional) e 16% estavam realizando estudos ou testando o sistema eletrônico (figura 1).

Figura 1 - Adoção da votação eletrônica no mundo



Fonte: IIDEA

De acordo com Goldsmith e Ruthrauff (2013, p. 210), além do Brasil, apenas Índia, Venezuela e Butão utilizam a votação eletrônica para todo eleitorado. Tal fato demonstra que a adoção do voto eletrônico ainda tem bastante espaço para evoluir em âmbito mundial.

No Brasil, a Lei n. 9.504/1997 estabelece que a votação e a totalização dos votos serão feitas por sistema eletrônico. Em 1996 foi feito o primeiro piloto com o uso de urnas eletrônicas por parte do eleitorado, de forma a fundamentar a alteração na legislação. As eleições de 2000 já foram completamente informatizadas.

2.2 Diretrizes internacionais para uso da votação eletrônica

Foram analisadas as normas mais recentes do Conselho da Europa (Coe) e do Comitê de Assistência Eleitoral dos EUA (EAC) sobre votação eletrônica. As primeiras orientações europeias para a votação eletrônica foram expedidas em 2004, sendo atualizadas em 2017. Já a normatização americana iniciou-se em 2002, sendo atualizada em 2015.

Segundo Prandini e Ramilli (2012) quanto a regulação dos sistemas de votos eletrônicos, duas potências políticas como os Estados Unidos da América (EUA) e a União Européia (EU) apresentam abordagens muito diferentes, descrevendo os procedimentos americanos definidos de baixo para cima, com controles independentes e bem detalhados sobre componentes físicos e lógicos críticos, com a segurança geral sendo devirada da soma dessas partes. Inversamente, os autores destacam que a UE não possui um conjunto real de procedimentos de certificação, tendo adotado uma recomendação que descreve os aspectos gerais a serem levados em consideração em uma votação eletrônica.

Em seu trabalho esses autores integram as duas abordagens, adotando a recomendação do CoE como uma diretriz de alto nível, útil para manter em foco qual deveria ser o objetivo final da votação eletrônica: buscar a corretude do resultado e garantir os direitos e obrigações de todos os atores envolvidos. Já os procedimentos de teste propostos pelo EAC são utilizados para fornecer a concretude necessária do lado operacional para a certificação.

2.3 Orientações do conselho da Europa sobre voto eletrônico

O Conselho da Europa[1] (Council of Europe – CoE), estabeleceu padrões intergovernamentais de voto eletrônico por meio da Recomendação CM/Rec(2017)5. A reco-

1 O Conselho da Europa (Council of Europe) atualmente tem 47 estados membros, incluindo todos os membros da União Europeia, bem como Albânia, Andorra, Armênia, Azerbajão, Bósnia e Herzegovina, Geórgia, Irlanda, Liechtenstein, República da Moldova, Mônaco, Montenegro, Noruega, Rússia, San Marino, Servia, Suíça, Macedônia, Turquia e Ucrânia.

mendação é composta por três documentos, um com os aspectos principais do voto eletrônico, outro com as diretrizes para a implementação dessas disposições e um com a exposição de motivos Os principais aspectos da votação eletrônica destacados pelo CoE (2017) na Recomendação CM/Rec(2017)5 são os seguintes:

- votação universal;
- votação equânime;
- votação livre;
- sigilo do voto;
- requerimentos regulatórios e organizacionais;
- transparência e observação;
- accountability;
- confiabilidade e segurança do sistema.

As diretrizes relacionadas à votação universal, equânime e livre são princípios já difundidos nas normas eleitorais brasileiras. Dessa forma, consideramos desnecessário adentrar na descrição no presente trabalho.

Sobre sigilo do voto, o CoE (2017c, p. 10) estabelece que a votação eletrônica será organizada de modo a garantir que o segredo do voto seja respeitado em todas as fases do processo da eleição. Além de serem criptografados, os votos devem ser misturados na urna eletrônica de forma que a ordem em que eles foram contados não coincida com a ordem de votação dos eleitores.

Nos casos em que as informações dos eleitores e os votos sejam mantidos em um mesmo equipamento orienta-se que os dados tenham criptografia de ponta a ponta (CONSELHO DA EUROPA, 2017c, p. 10). Esse é o caso das urnas eletrônicas utilizadas nas eleições no Brasil, em que na mesma urna ficam os votos e o registro dos eleitores.

Sobressai a orientação de que a urna deve proteger os dados, para que terceiros não possam usar indevidamente, interceptar, modificar ou obter conhecimento sobre essas informações (CONSELHO DA EUROPA, 2017c, p. 10). O voto não pode ser violado, essa orientação norteia a necessidade de adotar mecanismos para evitar fraudes.

Os votos armazenados ou comunicados pelo sistema de votação eletrônica somente podem ser acessados por partes autorizadas (CONSELHO DA EUROPA, 2017c, p. 10).

Deve haver restrições ao acesso físico e lógico às urnas eletrônicas, não é apropriado o livre acesso ao equipamento.

Um sistema de voto eletrônico não deve fornecer ao eleitor a prova do conteúdo do voto emitido. Isso evita a violação do sigilo de votos, bem como a venda de votos ou o uso por terceiros. Todavia a verificabilidade individual pode ser implementada desde que existam salvaguardas adequadas para prevenir a coerção ou a compra de votos (CONSELHO DA EUROPA, 2017c, p. 11). O eleitor deve ter certeza de que a urna eletrônica registrou sua escolha, mas não é desejável que receba comprovante que possa provar a escolha do seu voto. A existência de provas do voto pode levar a práticas fraudulentas como o oferecimento de vantagens financeiras em contrapartida ao comprovante do voto ou a coação para que seja apresentado a prova das escolhas do voto.

Quanto aos requerimentos regulatórios e organizacionais, o CoE (2017c, p. 12) orienta que as tecnologias relacionadas à votação eletrônica sejam introduzidas de forma gradual e testadas sob condições realistas. Essa orientação pode mitigar riscos de se adotar uma tecnologia de forma massiva, que após uma eleição se mostre inadequada. A adoção de tecnologias deve ser gradual e devidamente testada antes da sua adoção em massa.

Na parte de transparência a votação eletrônica deve ser introduzida quando os eleitores tiverem confiança no sistema, devendo ser buscada a continuidade da confiança ao longo do tempo. A possibilidade de verificar se a votação eletrônica está sendo efetiva deve ser garantida. Além disso a transparência pode ser obtida com a divulgação dos procedimentos de votação (CONSELHO DA EUROPA, 2017c, p. 13).

Os componentes do sistema de voto eletrônico devem ser disponibilizados para fins de verificação e certificação. A avaliação de que os sistemas de votação eletrônica funcionam corretamente e que há a manutenção da segurança é essencial. O meio para conseguir isso é a avaliação independente ou certificação do sistema como um todo ou de seus componentes. A avaliação pode ser realizada, por exemplo, divulgando o projeto do sistema, permitindo a inspeção dos detalhes da documentação, divulgando o código-fonte, permitindo a inspeção de componentes, de relatórios de certificação, bem como por testes aprofundados de segurança (CONSELHO DA EUROPA, 2017c, p. 14).

As normas de auditoria da Intosai conceituam a *accountability*[2] pública como a obrigação que as pessoas ou entidades têm, às quais se tenham confiado recursos, incluídas as

2 O termo *accountability*, que não possui tradução precisa para o nosso idioma, representa, segundo definição extraída do Manual de Auditoria Integrada do Escritório do Auditor-Geral do Canadá, a obrigação de responder por uma responsabilidade outorgada. Pressupõe a existência de pelo menos duas partes: uma que delega a responsabilidade e outra que a aceita, mediante o compromisso de prestar contas sobre como essa responsabilidade foi cumprida. O termo sintetiza a preservação dos interesses dos cidadãos por meio da transparência, responsabilização e prestação de contas pela administração pública.

empresas e corporações públicas, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a quem lhes delegou essas responsabilidades. Há a obrigação imposta à entidade auditada de demonstrar que administrou ou controlou os recursos que lhe foram confiados em conformidade com os termos da atividade designada (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2011).

Quanto à *accountability*, o CoE (2017c, p. 15) destaca que deverão ser desenvolvidos requisitos técnicos, de avaliação e certificação que reflitam os princípios legais e democráticos relevantes associados à votação eletrônica. Enfatiza que o órgão responsável pela eleição deve desenvolver requisitos para os sistemas de votação eletrônica, bem como para avaliações técnicas que vão desde testes até a certificação formal de sistemas de votação eletrônica. Essas condições visam garantir que o sistema foi concebido em conformidade com uma eleição democrática e que ele opera corretamente, ou seja, faz exatamente o que é suposto fazer. Esses requisitos devem manter-se atualizados ao longo do tempo.

Os sistemas de votação eletrônica devem ser avaliados periodicamente e, em especial, após quaisquer alterações significativas, por organismo independente e competente que verificaria a conformidade do sistema de votação eletrônica e de qualquer tecnologia de informação e comunicação com os requisitos técnicos. Isto pode assumir a forma de certificação formal ou outro controle apropriado. A existência de controles adequados fornece provas quanto à compatibilidade do sistema com requisitos técnicos. O valor agregado de tal controle não é apenas assegurar que um sistema de votação eletrônica esteja em conformidade com os requisitos e padrões, mas também seja uma ferramenta importante no estabelecimento da confiança na votação eletrônico (CONSELHO DA EUROPA, 2017c, p. 15).

A noção de um corpo independente abrange tanto a independência do fabricante do sistema ou do prestador do serviço, quanto a ausência de interferência política. A verificação supra pode ser aplicada de diferentes maneiras, podendo certificar todo o sistema ou apenas componentes do mesmo, tendo em conta a necessidade de assegurar que o sistema e os procedimentos eleitorais possam responder a possíveis ameaças e riscos e respeitar os padrões para uma eleição democrática (CONSELHO DA EUROPA, 2017c, p. 15, 16). No caso brasileiro, o TSE atua desenvolvendo o software e especificando o hardware para a fabricação das urnas eletrônicas por terceiros, ou seja, o órgão eleitoral controla etapas cruciais para o funcionamento dos equipamentos.

O CoE (2017c, p. 16) destaca que a votação eletrônica deva ser auditável. A auditoria deve ser aberta e abrangente, informando ativamente sobre possíveis problemas e ameaças. A fiscalização do processo de votação eletrônica, recursos ou infraestrutura é um meio para estabelecer confiança nas eleições. A fiscalização deve verificar a integridade e autenticidade das informações dos sistemas implantados, visando detectar possíveis ataques aos sistemas. Procedimentos independentes e extensivos

de monitoramento de segurança, auditoria, verificação cruzada e relatórios são uma parte crítica dos sistemas de votação eletrônica. Esses sistemas devem, portanto, ter pontos de verificação em cada um dos componentes principais (votação, contagem, etc.) e em diferentes níveis do sistema: lógico, aplicação, técnico.

Os pontos de auditoria no nível lógico devem informar sobre o uso que está sendo feito do sistema. Os pontos de auditoria no nível de aplicativo devem fornecer informações sobre as atividades que o sistema suporta para permitir a reconstrução das operações. Pontos de auditoria no nível técnico devem fornecer informações sobre as atividades que a infraestrutura que está sendo usada suporta. Isso varia de informações de rotina sobre, por exemplo, informações de carga específicas e mau funcionamento do sistema, até informações específicas sobre os sinais de possíveis ataques ao sistema (CONSELHO DA EUROPA, 2017c, p. 16). Do ponto de vista lógico é importante que a urna eletrônica gere arquivos de log com os eventos mencionados acima, de forma que se possa rastrear as intervenções realizadas no equipamento ao longo do período eleitoral.

As trilhas de auditoria são críticas para os sistemas de voto eletrônico, portanto, devem ser abrangentes e abertas ao exame de terceiros autorizados, sendo que as informações auditadas devem ser fornecidas em vários pontos e níveis dentro de um sistema de votação eletrônica. Deve haver procedimentos processuais especificados para o uso de sistemas de auditoria enquanto eleições estão em andamento e procedimentos predeterminados para cenários de resposta rápida (CONSELHO DA EUROPA, 2017c, p. 16).

O sistema de auditoria deve ser capaz de detectar fraude de eleitores e fornecer provas de que todos os votos contados são autênticos. Todas as ocorrências de tentativas de fraude de eleitores devem ser registradas; os registros do sistema de auditoria devem conter dados que possibilitem a verificação cruzada do título de eleitor e garantam que todos os votos contados sejam dados por um eleitor com direito a fazê-lo e que todos os votos autênticos tenham sido contados como tal (CONSELHO DA EUROPA, 2017c, p. 17).

O cruzamento de dados na auditoria independente aumenta a probabilidade de detecção de ataques a sistemas de votação eletrônica. O ataque teria que ser escondido de forma consistente tanto no sistema de votação utilizado pelo órgão eleitoral quanto nas informações coletadas pela auditoria independente (CONSELHO DA EUROPA, 2017c, p. 17). A orientação reforça o papel da auditoria independente, que em sua atuação dificulta a materialização de fraudes, que teriam de burlar os controles internos e a atuação do controle externo.

O sistema de auditoria deve ser protegido contra ataques destinados ou susceptíveis de corromper, alterar ou levar à perda de registros. A detecção de quaisquer ataques internos ou externos no sistema de auditoria deve ser relatada e medidas devem ser adotadas imediatamente (CONSELHO DA EUROPA, 2017c, p. 17).

Quanto à confiabilidade e segurança do sistema, o CoE destaca que além de estar disponível e utilizável, o sistema de votação eletrônica precisa ser confiável e seguro para cumprir os princípios de uma eleição democrática. O sistema de votação eletrônica deve ser seguro, ou seja, robusto para resistir a ataques deliberados, bem como confiável, devendo haver contingências que garantam a realização das eleições independentemente de deficiências no *hardware* ou *software* das urnas eletrônicas (CONSELHO DA EUROPA, 2017c, p. 17).

Apenas pessoas autorizadas pelo órgão de administração eleitoral devem ter acesso à infraestrutura central, aos servidores e aos dados eleitorais. Qualquer intervenção em *hardware* ou *software* acarreta riscos técnicos e humanos intrínsecos, que devem ser mantidos ao mínimo enquanto uma eleição está em andamento. É por isso que os controles automáticos devem ser preferidos. Se houver necessidade de intervir, os riscos de invasão, erro humano, sabotagem, devem ser reduzidos ao máximo possível. Isso deve ser feito através do estabelecimento de um procedimento de trabalho a ser seguido e validado, restringindo o número de pessoas autorizadas a realizar o trabalho a um pequeno grupo supervisionado e requer a verificação de cada ato através da presença física de duas ou mais pessoas qualificadas. Essas pessoas devem cumprir as regras de segurança estabelecidas pela autoridade competente (CONSELHO DA EUROPA, 2017c, p. 17).

Se armazenados ou transmitidos para fora de ambientes controlados, os votos devem ser criptografados. A partir do momento em que voto é coletado, ninguém deve ser capaz de alterálo ou vinculá-lo ao eleitor que o emitiu (CONSELHO DA EUROPA, 2017c, p. 18)

O CoE (2017c, p. 18) destaca que os incidentes que ameaçam a integridade do sistema devam ser imediatamente comunicados ao órgão eleitoral. Deve ser assegurada a adoção das medidas necessárias e que todos os interessados, como partidos políticos e eleitores, sejam devidamente informados.

2.4 Normas do comitê de assistência eleitoral dos EUA sobre voto eletrônico

O Comitê de Assistência Eleitoral dos EUA (U.S. *Election Assistance Commission* EAC) também edita normas sobre voto eletrônico que orientam os estados americanos. As Diretrizes do Sistema de Votação Voluntária (*Voluntary Voting System Guidelines* - VVSG) são um conjunto de especificações e requisitos com base nos quais os sistemas de votação podem ser testados para determinar se atendem aos padrões daquele país.

As VVSG dividem-se em dois volumes. O Volume I descreve os requisitos para os componentes eletrônicos dos sistemas de votação. O Volume II fornece uma visão geral e detalhes específicos do processo de teste de certificação, que no caso dos Estados Unidos é realizado por entidades acreditadas.

O Volume II das VVSG é um documento complementar ao Volume I. Este especifica os requisitos aos quais um sistema de votação deve obedecer para ser nacionalmente certificado como aceitável para uso em eleições federais americanas. Aquele descreve o processo de testes que devem ser realizados para fornecer uma verificação independente, que deve ser documentada por um laboratório de ensaios do sistema de votação acreditado, para atestar que o sistema está em conformidade com os requisitos do Volume I e, portanto, podendo receber a certificação americana (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015b). Dessa forma, o Volume I traz os requisitos e o Volume II, os testes que devem ser realizados para certificar que aqueles requisitos foram adotados.

A finalidade das VVSG é fornecer um conjunto de especificações e requisitos com base nos quais os sistemas de votação podem ser testados para determinar se eles fornecem todos os recursos básicos de funcionalidade, acessibilidade e segurança exigidos dos sistemas de votação. Esses requisitos e especificações são descritos para que possam ser avaliados por meio de testes objetivos no *hardware* e *software* utilizados em uma votação eletrônica (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a).

Ambos volumes são divididos em oito seções, que tratam de introdução às diretrizes de desempenho do sistema de votação; requisitos funcionais; requisitos de usabilidade, acessibilidade e privacidade; requisitos de *hardware*; requisitos de *software*; requisitos de telecomunicações; requisitos de segurança; e asseguração de qualidade e gerenciamento de configurações (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a).

Embora não seja possível identificar todos os riscos potenciais, o Volume I identifica vários tipos de riscos que devem ser abordados, que incluem (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a):

- mudanças não autorizadas no sistema de votação eletrônica que possam alterar:
  - a interface de votação;
  - a coleta e gravação de votos;
  - o cálculo dos totais de votos e o a emissão de relatórios de totalização dos votos;
- alteração de trilhas de auditoria do sistema de votação;
- impedimento de gravação de votos;
- introdução de dados que representem votos não coletados por um eleitor;

- acesso indevido a dados de voto - incluindo votos individuais e totais - por pessoas não autorizadas

- acesso indevido aos dados de identificação dos eleitores e dos votos, de tal forma que um indivíduo possa determinar o conteúdo de votos específicos.

A introdução às diretrizes de desempenho do sistema destaca a evolução dos sistemas, definições, referências e tipos de sistemas, bem como descreve como as VVSG devem ser aplicadas (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a). Essa seção esclarece os propósitos e aplicação da VVSG.

Nos requisitos funcionais, são detalhados os recursos funcionais exigidos de um sistema de votação. A seção define o que o sistema deve ser capaz de realizar. A segurança do sistema é conseguida com uma combinação de recursos técnicos e práticas administrativas sólidas (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a).

São descritos o contexto e o propósito das auditorias do sistema de votação, estabelecendo requisitos funcionais. Segundo o EAC (2015a) as trilhas de auditoria eleitoral na forma de *log* fornecem informação de apoio para verificar a exatidão dos resultados eleitorais reportados. Elas devem apresentar registro concreto de todas as atividades do sistema relacionadas à contagem de votos e são essenciais para a confiança do público na exatidão do pleito. Os requisitos baseiam-se na premissa de que o sistema deva gerar os registros de auditoria, o que reduz a chance de erro associada aos registros de auditoria gerados manualmente. Como a maioria dos registros é automática, é menos provável a presença de erros ou omissões humanas.

Os objetivos dos requisitos de usabilidade, acessibilidade e privacidade são para garantir que os eleitores possam usar o sistema de votação de maneira confortável, eficiente e com a confiança de que eles tenham votado corretamente. Visam garantir que todos os eleitores tenham acesso à votação eletrônica sem discriminação, que as urnas eletrônicas capturem cada voto dos eleitores de forma confiável e que seja preservado o sigilo do voto (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a).

Os requisitos de *hardware* são especificados para os equipamentos que fazem parte de um sistema de votação, como a urna eletrônica. Além dos requisitos, devem ser especificados critérios mínimos para características de desempenho, físicas, e de desenho, bem como de construção e manutenção para o *hardware* e componentes relacionados selecionados de todos os sistemas de votação (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a).

Os requisitos de *software* destinam-se a garantir que a lógica do sistema de votação seja confiável, robusta, testável e passível de manutenção (*U.S. ELECTION*

ASSISTANCE COMMISSION, 2015a). Nesses requisitos são descritas as características essenciais de projeto e o desempenho da lógica usada nos sistemas de votação.

Quanto aos requisitos de telecomunicações, devem ser definidos níveis aceitáveis de desempenho para a combinação de telecomunicações, *hardware* e *software* relacionados à transmissão de dados que são usados para operar o sistema e gerar os resultados eleitorais. Não se aplica a outros meios de movimentação de dados como informações impressas ou a mídia de memórias físicas (*U.S. ELECTION ASSISTANCE COMMISSION*, 2015a).

Os requisitos de segurança descrevem os recursos de segurança essenciais para um sistema de votação, abrangendo o *hardware*, o *software*, as comunicações e a documentação do sistema. O EAC (2015a) destaca que nenhum conjunto predefinido de padrões de segurança abordará e inibirá todas as ameaças concebíveis ou teóricas da votação eletrônica. Entretanto as diretrizes articulam os requisitos necessários para atingir níveis aceitáveis de integridade e confiabilidade. Elencam-se os seguintes objetivos para a norma de segurança:

- proteger elementos críticos do sistema de votação eletrônica;
- estabelecer e manter controles para minimizar erros;
- proteger o sistema da manipulação intencional e fraude;
- identificar alterações fraudulentas ou erradas no sistema de votação;
- proteger o sigilo no processo de votação.

Por fim, os requisitos de asseguração de qualidade e gerenciamento de configuração ajudam a garantir que os sistemas de votação estejam em conformidade com os requisitos do VVSG. Segundo o EAC, a asseguração de qualidade se concentra na garantia do bom funcionamento de um sistema e na redução da dependência de testes no final do ciclo de vida, para detectar deficiências. Já o gerenciamento de configuração é um conjunto de atividades e práticas associadas que garantem o conhecimento e o controle dos componentes de um sistema, começando com seu desenvolvimento inicial, progredindo através de sua manutenção e aprimoramento contínuos, durante seu ciclo de vida operacional.

2.5 Normas brasileiras para a votação eletrônica

O Código Eleitoral Anotado destaca que o processo eleitoral no Brasil ocorre a cada dois anos, com o primeiro turno ocorrendo no primeiro domingo de outubro e o se-

gundo turno no último domingo daquele mês de acordo com a Constituição Federal. Sucedem-se os pleitos que definem Presidente e Vice-Presidente da República; Senadores; Deputados Federais; Governadores e Vice-Governadores de Estado e do Distrito Federal e Deputados Estaduais e Distritais, com a realização das eleições em que são eleitos os Prefeitos e Vice-Prefeitos de Município e Vereadores. Nessas últimas não há votação no Distrito Federal e nas seções eleitorais localizadas no exterior, bem como não há voto em Trânsito (BRASIL. TRIBUNAL SUPERIOR ELEITORAL, 2018b).

Quando, na eleição, um candidato a Presidente da República ou Governador consegue a maioria absoluta dos votos, descartados os votos brancos e nulos, ele é eleito já no primeiro turno, caso não consiga a maioria, os dois candidatos mais votados disputam o segundo turno. O mesmo acontece para os candidatos a prefeito em municípios com mais de 200.000 eleitores.

A Lei n. 9.504/1997 estabelece normas para as eleições. Em seu art. 59 estabelece-se que a votação e a totalização dos votos serão feitas por sistema eletrônico. No § 4º desse artigo é definido o registro digital do voto (RDV) e o boletim de urna (BU).

O RDV traz uma tabela com cada um dos votos gravados de forma aleatória. Já o BU traz informações resumidas sobre a votação na seção eleitoral, como a quantidade de votos que cada candidato recebeu na urna e é utilizado na totalização dos votos da eleição.

O art. 66 da lei define que os partidos políticos e as coligações poderão realizar a fiscalização das fases do processo de votação e apuração das eleições e o processamento eletrônico da totalização do resultado, conforme definido nos parágrafos abaixo:

> § 1º Todos os programas de computador de propriedade do Tribunal Superior Eleitoral, desenvolvidos por ele ou sob sua encomenda, utilizados nas urnas eletrônicas para os processos de votação, apuração e totalização, **poderão ter suas fases de especificação e de desenvolvimento acompanhadas por técnicos** indicados pelos partidos políticos, Ordem dos Advogados do Brasil e Ministério Público, até seis meses antes das eleições.
>
> § 2º Uma vez concluídos os programas a que se refere o § 1º, **serão eles apresentados, para análise**, aos representantes credenciados dos partidos políticos e coligações, **até vinte dias antes das eleições, nas dependências do Tribunal Superior Eleitoral, na forma de programas-fonte e de programas executáveis, inclusive os sistemas aplicativo e de segurança e as bibliotecas especiais**, sendo que as chaves eletrônicas privadas e senhas eletrônicas de acesso manter-se-ão no sigilo da Justiça Eleitoral. **Após a apresentação e conferência, serão lacradas cópias dos programas-fonte e dos programas compilados**.

(...)

§ 5º **A carga ou preparação das urnas eletrônicas será feita em sessão pública**, com prévia convocação dos fiscais dos partidos e coligações para a assistirem e procederem aos atos de fiscalização, inclusive para **verificarem se os programas carregados nas urnas são idênticos aos que foram lacrados** na sessão referida no § 2º deste artigo, após o que as urnas serão lacradas.

§ 6º **No dia da eleição, será realizada**, por amostragem, auditoria de verificação do funcionamento das urnas eletrônicas, através de **votação paralela**, na presença dos fiscais dos partidos e coligações, nos moldes fixados em resolução do Tribunal Superior Eleitoral.

§ 7º **Os partidos concorrentes ao pleito poderão constituir sistema próprio de fiscalização, apuração e totalização dos resultados** contratando, inclusive, empresas de auditoria de sistemas, que, credenciadas junto à Justiça Eleitoral, receberão, previamente, os programas de computador e os mesmos dados alimentadores do sistema oficial de apuração e totalização. (BRASIL XXX, grifos nossos)

Observa-se, da leitura desse artigo, que a lei define que a fiscalização das eleições deveria ser realizada em sua maior parte pelos partidos políticos, com a participação da Ordem dos Advogados do Brasil (OAB) e do Ministério Público (MP). A Resolução-TSE n. 23.555/2017 fixa o calendário eleitoral. Das datas trazidas pela norma destacamos as relacionadas com a fiscalização e a segurança das urnas (tabela 1):

Tabela 1 - Calendário eleitoral 2018

Data	Evento
28/11/2017 a 1/12/2017	Realização, no TSE, dos testes públicos de segurança (TPS) no sistema eletrônico de votação.
12/12/2017	Divulgação do resultado dos TPS no sistema eletrônico de votação.
5/3/2019	Os partidos políticos, as coligações, a OAB o MP, o Congresso Nacional, o STF, a CGU, o DPF, a Sociedade Brasileira de Computação, o CREA, os departamentos de Tecnologia da Informação de universidades poderão acompanhar as fases de especificação e de desenvolvimento dos sistemas relacionados à votação eletrônica.

9/7/2018 (90 dias antes do 1º turno)	Último dia para os representantes dos partidos políticos, da OAB, do MP e as demais pessoas autorizadas em resolução específica, interessados em assinar digitalmente os programas a serem utilizados nas eleições, entregarem à Secretaria de Tecnologia da Informação (STI) do TSE programa próprio, para análise e posterior homologação.
3/9/2018	Último dia para o TSE convocar os partidos políticos, as coligações, a OAB, o MP e as pessoas autorizadas em resolução específica para a Cerimônia de Assinatura Digital e Lacração dos Sistemas a serem utilizados nas Eleições 2018
7/9/2018 (30 dias antes do 1º turno)	Último dia para os TRE designarem, em sessão pública, a Comissão de Auditoria da Votação Eletrônica.
10/9/2018	Último dia para os representantes das entidades informarem à STI o interesse em assinar digitalmente os programas.
17/9/2018 (20 dias antes do 1º turno)	Último dia para o TSE compilar, assinar digitalmente, gerar os resumos digitais (*hash*) e lacrar todos os programas-fonte, programas-executáveis, arquivos fixos, arquivos de assinatura digital e chaves públicas em cerimônia marcada para essa finalidade.
2/10/2018 (5 dias antes do 1º turno)	Último dia para que os representantes dos partidos políticos e das coligações, da OAB, do MP e as pessoas autorizadas em resolução específica formalizem pedido ao juízo eleitoral para a verificação das assinaturas digitais do Sistema de Transporte de Arquivos da Urna Eletrônica, do Subsistema de Instalação e Segurança e da Solução JE-Connect instalados nos equipamentos da Justiça Eleitoral.
5/10/2018 (2 dias antes do 1º turno)	Data a partir da qual, desde 8 até as 17 horas do dia da eleição, poderá ser realizada a verificação da assinatura digital e dos resumos digitais (hash) do Sistema de Transporte de Arquivos da Urna Eletrônica, do Subsistema de Instalação e Segurança e da Solução JE-Connect instalados nos equipamentos da Justiça Eleitoral, observada a antecedência de 5 (cinco) dias para o requerimento.

6/10/2018 (1 dia antes do 1º turno)	Data em que a Comissão de Auditoria da Votação Eletrônica deverá promover, entre as 9 e as 12 horas, em local e horário previamente divulgados, os sorteios das seções eleitorais cujas urnas serão submetidas aos procedimentos de auditoria da votação eletrônica. Último dia para o TSE tornar disponível, na sua página da internet, arquivo contendo as correspondências esperadas entre urna e seção, podendo ser atualizada até as 16 horas do dia da eleição. Data em que será realizada, no TSE, a verificação dos Sistemas de Gerenciamento, Preparação e Receptor de Arquivos da Urna.
7/10/2018 – Dia do 1º turno A partir das 7 h	Realização dos procedimentos, por amostragem, de auditoria do funcionamento das urnas eletrônicas no dia da votação por meio da verificação da autenticidade e integridade dos sistemas, a partir das 7 horas e antes da emissão da zerésima da urna, nas dependências da seção eleitoral. Data Evento Realização dos procedimentos, por amostragem, de auditoria da votação eletrônica sob condições normais de uso, das 8 às 17 horas, em cada unidade da Federação, em um só local, público e com expressiva circulação de pessoas, designado pelo respectivo TRE. Emissão do Relatório Zerésima da urna eletrônica instalada na seção eleitoral.
7/10/2018 – Dia do 1º turno A partir das 17 h	Emissão dos BU e transmissão desse arquivo e do log das urnas eletrônicas aos TRE.
8/10/2018 (1 dia após o 1º turno)	Último dia para os TRE informarem, em edital e mediante divulgação nos respectivos sítios na internet, o local onde será realizada a auditoria da votação eletrônica relativa ao segundo turno.
10/10/2018 (3 dias após o 1º turno)	Último dia para a Justiça Eleitoral tornar disponível, em sua página na internet, opção de visualização dos boletins de urna recebidos para a totalização, assim como as tabelas de correspondências efetivadas, observado o horário de encerramento da totalização em cada unidade da Federação.

22/10/2018 (5 dias antes do 2º turno)	Último dia para que os representantes dos partidos políticos e das coligações, da OAB, do MP e as pessoas autorizadas em resolução específica formalizem pedido ao juízo eleitoral para a verificação das assinaturas digitais do Sistema de Transporte de Arquivos da Urna Eletrônica, do Subsistema de Instalação e Segurança e da Solução JE-Connect instalados nos equipamentos da Justiça Eleitoral a serem utilizados no segundo turno
26/10/2018 (2 dias antes do 2º turno)	Data a partir da qual, desde 8 até as 17 horas do dia da eleição, poderá ser realizada a verificação da assinatura digital e dos resumos digitais (hash) do Sistema de Transporte de Arquivos da Urna Eletrônica, do Subsistema de Instalação e Segurança e da Solução JE-Connect instalados nos equipamentos da Justiça Eleitoral, observada a antecedência de 5 (cinco) dias para o requerimento.
27/10/2018 (1 dia antes do 2º turno)	Data em que a Comissão de Auditoria da Votação Eletrônica deverá promover, entre as 9 e as 12 horas, em local e horário previamente divulgados, os sorteios das seções eleitorais cujas urnas serão submetidas aos procedimentos de auditoria da votação eletrônica. Último dia para o TSE tornar disponível, na sua página da internet, arquivo contendo as correspondências esperadas entre urna e seção, podendo ser atualizada até as 16 horas do dia da eleição. Data em que será realizada, no TSE, a verificação dos Sistemas de Gerenciamento, Preparação e Receptor de Arquivos da Urna.
28/10/2018 – Dia do 1º turno A partir das 7 h	Realização dos procedimentos, por amostragem, de auditoria do funcionamento das urnas eletrônicas no dia da votação por meio da verificação da autenticidade e integridade dos sistemas, a partir das 7 horas e antes da emissão da zerésima da urna, nas dependências da seção eleitoral. Realização dos procedimentos, por amostragem, de auditoria da votação eletrônica sob condições normais de uso, das 8 às 17 horas, em cada unidade da Federação, em um só local, público e com expressiva circulação de pessoas, designado pelo respectivo TRE. Emissão do Relatório Zerésima da urna eletrônica instalada na seção eleitoral.

28/10/2018 – Dia do 1º turno A partir das 17 h	Emissão dos BU.
31/10/2018 (3 dias após o 2º turno)	Último dia para a Justiça Eleitoral tornar disponível, em sua página na internet, opção de visualização dos boletins de urna recebidos para a totalização, assim como as tabelas de correspondências efetivadas, observado o horário de encerramento da totalização em cada unidade da Federação.
6/11/2018 (30 dias após o 1º turno)	Data-limite para a publicação, na página da internet do TSE, do relatório conclusivo sobre a fiscalização realizada na auditoria da votação eletrônica no primeiro turno elaborado pela empresa de auditoria.
27/11/2018 (30 dias após o 2º turno)	Data-limite para a publicação, na página da internet do TSE, do relatório conclusivo sobre a fiscalização realizada na auditoria da votação eletrônica no primeiro turno elaborado pela empresa de auditoria.
19/12/2018	Último dia para a diplomação dos eleitos.
12/1/2019	Último dia para os representantes dos partidos políticos, da OAB, do MP e as demais pessoas autorizadas em resolução específica, interessados em realizar a verificação pós-pleito das assinaturas digitais do Sistema de Transporte de Arquivos da Urna Eletrônica, do Subsistema de Instalação e Segurança, da Solução JE-Connect, do Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica, Sistema de Preparação, Sistema de Gerenciamento, Infoarquivos, Receptor de Arquivos de Urna, e dos sistemas de urna eletrônica, instalados nos equipamentos da Justiça Eleitoral, formalizarem o pedido ao juiz eleitoral, TRE ou ao TSE, de acordo com o local de sua utilização, desde que sejam relatados fatos e apresentados indícios e circunstâncias que a justifique.

17/1/2018	Último dia para os partidos políticos, as coligações, MP e a OAB solicitarem aos TRE as seguintes cópias dos arquivos e informações: a) log do Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica; b) log do Sistema de Gerenciamento; c) imagem dos BU; d) log das urnas; e) RDV; f) ocorrências de substituição de urnas; e g) relatório dos boletins de urna que estiveram em pendência, sua motivação e respectiva decisão. Último dia para a verificação da assinatura digital e dos resumos digitais (*hash*) dos sistemas eleitorais e de urna, realizada após o pleito.
18/1/2018	Data a partir da qual poderão ser retirados das urnas os lacres e os cartões de memória de carga, desde que as informações neles contidas não sejam objeto de discussão em processo judicial, sendo permitidos os seguintes procedimentos: I — a remoção dos lacres das urnas eletrônicas; II — a retirada e a formatação das mídias de votação; III — a formatação das mídias de carga; IV — a formatação das mídias de resultado da votação; V — a manutenção das urnas eletrônicas. Data a partir da qual os sistemas utilizados nas eleições de 2018 poderão ser desinstalados, desde que os procedimentos a eles inerentes não sejam objeto de discussão em processo judicial. Data a partir da qual não há mais necessidade de preservação e guarda dos documentos e materiais produzidos nas eleições de 2018, dos meios de armazenamento de dados utilizados pelos sistemas eleitorais, bem como das cópias de segurança dos dados, desde que as informações neles contidas não sejam objeto de discussão em processo judicial.

Fonte: Resolução-TSE n. 23.550/2017 e 23.555/2017

A Resolução-TSE 23.550/2017 dispõe sobre a cerimônia de assinatura digital e A fiscalização do sistema eletrônico de votação, do registro digital do voto, das auditorias de funcionamento das urnas eletrônicas e dos procedimentos de segurança dos dados dos sistemas eleitorais. A norma traz controles internos executados pelo TSE e pelos TRE para garantir a segurança da votação eletrônica.

O art. 1º elenca os seguintes legitimados para ter acesso antecipado aos programas de computador, desenvolvidos pelo TSE ou sob sua encomenda, a serem utilizados nas eleições, para fins de fiscalização e auditoria, em ambiente específico e sob a supervisão do órgão, conforme a lista que se segue:

- Fiscais dos partidos políticos e das coligações;
- Ordem dos Advogados do Brasil (OAB);
- Ministério Público (MP);
- Congresso Nacional;
- Supremo Tribunal Federal (STF);
- Controladoria-Geral da União (CGU);
- Departamento de Polícia Federal (DPF);
- Sociedade Brasileira de Computação (SBC);
- Conselho Federal de Engenharia e Agronomia (Confea);
- Departamentos de Tecnologia da Informação de universidades.

O TSE estabelece que serão fiscalizados, auditados, assinados digitalmente, lacrados e verificados todos os sistemas e programas, listando-os:

- Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica;
- Preparação;
- Gerenciamento;
- Transporte de Arquivos da Urna Eletrônica;
- Informação de Arquivos de Urna - InfoArquivos;

- JE-Connect;
- Receptor de Arquivos de Urna;
- Votação, Justificativa Eleitoral, Apuração da Urna Eletrônica e demais aplicativos;
- Sistemas operacional e de segurança da urna;
- Bibliotecas-padrão e especiais;
- Programas de criptografia, inseridos nos programas utilizados nos sistemas de coleta, totalização e transmissão dos votos; e
- Programas utilizados para compilação dos códigos-fonte de todos os programas desenvolvidos e utilizados no processo eleitoral.

A partir de seis meses antes do primeiro turno, os representantes daquelas entidades poderão acompanhar a especificação e o desenvolvimento desses sistemas. Esse acompanhamento será realizado no TSE, em ambiente controlado, sem acesso à internet, sendo vedado portar qualquer dispositivo que permita o registro ou a gravação de áudio ou imagem, bem como retirar, sem a expressa autorização da Secretaria de Tecnologia da Informação (STI), qualquer elemento ou fragmento dos sistemas ou programas elaborados ou em elaboração.

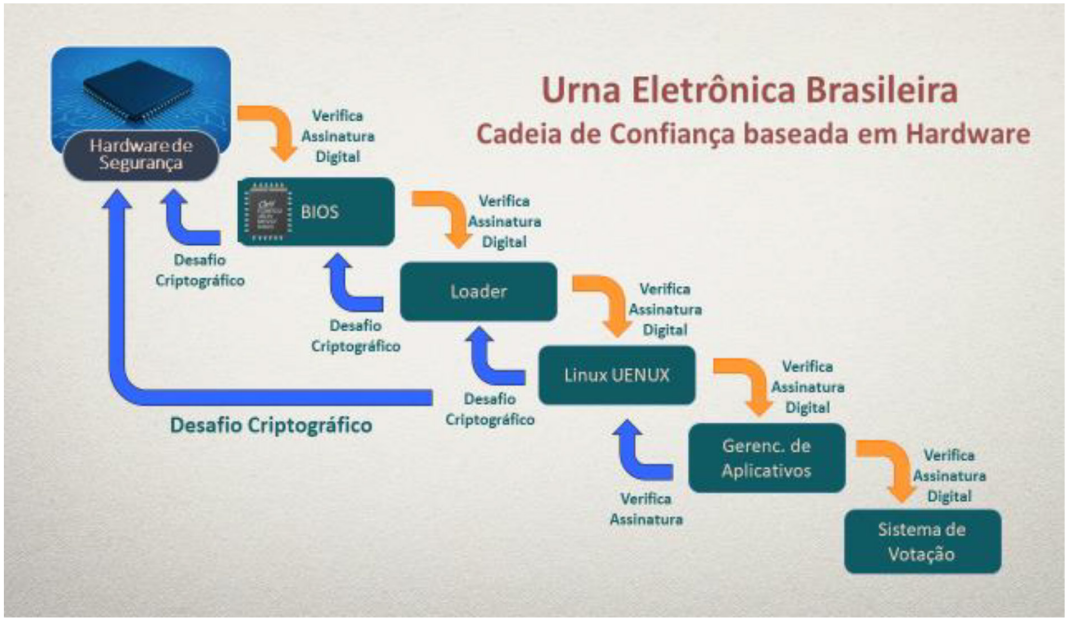
Os programas disponibilizados para verificação, após concluídos, serão apresentados, compilados e assinados digitalmente pelo TSE em Cerimônia de Assinatura Digital e Lacração dos Sistemas. Durante a cerimônia, que terá duração mínima de três dias, esses programas ficarão disponíveis para análises daquelas entidades. Após os procedimentos de compilação e assinatura digital, serão calculados os resumos digitais (hash) de todos os programas-fonte, programas-executáveis, arquivos fixos dos sistemas, arquivos de assinatura digital e chaves públicas.

As entidades e instituições credenciadas poderão utilizar programas de análise de códigos para a análise estática do *software*. É necessário que sejam programas de conhecimento público e normalmente comercializados ou disponíveis no mercado para proceder à fiscalização e à auditoria na fase de especificação e de desenvolvimento, assim como na Cerimônia de Assinatura Digital e Lacração dos Sistemas. A norma também estabelece que as ferramentas e o uso têm de ser aprovados previamente pela STI.

As assinaturas digitais e os hash dos aplicativos compõem a cadeia de segurança das urnas eletrônicas. Durante o uso as urnas eletrônicas executam diversos testes para verificar se os programas que estão sendo executados são aqueles que compilados

e assinados digitalmente pelo TSE. O objetivo dessa cadeia de segurança é reduzir o risco de execução de aplicativos estranhos ao ecossistema da urna (figura 2).

Figura 2 – Cadeia de confiança da urna eletrônica



Fonte: TSE

Há a previsão do TSE de fornecer programas para a verificação do hash dos arquivos utilizados. Para isso há os aplicativos Verificação Pré-Pós Eleição (VPP), que é parte integrante dos programas da urna, para conferir os sistemas nela instalados, e Verificador de Autenticação de Programas (VAP), para conferir os sistemas instalados em microcomputadores.

Após a realização do pleito, o art. 36, da Resolução-TSE 23.550/2017 estipula que a verificação do hash somente poderá ser realizada após relatados fatos e apresentados indícios e circunstâncias que a justifique, sob pena de indeferimento liminar. No art. 39, é destacado que o procedimento somente poderá ser realizado por técnico da JE, independentemente do programa a ser utilizado, e ocorrerá na presença dos representantes das entidades e instituições que comparecerem ao ato.

A resolução também trata do RDV. Estabelece que cada voto será gravado de forma aleatória em arquivo único. A JE fornecerá cópia do RDV para fins de fiscalização, conferência, estatística e auditoria do processo de totalização das eleições. Esses arquivos somente poderão ser descartados 180 dias após as eleições.

Os TRE deverão, ainda, realizar por amostragem, no dia da votação, auditoria de funcionamento das urnas eletrônicas sob condições normais de uso, em ambiente controlado, que é a chamada votação paralela. Além disso, nas seções eleitorais, farão a verificação de autenticidade e integridade dos sistemas instalados nas urnas. Em cada unidade da Federação são sorteadas de seis a 15 urnas, dependendo da quantidade de seções eleitorais, sendo que de três a cinco são submetidas à votação paralela e o restante à verificação de autenticidade e integridade. Poderá, ainda, haver restrição, de comum acordo com os representantes de partidos políticos, das coligações, da OAB e do MP, a abrangência dos sorteios a determinados Municípios ou zonas eleitorais, na hipótese da existência de localidades de difícil acesso, onde o tempo hábil para o recolhimento da urna seja inviável. Portanto, a amostragem nessas auditorias não representa a população total de urnas.

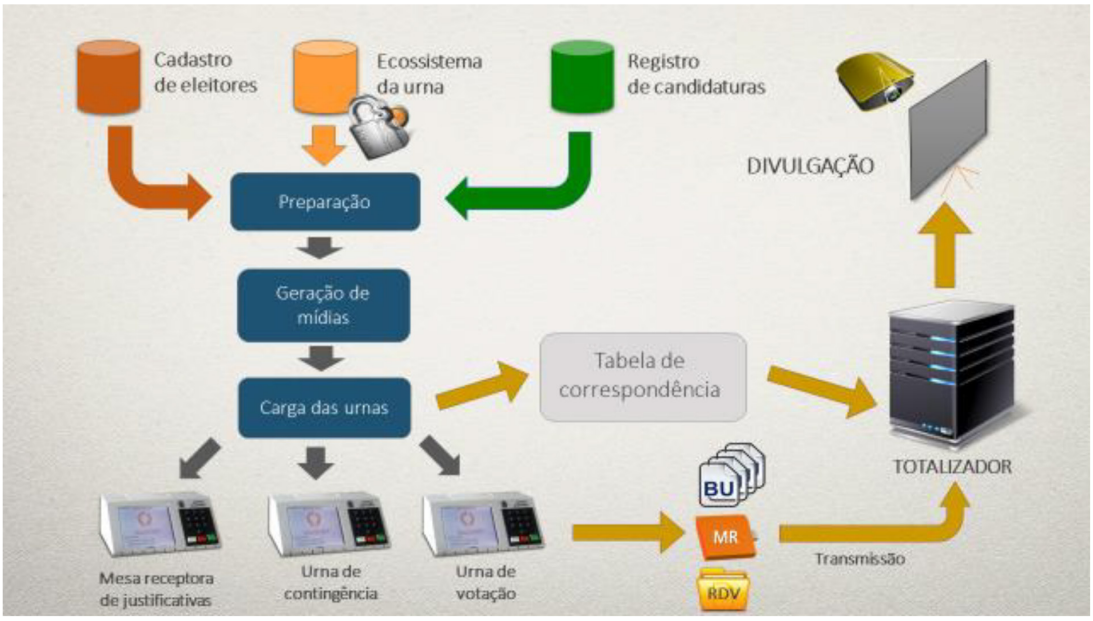
A Resolução-TSE n. 23.554/2017 dispõe sobre os procedimentos preparatórios para as eleições de 2018. Nos artigos 78-98, são descritos os procedimentos de preparação das urnas como a geração de mídias, preparação, testes e lacração física dos equipamentos, garantindo aos partidos políticos, coligações, OAB e MP a conferência dos dados e programas constantes das urnas. A verificação deverá ser realizada em até três por cento das urnas preparadas para cada zona eleitoral, observado o mínimo de uma urna por zona.

A fiscalização da totalização também é tratada na resolução. Define, em linhas gerais, que os partidos políticos, a OAB e o MP podem acompanhar a totalização e constituir sistema próprio de fiscalização, apuração e totalização dos resultados, contratando, inclusive, empresas de auditoria de sistemas, que, credenciadas na JE, receberão os dados alimentadores dos sistemas de totalização.

É ainda previsto, no art. 256, que havendo ação judicial relativa aos sistemas de votação ou de apuração, a autoridade judiciária designará dia e hora para realização de audiência pública. Serão intimados a participar o partido político ou a coligação reclamante e demais interessados. Também será escolhida e separada uma amostra das urnas eletrônicas alcançadas pela ação. Essa amostra será composta por urnas sorteadas entre todas aquelas que foram utilizadas nas seções eleitorais ou considerando-se delimitação a ser apontada pelo recorrente. O requerente deverá indicar técnicos ou auditores próprios para acompanhar os trabalhos de auditoria, que serão realizados por servidores da JE ou funcionários designados pela autoridade administrativa do órgão.

Dentre os principais processos de votação destacam-se a preparação de urnas, geração de mídia e carga dos equipamentos, bem como a transmissão e totalização de votos (figura 3).

Figura 3 – Principais processos da votação



Fonte: TSE

Por sua vez, a Resolução-TSE 23.552/2017 estabelece que serão utilizados lacres e envelopes para garantir a inviolabilidade das urnas e das respectivas mídias utilizadas nas eleições, como fator de segurança física. São descritos os requisitos de segurança dos lacres que deverão ser fornecidos pela Casa da Moeda do Brasil.

2.6 Normas de fiscalização

Segundo a NAT, a Constituição de 1988 ampliou substancialmente a jurisdição e a competência do TCU, para, em auxílio ao Congresso Nacional, exercer a fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, à legitimidade e à economicidade. A auditoria governamental realizada pelo TCU é um elemento primordial para assegurar e promover o cumprimento do dever de *accountability*. Dever esse que os administradores públicos têm para com a sociedade e o Parlamento, dado que a Constituição lhe atribuiu a missão explícita de examinar, como instituição independente de controle, as ações governamentais, cobrar explicações e impor penalidades e limites aos agentes estatais quando exercerem atividades impróprias ou em desacordo com as leis e os princípios de administração pública (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2011).

A ISSAI 100 define que trabalhos de auditoria no setor público podem ser classificados em dois tipos diferentes: trabalhos de certificação e trabalhos de relatório direto. Nos de certificação, "a parte responsável mensura o objeto de acordo com os critérios e apresenta a informação do objeto, sobre a qual o auditor então obtém evidência de auditoria suficiente e apropriada para proporcionar uma base razoável para expressar uma conclusão". Já nos de relatório direto, "é o auditor quem mensura ou avalia o objeto de acordo com os critérios". Assim o auditor define o objeto e os critérios, a partir do risco e materialidade, produzindo, por fim, um relatório de auditoria na forma de achados, conclusões, recomendações ou de uma opinião (INTOSAI - I*NTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS,* 2006).

Os usuários previstos das auditorias desejam ter segurança sobre a confiabilidade e a relevância das informações das fiscalizações para que possam tomar decisões. Assim, na realização de auditorias, deve-se fundamentar as informações em evidências suficientes e apropriadas a partir da execução de procedimentos para administrar o risco de chegar a conclusões inadequadas (risco de auditoria). As partes interessadas devem ser comunicadas de forma transparente do nível de asseguração das auditorias, destacando-se que devido a limitações que lhes são inerentes, as auditorias nunca poderão oferecer uma asseguração absoluta (INTOSAI - *INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS*, 2006).

A asseguração pode ser razoável ou limitada conforme define a ISSAI 100 (*INTOSAI - INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS*, 2006):

> A asseguração razoável é alta, mas não absoluta. A conclusão da auditoria é expressa de forma positiva, transmitindo que, na opinião do auditor, o objeto está ou não em conformidade em todos os aspectos relevantes, ou, quando for o caso, que a informação sobre o objeto fornece uma visão verdadeira e justa, de acordo com os critérios aplicáveis.
>
> Ao fornecer uma asseguração limitada, a conclusão da auditoria afirma que, com base nos procedimentos executados, nada veio ao conhecimento do auditor para fazê-lo acreditar que o objeto não está em conformidade com os critérios aplicáveis. Os procedimentos executados em uma auditoria de asseguração limitada são limitados em comparação com os que são necessários para obter asseguração razoável, mas é esperado que o nível de asseguração, baseado no julgamento profissional do auditor, seja significativo para os usuários previstos. Um relatório de asseguração limitada transmite a natureza limitada da asseguração fornecida.

Um cuidado especial que se deve ter no processo eleitoral é com fraudes. O Referencial de Combate à Fraude e Corrupção traz algumas definições de fraude. Destaca que a intenção é um elemento importante para diferenciar a fraude do erro (BRASIL. TRIBUNAL

DE CONTAS DA UNIÃO, 2018b). A partir do contexto de verificação da votação eletrônica, define-se neste estudo, fraude como um ato ou omissão intencional para manipular, falsificar ou alterar registros eletrônicos de modo a modificar o resultado das eleições.

A ISSAI 100 define que os auditores devem identificar e avaliar os riscos de fraude relevantes para os objetivos da auditoria. Para isso fazem-se indagações e executam-se procedimentos para identificar e responder a esses riscos, mantendo uma atitude de ceticismo profissional e estando alertas para a possibilidade de fraude, durante todo o processo de auditoria. Dessa forma, no planejamento das fiscalizações devem ser previstos procedimentos para verificar o risco de fraude (INTOSAI - *INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS*, 2006).

A seguir serão descritos o levantamento, a auditoria baseada em risco e o manual de auditoria de controles de sistemas de informações federais do GAO, sobre os quais serão sugeridas fiscalizações que poderiam ser aplicadas no processo de votação eletrônica.

2.7 Levantamento

O levantamento é um instrumento de fiscalização que permite a coleta e a sistematização de informações do objeto fiscalizado, com os seguintes objetivos (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2012):

- conhecer a organização e o funcionamento dos órgãos e entidades da administração direta, indireta e fundacional dos Poderes da União, incluindo fundos e demais instituições que lhe sejam jurisdicionadas, assim como dos sistemas, programas, projetos e atividades governamentais no que se refere aos aspectos contábeis, financeiros, orçamentários, operacionais e patrimoniais;

- identificar objetos e instrumentos de fiscalização, permitindo a proposição de trabalhos que se mostrarem mais relevantes para o aperfeiçoamento da gestão pública, detecção de irregularidades administrativas, economia de recursos e efetividade social; e

- avaliar a viabilidade da realização de fiscalizações.

Quando o objetivo é descrever o objeto fiscalizado, o levantamento é descritivo, ou seja, seu relatório irá fornecer uma série de informações detalhadas e sistematizadas para que a unidade técnica (UT) possa, por exemplo, compreender o ambiente, as mudanças ocorridas, os problemas recorrentes e as condições de implementação e operação de organizações, políticas, programas ou projetos públicos (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2018a).

O TCU (2018a) destaca que, quando o levantamento é para identificar objetos e instrumentos de fiscalização, a ação de controle é analítica, havendo a descrição do objeto fiscalizado e seu cenário, sendo realizadas análises que irão orientar a atuação da UT, seja identificando um rol de trabalhos futuros, seja fornecendo subsídios para o posicionamento quanto à viabilidade de realização ou não de uma fiscalização específica.

A necessidade de a UT obter e manter atualizado o conhecimento acerca das unidades jurisdicionadas pode ensejar a realização de levantamento ou produção de conhecimento. O levantamento será determinado, também, para a definição de futuras ações de controle em áreas ou assuntos específicos sobre os quais exista pouca informação disponível na UT (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2018a).

O levantamento pode ser de escopo amplo ou restrito. Levantamentos realizados em programas de governo, políticas públicas, organizações e instituições públicas são exemplos de trabalhos de escopo amplo. Já nos de escopo restrito, são realizadas a coleta e a análise de dados de objetos de controle específicos, pontuais, como um processo de trabalho que entrega um produto de uma política pública (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2018a).

As principais técnicas de coleta de dados nos levantamentos são: entrevista, pesquisa, observação direta e uso de dados existente. Nos procedimentos de análise de dados, são utilizadas técnicas de diagnóstico que auxiliam a sistematizar informações relativas ao objeto fiscalizado. As principais técnicas de diagnóstico são: análise SWOT, Diagrama de Verificação de Risco (DVR), Análise Stakeholder, mapeamento de processos, avaliação de riscos, Diagrama de Causa-Efeito e árvore de problemas, dentre outras (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2018a). O levantamento é realizado seguindo as etapas mostradas na figura 4.

Figura 4 – Etapas do Levantamento

Fonte: TCU

A decisão sobre quais técnicas de diagnóstico utilizar fica a critério do julgamento profissional da equipe, porém, ao final do planejamento, o escopo do trabalho e a matriz devem estar concluídas. As informações obtidas na fase de planejamento auxiliam na elaboração da visão geral do objeto. Ao final da fase de execução, as técnicas de diagnóstico devem estar concluídas, documentadas e validadas com o gestor.

A avaliação de viabilidade é composta por duas etapas. A primeira, que é comum aos demais levantamentos, consiste no entendimento do objeto e do seu ambiente. A segunda corresponde à manifestação valorativa, substantiva e convincente da UT sobre a conveniência e a oportunidade de se realizar fiscalização específica. O relatório abrange análises sobre as razões que recomendaram a escolha do objeto de controle; custo benefício da atuação do Tribunal; os riscos assumidos pelo TCU caso opte pela não realização do trabalho; as oportunidades que uma ação do TCU pode trazer para promover aperfeiçoamentos na administração pública, além de destacar temas relevantes, gerando resultados que agreguem valor (BRASIL. TRIBUNAL DE CONTAS DA UNIÃO, 2018a). O estudo de viabilidade traz informações sobre os principais processos de trabalho e seus produtos.

2.8 Auditoria baseada em risco

Auditoria baseada em risco (ABR) é a abordagem que utiliza a avaliação de riscos para a definição do escopo, natureza, época e extensão dos procedimentos adicionais de auditoria, com o propósito de reduzir o risco de emitir opinião ou conclusão inadequada às circunstâncias do trabalho (INTOSAI - *INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS*, 2006).

A metodologia agrega valor por permitir à equipe de auditoria estabelecer o foco do trabalho nos aspectos mais relevantes, considerando as deficiências, os desvios ou as distorções que possam ocorrer, com base nos resultados da avaliação de riscos, bem como por permitir ao auditor gerenciar o risco de auditoria em um nível aceitável, para fornecer a asseguração de auditoria que atenda às expectativas dos usuários. Essas expectativas são segurança, confiabilidade, relevância do trabalho e reponsabilidade (INTOSAI - *INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS*, 2006).

Gomes (2017) destaca que, durante uma ABR, o risco de auditoria deve ser controlado. De acordo com a ISSAI 100 o risco de auditoria é o risco de que o relatório de auditoria possa ser inadequado, ou mais especificamente em auditorias de conformidade é o risco de que a conclusão ou a opinião do auditor possam ser inadequados às circunstâncias da auditoria.

A ABR busca comparar um critério com uma situação encontrada, podendo verificar a existência de distorção relevante, ou seja, uma discrepância entre a informação

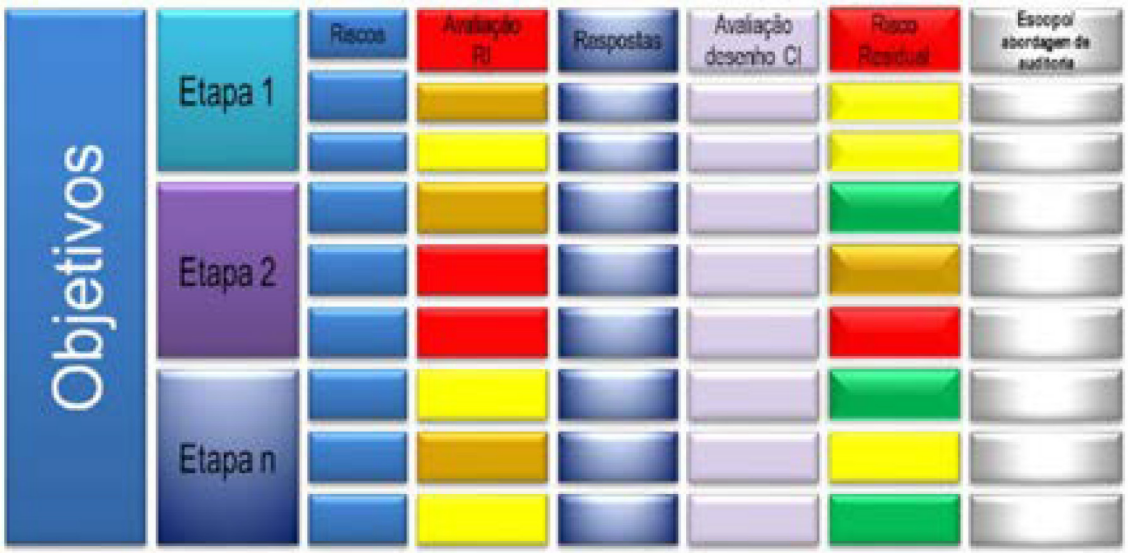
sobre o objeto e a sua substância ou essência (condição real), causada por erro ou fraude, e que pode levar os usuários da informação a tomar decisões incorretas ou inadequadas (GOMES, 2017).

Compõem o risco de auditoria os riscos que não dependem diretamente do auditor, que são o risco inerente e o risco de controle, bem como o risco que depende diretamente do auditor, que é o risco de detecção. Quando o risco inerente e o risco de controle são altos, há a necessidade de adotar provimentos de auditorias mais complexos e de maior extensão, a fim de reduzir a chance de que uma não conformidade seja detectada.

Na ABR, é necessário buscar na fase de planejamento o entendimento do objeto auditado, do ambiente, e do controle interno. O controle interno é aqui entendido como o processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade. O controle interno pode ser avaliado em nível de entidade, processos ou atividade (GOMES, 2017).

Segundo Gomes (2017) na ABR será produzida uma matriz de avaliação de riscos em que são descritos os objetivos e as etapas de um processo de trabalho. São identificados e avaliados os riscos, bem com o desenho dos controles internos, obtendo-se, assim, o risco residual sobre o qual será avaliado o ingresso no escopo ou abordagem de auditoria (figura 5).

Figura 5 – Matriz de avaliação de riscos



Fonte: (GOMES, 2017) (Adaptado)

O risco inerente é relacionado ao risco do negócio, processo ou atividade, independente dos controles adotados, na ausência de ações gerenciais que possam reduzir a probabilidade de materialização do risco ou do impacto nos objetivos. Na avaliação dos riscos é utilizada uma matriz para comparar a probabilidade e impacto dos riscos (GOMES, 2017) (figura 6).

Figura 6 – Matriz Impacto x Probabilidade e Níveis de Risco

Legenda Nível de Risco Extremo Alto Médio Baixo		Probabilidade				
		0,1 Muito Baixa	0,2 Baixa	0,5 Média	0,8 Alta	1 Muito Alta
Impacto	1 Muito Alto	0,10	0,20	0,50	0,80	1,00
	0,8 Alto	0,08	0,16	0,40	0,64	0,80
	0,5 Médio	0,05	0,10	0,25	0,40	0,50
	0,2 Baixo	0,02	0,04	0,10	0,16	0,20
	0,1 Muito Baixo	0,01	0,02	0,05	0,08	0,10

Fonte: TCU (adaptado)

Na avaliação da adequação do desenho do controle será considerado se o controle, individualmente ou em combinação com outros controles, é capaz de impedir, ou de detectar e corrigir efetivamente, distorções relevantes. Na fase de execução da auditoria será verificado se o controle existe e foi implementado pela entidade (GOMES, 2017).

Os procedimentos para obter evidências a respeito do desenho e implementação dos controles são indagações, observações e inspeção de documentos e relatórios. A partir dessa avaliação, é elaborada a escala de riscos residuais, bastante semelhante à matriz constante da figura 6. Na matriz, são contabilizados os riscos e a eficácia do controle.

Esses procedimentos permitem a avaliação do risco, sendo realizados em grande parte na fase de planejamento da auditoria. Na fase de execução, serão realizados os procedimentos adicionais de auditoria, que são planejados em reposta aos riscos significativos identificados na aplicação dos procedimentos de avaliação dos riscos.

O risco de detecção definirá a natureza e extensão dos testes substantivos, que envolvem procedimentos analíticos, confirmação, recálculo e reexecução. São empregados para confirmar que não existem distorções relevantes nas informações do objeto em relação a sua condição real (GOMES, 2017).

2.9 Manual de auditoria de controles de sistemas de informações federais do GAO

O *United States Government Accountability Office* (GAO), entidade fiscalizadora superior americana, que é o equivalente ao TCU nos Estados Unidos da América, publicou um manual de auditoria de controles de sistemas de informações federais (*Federal Information System Controls Audit Manual* – Fiscam). Esse manual apresenta uma metodologia para execução de auditoria em sistemas de informação dos órgãos federais daquele país.

Controles de sistemas de informações são os controles internos que dependem de informações que são processadas por sistemas e incluem controles gerais e controle de aplicativos (*U.S. GOVERNMENT ACCOUNTABILITY OFFICE*, 2009). O objetivo do manual é trazer uma metodologia de avaliação desses controles gerais e de aplicativos.

Segundo o Fiscam, os controles gerais incluem o gerenciamento de segurança, para assegurar a efetividade desses controles. São verificados o programa de gerenciamento de riscos, avaliações e validações periódicas de riscos, procedimentos e políticas de segurança, medidas para tratar de deficiências de segurança de informação e segurança sobre atividades realizadas por terceiros externos. Também podem ser avaliados os controles de acesso para garantir que o ingresso a recursos computacionais (dados, equipamentos e instalações) são razoáveis e restringem o acesso a pessoas autorizadas. Além desses controles gerais, o manual também aborda gerenciamento de configurações, segregação de funções e plano de contingência.

Os controles de aplicativos envolvem a avaliação da completude, acurácia, validade, confidencialidade e disponibilidade. Em relação à completude avaliam-se se todas as transações que dão entrada nos sistemas são aceitas para processamento, processadas e incluídas corretamente nas saídas. Na avaliação da acurácia, verificam-se os seguintes requisitos: se as transações são registradas adequadamente, com quantidade / dados corretos e em tempo hábil (no período apropriado); se a entrada dos principais elementos de dados para transações é precisa; se os elementos de dados são processados com precisão por aplicativos que produzem resultados confiáveis; e se a saída é precisa. Os controles de validade asseguram que todas as transações registradas de fato ocorreram (são reais), que estão relacionadas à organização, são autênticas e foram devidamente validadas e que a saída contém apenas dados válidos. Os controles de confidencialidade garantem que os dados do aplicativo, relatórios e outras saídas são protegidos de contra acesso não autorizado. Por fim, os controles

de disponibilidade garantem que esses dados estão prontamente disponíveis quando as partes interessadas necessitem.

A partir desses controles o manual lista as técnicas e sugere procedimentos de auditorias relacionados. Esses são descritos em alto nível e se assume que os auditores têm um nível de especialização suficiente para executar os procedimentos de auditoria de forma eficaz.

3. Metodologia

3.1 Classificação da pesquisa

Nas palavras de Souza (2010, p. 12), "pesquisa pode ser definida como a atividade científica por meio da qual se revelam aspectos da realidade". De acordo com Silva e Menezes (2005), existem várias formas de classificar as pesquisas.

Do ponto de vista da sua **natureza**, foi uma **pesquisa aplicada**: objetivou gerar conhecimentos para aplicação prática e dirigidos à solução de problemas específicos. Envolveu verdades e interesses locais (SILVA e MENEZES, 2005, p. 20).

Do ponto de vista da forma de **abordagem do problema**, foi uma **pesquisa qualitativa**:

> considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa. Não requer o uso de métodos e técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave. É descritiva. Os pesquisadores tendem a analisar seus dados indutivamente. O processo e seu significado são os focos principais de abordagem (SILVA e MENEZES, 2005, p. 20).

Do ponto de vista de seus **objetivos**, foi uma **pesquisa exploratória**:

> visa proporcionar maior familiaridade com o problema com vistas a torná-lo explícito ou a construir hipóteses. Envolve levantamento bibliográfico; entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; análise de exemplos que estimulem a compreensão. (GIL, 1991, apud SILVA e MENEZES, 2005, p. 21).

Do ponto de vista dos **procedimentos técnicos**, adotou mais de uma forma (GIL, 1991, apud SILVA e MENEZES, 2005, p. 21):

pesquisa bibliográfica: quando elaborada a partir de material já publicado, constituído principalmente de livros, artigos de periódicos e atualmente com material disponibilizado na Internet;

pesquisa documental: quando elaborada a partir de materiais que não receberam tratamento analítico;

3.2 Classificação do método científico

Os procedimentos utilizados nesta investigação científica partiram da análise de avaliações sobre a votação eletrônica e de diretrizes internacionais buscando identificar trabalhos de auditoria que realizados em sequência levarão a uma asseguração razoável de que o voto dos eleitores em seus representantes foi devidamente coletado e totalizado pela Justiça Eleitoral. Trata-se, portanto, do uso do método indutivo, o qual pode ser assim descrito:

> Método proposto pelos empiristas Bacon, Hobbes, Locke e Hume. Considera que o conhecimento é fundamentado na experiência, não levando em conta princípios preestabelecidos. No raciocínio indutivo a generalização deriva de observações de casos da realidade concreta. As constatações particulares levam à elaboração de generalizações (GIL, 1999; LAKATOS; MARCONI, 1993 apud SILVA, 2005, p.26).

3.3 Revisão bibliográfica

A presente pesquisa teve início pela revisão bibliográfica acerca dos assuntos que circundam o tema principal. Foram estudadas publicações sobre votação eletrônico (devido a identificação de boas práticas internacionais), direito eleitoral (devido a identificação dos processos de trabalho relacionados à votação eletrônica) e normas de auditoria (devido à identificação de tipos e técnicas de auditorias).

Ressalte-se que a etapa de revisão bibliográfica teve como objetivo trazer a mais recente produção científica acerca dos temas tratados. Para isso, foram realizadas pesquisas nas bases de dados Scielo.org. As pesquisas foram realizadas no dia 14 de outubro de 2018, com as palavras-chave “urna eletrônica” e “votação eletrônica”. A pesquisa por “urna eletrônica” encontrou três artigos, dos quais dois tratavam de temas próximos aos aqui debatidos. Já a pesquisa por “votação eletrônica” encontrou dois artigos, nenhum deles tratando de temas próximos.

Após leitura dos resumos dos artigos que tinham títulos sugestivos de que eles tratavam de temas próximos aos estudados, constatou-se que nenhum deles continha elementos diferentes daqueles já debatidos nas publicações utilizados como base teórica, nem tampouco temas similares ao desta monografia. Como já haviam sido

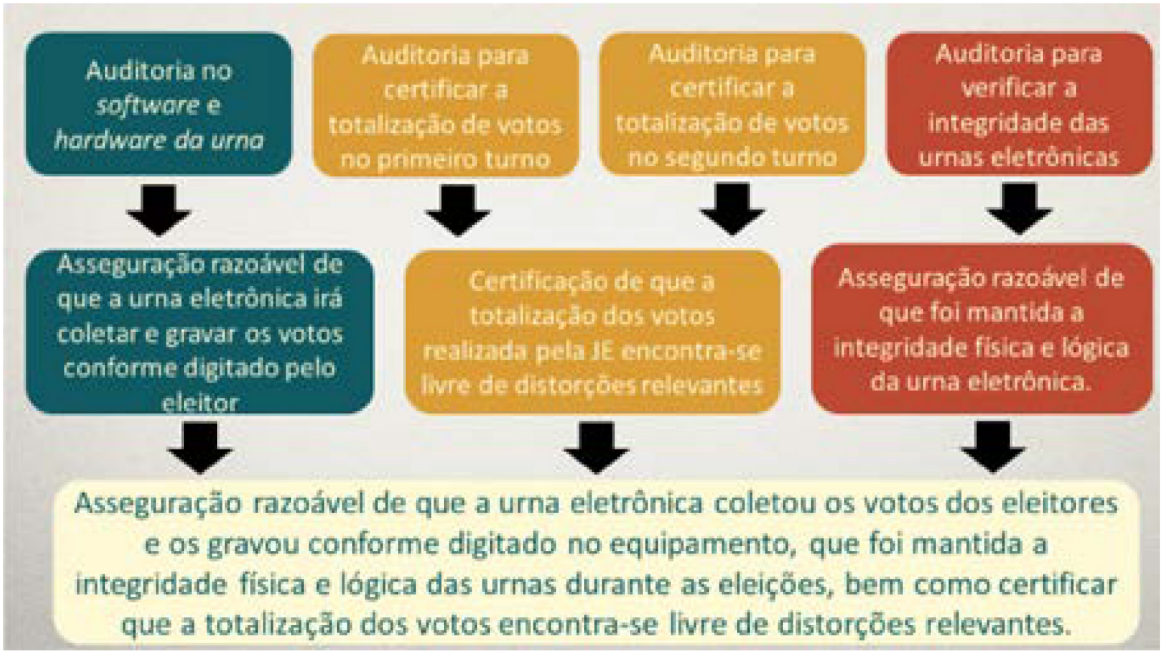
identificadas publicações sobre o assunto foi utilizada a técnica de snowball a partir das referências, sendo identificados artigos e outras publicações que foram utilizadas. Por estes motivos, o principal embasamento da revisão bibliográfica foram publicações, leis e normas que tratam sobre o tema, além de alguns artigos.

A etapa de revisão bibliográfica fundamentou o referencial teórico tratado no capítulo 2 desta monografia, e permitir a concretização dos objetivos específicos "descrever boas práticas internacionais que possam fornecer subsídios em auditorias relacionadas à votação eletrônica" e "descrever processos de trabalhos da justiça eleitoral nos quais possam ser executados procedimentos de auditoria, buscando identificar e avaliar os riscos de fraude".

4. Discussão dos resultados

Consideramos que seria possível definir auditorias por meio das quais se asseguraria de forma razoável a lisura da votação eletrônica. Antes das eleições seriam auditados software e o hardware da urna eletrônica, haveria a recontagem dos votos pelo controle externo a partir dos RDV e, por fim, seria auditada a integridade física e dos arquivos das urnas eletrônicas, para detectar a materialização de riscos de fraudes (figura 7).

Figura 7 – Auditorias que poderiam fornecer asseguração e certificação da votação eletrônica



Fonte: o próprio autor

Partindo do pressuposto anterior seriam realizadas quatro auditorias durante o ano em que houver eleições. A primeira seria no hardware e no software para assegurar, de forma razoável que: as urnas eletrônicas utilizadas sigam as especificações requeridas pelo TSE, que os programas garantam a segurança do sistema com a implementação de controles adequados e que funcionem de forma que os votos sejam coletados e gravados conforme a vontade do eleitor, garantindo o sigilo, a fidedignidade e a integridade dos votos.

A segunda e terceira auditorias seriam realizadas, respectivamente, após o primeiro e segundo turno das eleições para certificar que a totalização de votos realizada pela JE está, em todos os aspectos relevantes livre de distorções com os dados dos RDV fornecidos ao TCU. Para essa auditoria urnas eletrônicas gerariam uma cópia do RDV criptografada pelo TCU que seria transmitida junto com os demais arquivos da mídia de resultado aos TRE que fariam a retransmissão ao TCU. Dessa forma o tribunal de contas realizaria uma totalização própria, confrontada com os resultados divulgados pela JE.

A quarta auditoria seria realizada, utilizando amostragem probabilística, quando as urnas eletrônicas estivessem armazenadas após o segundo turno. Nessa auditoria, assegurar-seia que após o uso nas eleições, as urnas eletrônicas encontrar-se-iam com os lacres físicos devidamente intactos, com o software igual ao que foi assinado e lacrado digitalmente pelo TSE, sem arquivos estranhos ao sistema, bem como com o log sem sinalização de eventos anômalos. Seria verificado, ainda, se os RDV recebidos pelo TCU são os mesmos armazenados nas urnas, assegurando a integridade dos arquivos recebidos durante a certificação. Para isso, equipes de auditorias iriam aos locais de armazenamento das urnas para verificar, utilizando programa a ser desenvolvido pelo controle externo, o hash e a estrutura de arquivos das urnas e, ainda, seria copiado o log para análise.

As quatro auditorias iriam, por meio de evidências suficientes e apropriadas, formar uma convicção que asseguraria a lisura da votação eletrônica e da totalização dos votos a cada eleição. Com os resultados desses trabalhos, seria possível obter uma asseguração razoável de que a urna eletrônica coletou os votos dos eleitores e os gravou de forma íntegra e segura, certificaria que a totalização dos votos encontrar-se-ia livre de distorções relevantes, bem como que seria mantida a integridade física e lógica dos equipamentos durante as eleições (figura 8).

Figura 8 – Infográfico com a relação entre as auditorias da votação eletrônica

Fonte: o próprio autor.

Entendemos haver uma assimetria de informações entre o TSE e a sociedade. À medida que o órgão recebe poderes e recursos para realizar o processo eleitoral, a sociedade passa a depender unicamente da Justiça Eleitoral para obter informações sobre o processo. Assim, surge a necessidade de que uma terceira parte forneça asseguração, que mitigue a assimetria de informação e o conflito de agência. Esse papel de avaliar a accountability do agente é realizado pela auditoria.

A Recomendação CM/Rec(2017)5 do Conselho da Europa prevê que a votação eletrônica seja auditável e que haja uma avaliação, em intervalos de tempo regulares, por uma entidade independente do sistema de votação eletrônica. O EAC também prevê que haja um programa de testes e certificação dos sistemas de votação eletrônica com o propósito de ser realizado por meio de testes independentes. As normas internacionais trazem previsão de avaliação dos sistemas de votação eletrônica por entidades independentes, o que leva confiança e aceitação ao uso das urnas eletrônicas.

Atualmente o TSE garante que a urna eletrônica processe e grave corretamente os votos, faz a totalização, realiza testes públicos de segurança no funcionamento das urnas, promove a "votação paralela" e faz a auditoria dos softwares das urnas antes e no dia das eleições. Todavia a ausência de verificação externa mantém as informações centradas na JE. A realização de auditorias externas mitigaria essa assimetria, pela avaliação dos processos de trabalho do TSE e dos TRE.

Em consulta aos trabalhos do TCU relacionados ao sistema de votação eletrônica, verificamos que o tribunal tem tratado de temas relacionados a aquisição das urnas e à implantação do voto impresso, suspensa conforme decisão do STF. Não há trabalhos relacionados diretamente ao uso de urnas eletrônicas nas eleições. Em decorrência dessa lacuna de trabalhos sobre o tema, entendemos que haveria necessidade de uma ação de controle prévia que permitiria a coleta e a sistematização de informações sobre a votação eletrônica antes das auditorias sugeridas. Esse trabalho inicial serviria como uma ferramenta descritiva do processo eleitoral com o uso de urnas eletrônicas e para definir as fiscalizações decorrentes do entendimento da matéria.

4.1 Normas sobre votação eletrônica da JE e as diretrizes internacionais

Comparando as normas do TSE sobre votação eletrônica com a Recomendação CM/Rec(2017)5 do CoE e com as VVSG do EAC, mencionados no Referencial Teórico, verifica-se que o desenho das normas nacionais acompanham grande parte essas diretrizes, observando os parâmetros para a votação universal, equânime e livre; o sigilo do voto; requerimentos regulatórios e organizacionais; bem como a confiabilidade e segurança. Todavia, há oportunidade de melhoria em alguns outros aspectos.

Quanto a transparência, o CoE (2017c) orienta que os componentes físicos e lógicos do sistema de votação eletrônico devem ser verificados e certificados. No caso brasileiro, não há a divulgação extensiva do código-fonte, havendo acesso durante os TPS. Aranha et al (2018) consideram que, nesses eventos, é possível examinar os mecanismos de segurança por alguns dias, o que permite encontrar vulnerabilidades e sugerir correções, sendo uma alternativa útil para realizar análises independentes de segurança.

O TSE detém o código-fonte, bem como define o *hardware* da urna eletrônica, havendo uma centralização do processo, o que assegura ao órgão um controle alto sobre a votação eletrônica, não havendo certificação externa dos componentes ou *software*. Isso leva ao órgão ter uma alta confiança na votação eletrônica, deixando, porém, a própria JE como quase que a única fonte de informações sobre a segurança da votação eletrônica.

Segundo o CoE (2017c), o órgão eleitoral deveria desenvolver requisitos técnicos, de avaliação e certificação que refletissem os princípios legais e democráticos relevantes associado à votação eletrônica. Ressalta que deveria haver a avaliação por organismo independente e competente da conformidade do sistema de votação eletrônica com esses critérios, fomentando a *accountability* do processo. Nas aquisições das urnas eletrônicas são definidas especificações que podem ser avaliadas, bem como há disposições na legislação eleitoral que podem ser utilizadas como critérios. Além disso, as VVSG detalham procedimentos que podem ser aplicados em processos de trabalhos relacionados à votação eletrônica. Dessa forma seria possível que uma

entidade independente e competente, como uma Entidade Fiscalizadora Superior (EFS), realizasse esse trabalho de avaliação da votação eletrônica a partir de critérios da própria JE, bem como de diretrizes do CoE e do EAC.

É ressaltado pelo CoE (2017c) que um meio para estabelecer confiança nas eleições é pelo processo de fiscalização da votação eletrônica, que deve ser auditável. Além do TPS, a Resolução-TSE 25.550/2017 estabelece a auditoria de funcionamento das urnas eletrônicas sob condições normais de uso (votação paralela) e, nas seções eleitorais, a verificação de autenticidade e integridade dos sistemas instalados nas urnas.

Os partidos políticos e demais entidades que acompanham as eleições poderão observar a especificação, o desenvolvimento e a inspeção dos sistemas utilizados na votação eletrônica, podendo utilizar programas de análise de códigos para a análise estática do software. Também podem solicitar a verificação da assinatura digital e dos hash do software durante a cerimônia de geração de mídias e durante a carga das urnas. Além disso, desde as 48 horas que antecedem o início da votação até às 17 horas do dia da eleição, podem verificar os Sistemas de Transporte de Arquivos da Urna Eletrônica, o Subsistema de Instalação e Segurança e a Solução JEConnect. As urnas eletrônicas também podem ser verificadas por essas entidades após as eleições desde que relatados fatos e apresentados indícios e circunstâncias que justifiquem a análise.

Tanto a "votação paralela" quanto a auditoria para a verificação da autenticidade e integridade dos sistemas, a ser realizada no dia das eleições, têm as urnas selecionadas por amostragem pela JE. A Comissão de Auditoria da Votação Eletrônica, instituída em cada um dos TRE, deve sortear entre seis e quinze seções eleitorais dependendo da quantidade de seções da UF, sendo que de três a cinco urnas dessas seções seriam verificas na "votação paralela" e as restantes teriam a verificação da autenticidade e integridade dos sistemas realizada no dia da eleição, antes da emissão da zerésima.

A Comissão de Auditoria da Votação Eletrônica pode restringir, de comum acordo com os representantes dos partidos políticos, das coligações, da OAB e do MP, a abrangência dos sorteios a determinados municípios ou zonas eleitorais, na hipótese da existência de localidades de difícil acesso, onde o tempo hábil para o recolhimento da urna fosse inviável. Dessa forma, nessas auditorias, a amostra não representa a totalidade das urnas, levando os resultados à uma asseguração limitada, com as constatações servindo às urnas avaliadas.

Foi visto que há a previsão da fiscalização dos partidos políticos em diversas etapas, todavia não há elementos que indiquem uma atuação expressiva desses entes. Assim, seria desejável haver um treinamento dos representantes de partidos políticos para acompanhar essa etapa do processo, estimulando a prática de se verificar mais urnas eletrônicas no dia da votação.

Como exposto, a JE permite a diversas entidades acompanhar e atuar na votação eletrônica, todavia esse processo é regulado de forma que a própria Justiça Eleitoral é a avaliadora do sistema, havendo limitações na extensão e na época de procedimentos de auditoria. Não há no desenho da votação eletrônica a previsão de avaliação por organismo independente e competente para verificar a conformidade dos sistemas utilizados.

Dessa análise, observa-se que a ausência de controle externo na votação eletrônica leva a lacunas na comparação da votação eletrônica brasileira com as diretrizes de transparência e observação, bem como de accountability, do CoE. Os componentes e sistemas da votação eletrônica não passam por verificação externa por organismo independente e competente. Para mitigar a ausência dessa verificação a JE prevê a participação dos partidos políticos, OAB, MP e outras entidades no acompanhamento de auditorias realizadas pela JE, porém, nessas oportunidades a JE controla a extensão e a época dos procedimentos, o que reforça a concentração de informações sobre a votação eletrônica nos órgãos eleitorais, favorecendo a assimetria de informações entre a sociedade e a JE.

4.2 Levantamento sobre votação eletrônica

O levantamento consiste em uma ação de controle para a coleta e a sistematização de informações do objeto fiscalizado. Como há uma lacuna de trabalhos do TCU relacionados à votação eletrônica, seria necessário realizar um levantamento para o conhecimento de detalhes da votação eletrônica.

Dessa forma, inicialmente seria indicado um levantamento de escopo restrito às atividades relacionadas à votação eletrônica no processo eleitoral no TSE e TRE para conhecer o objeto fiscalizado e verificar a viabilidade de ações de controle, como as propostas no presente trabalho. A época ideal para essa ação seria no ano anterior às eleições gerais, para permitir a execução das auditorias no exercício seguinte no qual ocorreria o pleito.

Nesse trabalho seria essencial verificar junto ao TSE e aos TRE a viabilidade de procedimentos propostos para as demais auditorias, como a forma de se conceder o acesso aos códigos-fonte e códigos-executáveis dos programas utilizados na votação eletrônica, a viabilidade técnica de se adotar aplicativo que possibilite a geração do RDV criptografado pelo TCU, bem como a transmissão de arquivos dos TRE para a Corte de Contas. Além da parte técnica, também haveria a necessidade de analisar a necessidade de eventuais ajustes na legislação para que os procedimentos pudessem ser realizados.

Os processos de trabalhos decorrentes da cotação eletrônica deveriam ser mapeados para a identificação de riscos. Para isso seria desejável que a fase de execução dos

trabalhos coincidisse com alguma eleição suplementar[3] para ser possível acompanhar o pleito pontual e obter um melhor entendimento do processo de uso das urnas eletrônicas. A eleição suplementar seria acompanhada para comparar o desenho das normas eleitorais com o que efetivamente ocorre em uma eleição.

De acordo com Marcelo e Pereira (2005) em qualquer instituição, as pessoas são o elo mais fraco dentro da segurança da informação. Aranha et al (2018) também destacam os riscos de um ataque interno à medida que haveria graves riscos à segurança do processo caso houvesse o acesso chaves de autenticação, concluindo que a integridade do software e dos resultados depende do sigilo da chave simétrica, a qual teria acesso trivial para a equipe de desenvolvimento. Assim, deveriam ser identificados o pessoal com acesso privilegiado a informações chave da urna eletrônica, bem como empresas e demais envolvidos com o processo.

No levantamento seria verificada a viabilidade de fiscalizações no processo eleitoral analisando se as unidades técnicas do TCU teriam capacidade e recursos para analisar os códigos-fonte dos softwares utilizados pela JE nas eleições, indicando lacunas que deveriam ser preenchidas por meio de capacitação do corpo técnico ou por meio de especialistas externos.

Deveria haver uma avaliação inicial dos códigos-fontes utilizados na votação eletrônica. Aranha (2018) destaca que na base de código disponibilizada para o TPS 2017 havia mais de 40 milhões de linhas de código. Nessa etapa deverão ser verificadas as linguagens de programação utilizadas e a função dos programas. Ante a grandiosidade dos códigos, a equipe do levantamento poderia elaborar uma matriz de avaliação de riscos para definir o que seria materialmente relevante analisar em auditorias posteriores.

Nessa fase seria desejável haver contato com os Tribunais de Contas Estaduais para avaliar se haveria possibilidade desses órgãos participarem de eventual auditoria para verificar a integridade das urnas eletrônicas. Como descrito mais à frente há UF em que os depósitos de urnas são centralizados, porém, em especial nos estados de São Paulo, Rio Grande do Sul, Paraná, Mato Grosso do Sul e Bahia há depósitos de urnas em diversas zonas eleitorais, havendo, no caso paulista mais de duzentos municípios nos quais são armazenadas urnas. Assim, para que os equipamentos sejam avaliados em um tempo razoável seria desejável que houvesse participação dos TCE, pois os deslocamentos entre municípios podem tomar um tempo razoável levando a uma necessidade de mais equipes de auditorias para realizar a análise das urnas eletrônicas *in loco*.

---

3 As eleições suplementares ocorrem quando a votação para presidente, governador ou prefeito atingir nulidade em mais da metade dos votos válidos dados a candidatos com registro indeferido, após decisão indeferitória do pedido de registro no Tribunal Superior Eleitoral (TSE). Apenas em 2016 não houve eleições suplementares no período dos últimos 10 anos.

Nessa fase também poderia ser buscada formas de aprimorar o controle social e dos partidos políticos para que esses possam ter uma atuação de maior destaque na segurança da votação eletrônica. Poderiam ser elaborados, por exemplo, recursos educacionais (cartilhas, vídeos) com objetivo de orientar fiscais de partidos políticos a acompanhar os procedimentos utilizados pela JE para verificar a autenticidade e integridade das urnas durante as eleições. Isso contribuiria no aumento da confiança no processo eleitoral.

O TCU poderia passar a acompanhar os TPS, elaborando relatórios de produção de conhecimento a partir da atuação dos participantes do evento. Como esses testes têm previsão normativa de ocorrer no último semestre anterior aos anos com eleições gerais, possivelmente não estaria ocorrendo auditorias na JE no período, de forma que a produção de conhecimento seria a ferramenta propícia para essa avaliação.

Além de se verificar a viabilidade das auditorias aqui sugeridas, esse trabalho também poderia indicar outras fiscalizações pertinentes. Um exemplo seria obter entendimento sobre o armazenamento das urnas eletrônicas, em especial frente à fragmentação que ocorre nos TRE, havendo tribunais que centralizam esse armazenamento e outros que distribuem as urnas por diversas zonas eleitorais em dezenas de municípios.

4.3 Auditoria no software e hardware das urnas eletrônicas

Propomos uma auditoria baseada em risco, realizada a partir do entendimento dos controles internos em nível de atividade da votação eletrônica, avaliando o controle de aplicativos e verificando se as urnas eletrônicas atendem às especificações do TSE. Na fase de levantamento anterior já seriam elencados os riscos de forma que a fase de planejamento dessa etapa seria curta.

O Fiscam traz metodologia para a avaliação de controles de aplicativos que poderia ser utilizada na verificação do *software* utilizado na votação eletrônica. A partir desse manual do GAO haveria a possibilidade de auditar os controles críticos do sistema da urna eletrônica.

Deficiências no controle de aplicativos podem levar a acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados de aplicativos e dados (*U.S. GOVERNMENT ACCOUNTABILITY OFFICE*, 2009). Nessa avaliação poderiam ser consideradas as seguintes características:

- gerenciamento de segurança;
- autorizações;
- inteireza;

- precisão;
- integridade de processamento e dos arquivos de dados.

Os controles de gerenciamento de segurança servem como base para as entidades obterem segurança razoável de que o aplicativo é efetivamente seguro. Envolve estabelecer um plano de segurança do aplicativo, avaliar e validar periodicamente os riscos de segurança, documentar e implementar política de segurança e procedimentos para aplicativos, dentre outras. Poderia ser avaliado como o TSE aborda esses riscos e as medidas adotas para mitigálos.

Nos controles de autorização poderiam ser avaliadas restrições de acesso ao sistema da urna eletrônica, bem como se relatórios de exceções são usados para garantir que todos os dados processados sejam autorizados. A verificação desse controle permite fornecer uma garantia razoável de que apenas pessoal autorizado tenha acesso ao sistema da urna eletrônica e apenas para fins autorizados.

Sobre os controles da inteireza poderia ser verificado se todas as transações autorizadas são registradas e processadas pela urna eletrônica. A partir dessa análise poderia ser observado se os votos digitados são inseridos corretamente no sistema, aceitos para processamento, processados uma única vez e incluídos na saída de dados.

Na análise dos controles de precisão devem ser avaliadas se as transações são registradas adequadamente, com as informações corretas e em tempo hábil; se a entrada dos principais elementos de dados para transações é precisa; se as informações são processadas com precisão por aplicativos que produzem resultados confiáveis; e se a saída é precisa. Podem ser analisadas se as características do desenho da entrada de dados contribuem para a precisão dessas informações, bem como se dados são validados para identificar informações equivocadas.

Quanto aos controles de integridade de processamento e dos arquivos de dados poderiam, por exemplo, analisar se os programas incluem rotinas para verificar o uso da versão apropriada do arquivo de computador durante o processamento.

Em alguns dos aplicativos do sistema de votação também poderia ser analisado o código-fonte de forma direta ou por meio de *software* específico de análise de programas. Isso automatizaria parte dos procedimentos, permitindo uma maior eficiência dos trabalhos da auditoria.

Ao final dessa fiscalização seria emitida uma conclusão que deveria fornecer uma asseguração razoável de que o *software* da urna eletrônica está em conformidade em todos os aspectos relevantes para que haja a coleta, a gravação e a transmissão dos votos dos eleitores conforme digitado e de forma segura, bem como que o *hardware*

dessas urnas se encontre em conformidade em todos os aspectos relevantes com o especificado pelo TSE. Confirmadas essas informações haveria uma certeza alta de que as urnas eletrônicas, desde que não sejam alteradas, efetivamente registram o voto dos eleitores sem haver adulterações, além de haver controles que mitiguem o risco de ataque aos sistemas da votação eletrônica.

4.4 Auditoria para certificar a totalização dos votos

Em 2003 o RDV foi instituído como um arquivo que armazena em uma tabela, de forma aleatória, os dados brutos dos votos dos eleitores. O conceito desse arquivo é o de criar um registro eletrônico que possa servir de trilha de auditoria para a recontagem dos votos. A partir desses arquivos é possível gerar os boletins de urna e refazer a totalização dos votos.

Consideramos que esses arquivos podem ser utilizados para que o controle externo certifique a totalização dos votos realizada pela JE. De acordo com a ISSAI 100, nos trabalhos de certificação a parte responsável mensura o objeto de acordo com os critérios e apresenta a informação do objeto, sobre a qual o auditor, então, obtém evidência de auditoria suficiente e apropriada para proporcionar uma base razoável para expressar uma conclusão. Assim, a JE mensuraria os votos por meio da totalização e caberia ao controle externo obter evidência para emitir uma conclusão de que a totalização de votos realizada pela JE está em conformidade, em todos os aspectos relevantes, com o registro digital do voto emitido pelas urnas eletrônicas.

Propomos uma auditoria em que seria avaliada apenas a totalização dos votos. Os votos seriam recontados em sua totalidade de forma eletrônica a partir da cópia do RDV, realizada ainda na urna eletrônica, após o encerramento da votação devidamente criptografada por chave que apenas o controle externo teria.

Essa cópia poderia ser chamada de RDV Controle Externo (RDV-CE). O arquivo ficaria armazenado na urna e uma cópia dele seria transferida com os demais arquivos aos TRE através da gravação e transmissão da mídia de resultado. Além do RDV-CE também seria oportuno que TRE transferisse para o TCU o log das urnas, para a análise dos eventos pelo qual passaram as urnas (figura 9).

Figura 9 – Transmissão do RDV-TCU e Log das urnas ao TCU

Fonte: TSE, adaptado pelo autor

Embora o *log* das urnas não seja necessário para a recontagem dos votos, esses arquivos já são coletados na mídia de resultado e a análise dessas informações poderia ser realizada de forma automatizada, por meio de ferramentas de análise de dados, para detectar eventos como acionamentos indevidos da urna, tentativas de execução de aplicativos, testes realizados pelos partidos políticos, dentre outros, que poderiam sugerir incidentes relacionados a integridade das urnas eletrônicas. Assim, esses dados poderiam ser coletados nessa auditoria para uso na auditoria de verificação da integridade das urnas. Aranha (2018) destaca que o log pode ser adulterado caso o *software* esteja sob controle de terceiros e que não serviria como ferramenta de auditoria, todavia o que está sendo proposto não é que a auditoria seja concentrada nas informações do *log*, mas que ele seja coletado como uma ferramenta para indicar indícios de inconformidades. Haverá ainda outros procedimentos de auditoria na etapa seguinte do trabalho, como inspeção *in loco* de amostra das urnas eletrônicas, quando haveria a verificação de hash e do sistema de arquivos dos equipamentos.

Como as eleições são realizadas aos domingos e durante a totalização dos votos à restrição no uso das redes de dados pela JE, esses arquivos poderiam ser transferidos para o TCU na segunda-feira após o pleito. Os votos seriam totalizados de forma automatizada, a partir de ferramentas de análise de dados, gerando representações dos BU. No terceiro dia após a eleição o TSE divulga os BU no site daquele tribunal. Esses boletins do TSE seriam coletados e comparados com os BU gerados a partir

dos RDV-CE. Assim a totalização seria tanto em nível de BU, quanto nos totais gerais, o que facilitaria localizar fontes de divergência caso existam.

Os procedimentos desta auditoria seriam majoritariamente eletrônicos, devendo no levantamento anteriormente descrito ou no planejamento serem preparados, por exemplo, aplicativos que permitam a extração, preparação e o carregamento desses dados para a análise. Essa fiscalização deveria ocorrer após cada turno das eleições.

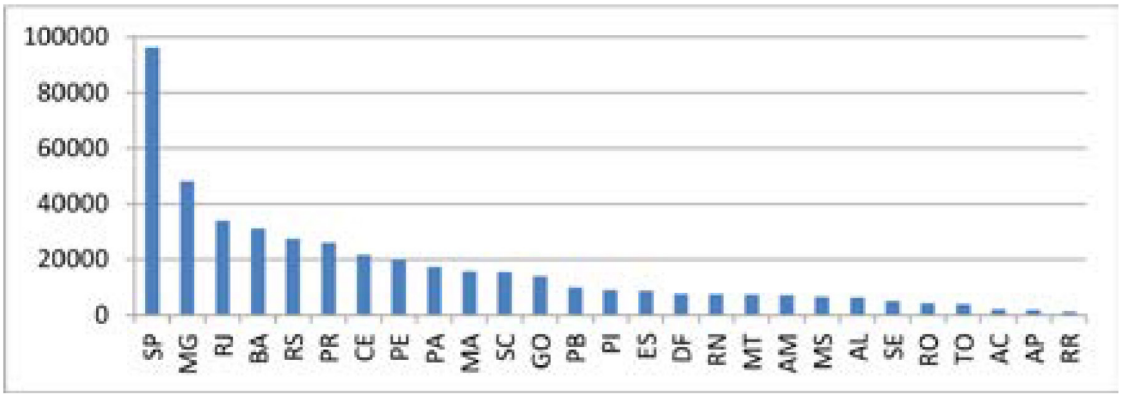
Também poderia ser gerada uma segunda cópia do RDV nas urnas eletrônicas, dessa vez criptografada pelo TSE e pelo TCU, para que, em caso de divergência dos dados da JE e do controle externo, esse arquivo, que somente poderia ser descriptografado conjuntamente, servisse como referência para validar os votos. Isso permitiria uma definição dos votos caso houvesse divergências.

O resultado dessa auditoria seria uma opinião sobre a totalização de votos indicando que a totalização realizada pela JE está ou não livre de distorções relevantes com os votos registrados por meio dos RDV nas urnas eletrônicas. Como esse processo seria eletrônico, acreditamos que poderia ser possível que o TCU apreciasse a auditoria a partir da quarta-feira da semana seguinte às eleições. Essa tempestividade traria confiança ao processo eleitoral.

4.5 Auditoria para verificar a integridade das urnas eletrônicas após votação

Essa seria uma auditoria desafiadora. Nas eleições de 2018 existiram mais de 450 mil seções eleitorais (gráfico 1) com cada uma delas utilizando urnas eletrônicas. Analisar in loco a totalidade das urnas seria uma tarefa praticamente impossível. Para essa auditoria seria utilizada amostragem estatística e coletando evidências sobre a integridade dos equipamentos.

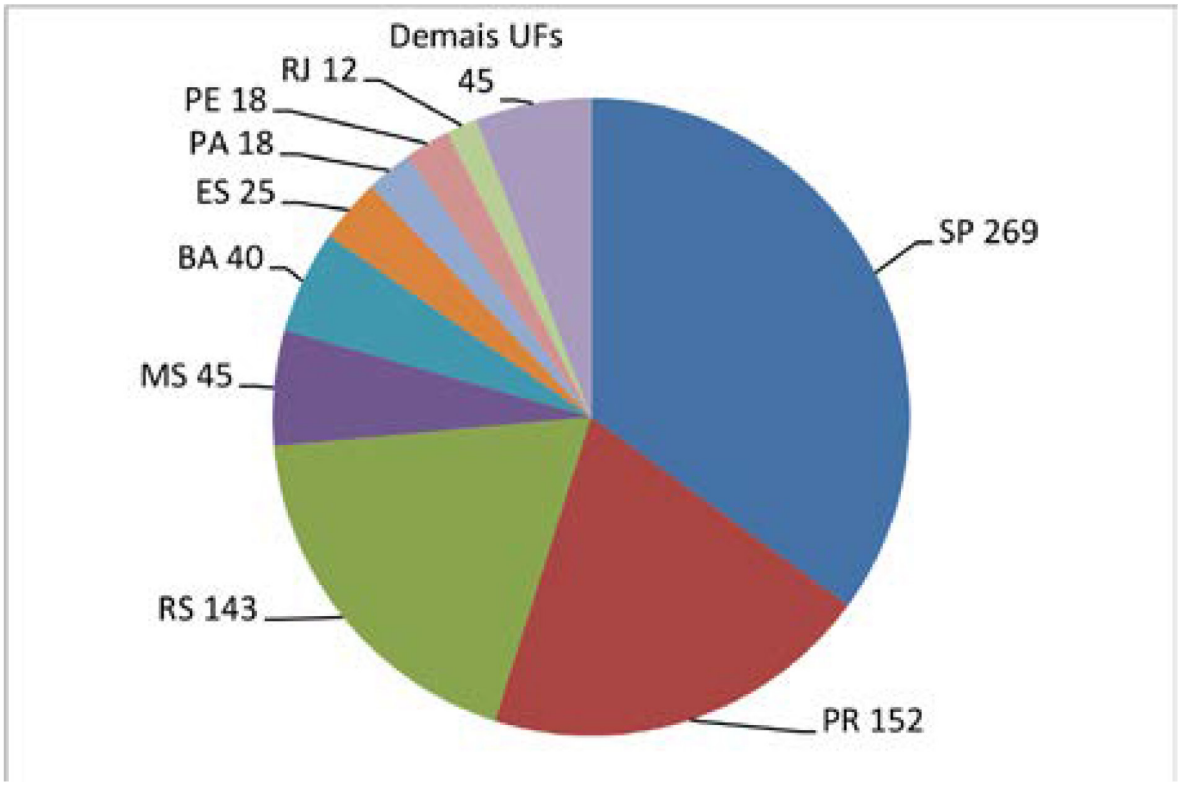
Gráfico 1 – Seções eleitorais por UF



Fonte: TSE adaptado pelo autor.

Destaca-se que parte dos TRE utilizam depósitos de urnas centralizados, havendo poucas instalações em um estado como o Amazonas com um depósito ou Minas Gerais com dois depósitos. Já em outros estados há depósitos em diversas zonas eleitorais, com São Paulo tendo depósitos em 269 municípios, Paraná e Rio Grande do Sul têm, cada um, mais de 140 municípios com depósitos de urnas eletrônicas (gráfico 2). Essas informações foram obtidas a partir do Anexo IIIA, do Edital da Licitação-TSE n. 106/2017, que tinha como objeto a aquisição de conjuntos de impressão de votos (BRASIL. TRIBUNAL SUPERIOR ELEITORAL, 2017a) e previa a entrega dos conjuntos de impressão nos locais onde são armazenadas as urnas eletrônicas.

Gráfico 2 – Quantidade de municípios por UF com depósitos de urnas

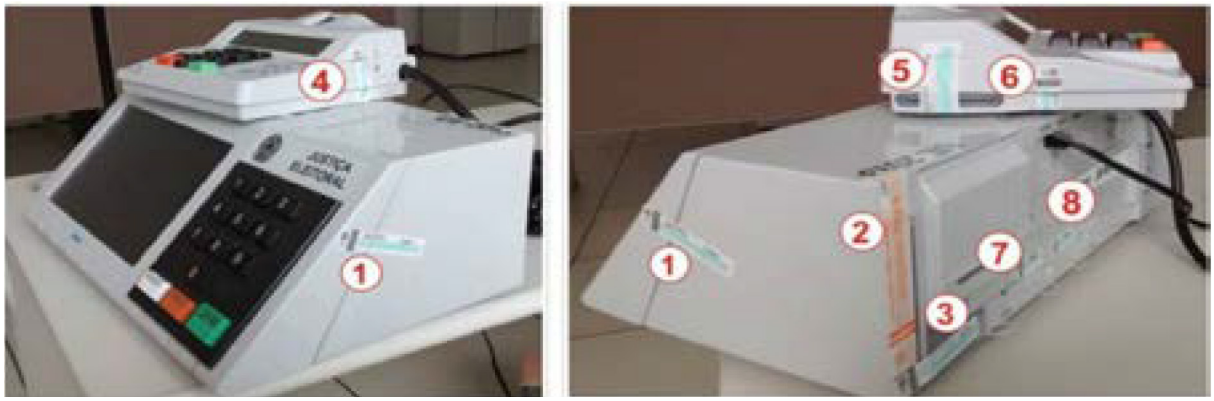


Fonte: TSE adaptado pelo autor.

A integridade física da urna é mantida por lacres físicos, que são emitidos pela Casa da Moeda do Brasil e assinados por Juiz Eleitoral. Quanto à integridade lógica, os arquivos são assinados digitalmente e há contingências nos aplicativos para que essas assinaturas sejam verificadas em cascata quando da ativação do equipamento e execução dos arquivos, além da criptografia de dados de alguns arquivos. No caso de haver fraudes nas urnas eletrônicas possivelmente haveria a quebra dessa integridade, de forma que a inspeção *in loco* dos equipamentos pode levar à detecção do fato.

Dessa forma, na auditoria proposta seria selecionada uma amostra estatisticamente representativa para avaliar os lacres físicos (figura 10), a integridade externa dos equipamentos bem como o *software*, nos quais poderiam ser analisados o *hash* dos arquivos e as assinaturas eletrônicas, além da presença de arquivos estranhos ao equipamento. O *hash* do RDV-CE gravado na urna seria comparado com o recebido pelo TCU e o *log* seria coletado para análise automatizada de eventuais eventos ocorridos após o encerramento da votação.

Figura 10 - Lacres físicos nas urnas eletrônicas



Fonte: TSE

De acordo com Angelini e Milone (1993) uma amostra é um subconjunto ou parte da população. Para que essa amostra seja representativa da população, deve-se selecionar os elementos de forma aleatória, com todos os elementos da população tendo a mesma chance de participar da amostra, bem como deve-se buscar minimizar o erro amostral. Para estabelecer o tamanho da amostra necessária para essa auditoria poderia ser utilizada a fórmula para determinação de amostras em populações infinitas (NATIONAL AUDIT OFFICE, 2001).

$$n = \frac{Z^2 \times (\hat{p} - \hat{q})}{E^2}$$

Onde:

n = número de indivíduos na amostra;

Z = intervalo de confiança

$\hat{p}$= proporção populacional dos indivíduos que pertencem a categoria avaliada

$\hat{q}$ = proporção populacional dos indivíduos que não pertencem a categoria avaliada (1- p)

E = erro amostral

Adotando um nível de confiança de 95% e um erro amostral de 3% seria obtida uma amostra de 1.068 urnas eletrônicas que deveriam ser analisadas. Para que todos os estados e o Distrito Federal fossem contemplados, poderia haver estratificação proporcional de acordo com a quantidade de seções eleitorais nas eleições de 2018 constantes nessas UF. Assim, o valor de 1.068 seria multiplicado pela proporção de urnas que a UF tinha em âmbito nacional e arredondado para o valor imediatamente superior, resultando em um total de 1.083 urnas. Para que os resultados das UF pudessem ser utilizados como referência estatística para o uso em auditorias futuras de amostragem estratificada de alocação ótima, sendo possível ter dados da variação da variável de interesse, seria adotada uma amostra mínima de quarenta urnas por UF para haver significância nos dados dos estados, resultando em uma amostra total de 1.481 urnas, conforme tabela 2.

Tabela 2 – Dados do tamanho da amostra

UF	Seções	Proporção de seções	Municípios com depósitos de urnas	Amostra estratificada	Amostra ajustada
SP	96.328	21,20%	269	227	227
MG	48.166	10,60%	2	114	114
RJ	33.901	7,46%	12	80	80
BA	31.192	6,86%	40	74	74
RS	27.274	6,00%	143	65	65
PR	26.136	5,75%	152	62	62
CE	21.449	4,72%	6	51	51
PE	19.797	4,36%	18	47	47
PA	17.286	3,80%	18	41	41
MA	15.830	3,48%	1	38	40
SC	15.562	3,42%	3	37	40
GO	13.995	3,08%	1	33	40
PB	9.955	2,19%	5	24	40
PI	8.930	1,97%	9	21	40
ES	8.724	1,92%	25	21	40
DF	7.476	1,65%	1	18	40

RN	7.389	1,63%	1	18	40
MT	7.247	1,59%	4	18	40
AM	7.017	1,54%	1	17	40
MS	6.529	1,44%	45	16	40
AL	6.387	1,41%	1	16	40
SE	5.137	1,13%	1	13	40
RO	4.181	0,92%	1	10	40
TO	3.832	0,84%	2	10	40
AC	1.924	0,42%	1	5	40
AP	1.632	0,36%	4	4	40
RR	1.172	0,26%	1	3	40
Total	454.448	100%	767	1.083	1.481

Fonte: do autor

Essa auditoria seria realizada quando as urnas eletrônicas estivessem armazenadas após o segundo turno para assegurar que após o uso nas eleições os equipamentos encontrar-se-iam com os lacres físicos devidamente intactos, com o *software* igual ao que foi assinado e lacrado digitalmente pelo TSE, sem arquivos estranhos ao sistema, bem como com o *log* sem indicativo de eventos anômalos. E confirmado, ainda, se os RDV recebidos pelo TCU são os mesmos armazenados nas urnas, assegurando a integridade dos arquivos recebidos durante a auditoria de certificação da totalização dos votos. Para isso equipes de auditorias iriam aos locais de armazenamento verificar, com programa a ser desenvolvido pelo próprio TCU, o *hash* e a estrutura de arquivos das urnas e copiado o *log* para análise.

Embora haja aplicativo na urna eletrônica que faça essa verificação, entendemos que nessa etapa poderia ser utilizado um aplicativo próprio para prevenir risco de que o programa fosse alterado na urna eletrônica para apresentar uma falsa conformidade. Atualmente nas normas do TSE há autorização para que partidos políticos utilizem programas próprios desde que homologados anteriormente por aquele tribunal.

As equipes de auditoria teriam que romper lacres físicos para a execução dos testes no *software* das urnas, devendo serem repostos ao final da análise, o que demandaria que o TCU obtivesse lacres conforme as especificações do TSE para essa etapa dos trabalhos, seja pela disponibilização pela JE ou pela Casa da Moeda. Como essa checagem seria realizada após o segundo turno das eleições não haveria o risco de alegações de que os procedimentos poderiam enfraquecer a segurança da votação eletrônica.

Em síntese as equipes de auditoria iriam aos locais de armazenamento de urnas, que podem estar em mais de 700 municípios, localizariam a urna eletrônica utilizada na seção

eleitoral selecionada na amostra, verificaria os lacres físicos e a integridade do gabinete da urna; romperia os lacres necessários à inclusão de pendrive com o aplicativo que seria executado para verificar as assinaturas digitais, *hash* e copiar o arquivo de *log* para o dispositivo de memória – poderia ser necessário instalar teclado na urna – e, por fim, colocaria novos lacres de acordo com o especificado pelo TSE, com assinatura do auditor. A coleta e transmissão dos dados das urnas avaliadas armazenados no pendrive seria de forma eletrônica devendo os arquivos serem analisados automaticamente.

Essa verificação in loco poderia ser acompanhada por servidor da JE. Caso houvesse evidências de inconformidades físicas as urnas deveriam ser fotografadas. A JE, o Ministério Público Eleitoral e a Polícia Federal deveriam ser comunicadas em caso de suspeita de fraude e a urna eletrônica com indícios de fraude deveria ser retida para perícia.

Parece-nos que para a análise das 1.481 urnas em um período de duas semanas seriam necessárias cerca de trinta equipes de auditorias (60 auditores). Considerando dez dias úteis de execução, cada equipe iria verificar cerca de cinquenta urnas no período, com uma média de quase cinco urnas por dia.

Nos locais em que o armazenamento fosse centralizado possivelmente os trabalhos das equipes ocorram em menos de uma semana, mas nos estados em que a amostra englobe vários municípios em que sejam verificadas poucas urnas em cada local o trabalho seria mais lento. Dessa forma, caso, por exemplo, uma equipe tenha de ir a diversos locais de armazenamento para analisar as urnas o tempo de deslocamento impactará na produtividade, por isso foi proposta uma estimativa conservadora da média de urnas analisadas por dia.

O resultado dessa auditoria seria uma conclusão, afirmando ou negando que a integridade física e lógica das urnas eletrônicas estão em conformidade em todos os aspectos relevantes com as características estabelecidas no momento da lacração física e eletrônica, que os RDV recebidos pelo controle externo são os mesmos presentes nas urnas e que não há eventos relevantes nos arquivos de log dos equipamentos que indiquem inconsistências.

4.6 Auditorias e o calendário eleitoral

A Lei n. 9.504/1997 define que a partir de seis meses antes das eleições todos os programas de computador de propriedade do TSE, utilizados nas urnas eletrônicas e nos computadores da JE para a votação eletrônica, poderão ter suas fases de especificação e de desenvolvimento acompanhadas pelos partidos políticos, pela OAB, pelo MP e por pessoas autorizadas em resolução específica, sendo que após concluídos serão apresentados para análise até vinte dias antes das eleições por essas entidades. Assim, uma auditoria no *software* deveria ter sua fase de execução prevista nesse período entre abril e setembro do ano em que houver eleições, para que a análise lógica

recaia sobre os aplicativos que efetivamente serão utilizados naquele pleito. O prazo final seria nesse último mês, setembro, para permitir a análise do *software* finalizado.

Nas Resoluções-TSE n. 23.550/2017 e 23.555/2017, podem ser observados momentos chave em que as auditorias sugeridas seriam realizadas. As eleições ocorrem em primeiro turno no primeiro domingo de outubro e em segundo turno no último domingo daquele mês. A JE deveria tornar os BU disponíveis na internet em até três dias após cada turno. E as urnas eletrônicas deveriam manter os lacres físicos e a memória intacta até 18/1/2019, desde que as informações contidas no equipamento não fossem objeto de discussão em processo judicial, caso em que os dados deveriam ser mantidos.

Nas eleições de 2018, o último dia para a diplomação dos eleitos foi 19/12/2018. Assim, para obter-se tempestividade nas opiniões e conclusões das auditorias, as fiscalizações deveriam ser programadas para serem apreciadas pelo TCU até a última seção antes do recesso do tribunal, de forma que os acórdãos fossem prolatados antes da diplomação dos candidatos pela JE.

A definição da extensão do período de execução das auditorias seria influenciada pelos produtos do levantamento inicialmente proposto. Como mencionado, nesse levantamento deveriam ser desenvolvidos aplicativos que seriam utilizados na urna eletrônica para gerar e criptografar o RDV-CE na urna eletrônica, bem como os programas que seriam usados internamente para o tratamento desses RDV-CE realizando a recontagem dos votos. Também como produto da primeira fiscalização estaria o aplicativo que seria executado para verificar a integridade lógica das urnas eletrônicas, que inclusive deveria ser homologado pelo TSE antes das eleições.

Tabela 3 – Cronograma de auditorias

Período	Auditoria no software e hardware	Auditoria para certificar a totalização	Auditoria para verificar a integridade das urnas eletrônicas
Abril - Set	A execução deveria iniciar dentro desse período, com a conclusão ocorrendo no final de setembro com a verificação dos aplicativos lacrados digitalmente.		

Outubro Semana seguinte ao 1º Turno	Início da fase de relatório	Execução da auditoria do 1º turno, com recepção dos RDV-CE e logs no primeiro dia após a votação, comparação com os BU no terceiro dia após o pleito e elaboração relatório.	
Outubro 2ª Semana após 1º turno	Relatório	Apreciação da auditoria do 1º turno pelo TCU	
Outubro última semana	Conclusão do relatório	Execução da auditoria do 2º turno e elaboração relatório.	
Novembro 1ª Semana	Início da análise da auditoria pelo Min. Relator	Apreciação da auditoria do 2º turno pelo TCU	Início da execução da auditoria nos locais de armazenamento
Novembro 2ª Semana	Análise da auditoria pelo Min. Relator	Final da execução da auditoria nos locais de armazenamento	
Novembro 3ª Semana	Análise da auditoria pelo Min. Relator	Elaboração e conclusão de relatório.	
Novembro 4ª Semana	Análise da auditoria pelo Min. Relator	Início da análise da auditoria pelo Min. Relator.	
Dezembro 1ª semana	Análise da auditoria pelo Min. Relator	Análise da auditoria pelo Min.	
Dezembro 2ª semana	Apreciação da auditoria do 2º turno pelo TCU	Apreciação da auditoria do 2º turno pelo TCU	
Dezembro 3ª semana	Diplomação dos candidatos eleitos (em 2018 o prazo final foi dia 19 de dezembro)		
Janeiro dia 16	Último dia que os TRE devem manter a integridades das urnas eletrônicas		

Fonte: Resoluções-TSE n. 23.550/2017 e 23.555/2017, adaptado pelo autor

Esse cronograma (tabela 3) seria viável se não houvesse impropriedades nas eleições, com as fiscalizações ratificando a lisura da votação eletrônica. Caso houvesse evidências no sentido oposto à regularidade do processo seria necessário, observar o contraditório e a ampla defesa, o que estenderia esses prazos. Além disso, nas eleições de 2018, havia previsão normativa da integridade das urnas ser mantida até o dia 17

de janeiro de 2019, quando os lacres físicos poderiam ser retirados e os equipamentos formatados, à exceção dos equipamentos objeto de discussão judicial. Dessa forma, as urnas selecionadas na amostra teriam que ser avaliadas, no máximo, até meados de janeiro caso não fosse possível cumprir os prazos estimados.

5. Considerações finais

A partir da revisão bibliográfica e documental observou-se a existência de diretrizes internacionais para a realização de eleições eletrônicas. O trabalho deu ênfase nas orientações do Conselho da Europa constantes da Recomendação CM/Rec(2017)5 e do Comitê de Assistência Eleitoral dos Estados Unidos. Entendemos que o TSE atende em grande parte as diretrizes europeias e americanas relacionadas à votação eletrônica, entretanto, diferente do que ocorre em outros países, o Tribunal Superior é proprietário do projeto da urna eletrônica e desenvolve o *software* do dispositivo. Talvez seja por isso que não há uma preocupação na realização de testes e certificações externas, uma vez que o órgão detém o conhecimento da urna eletrônica. Mas essa centralização leva a lacunas em diretrizes relacionadas à transparência e observação e *accountability*, que poderiam ser supridas pela atuação de controle externo.

Estes dados confirmam uma das hipóteses iniciais: assimetria de informações. O TSE desenvolveu inicialmente o projeto da urna eletrônica, em 1996, por meio de um grupo composto por pessoal da JE, das Forças Armadas, do Ministério da Ciência e Tecnologia, do Instituto Tecnológico de Aeronáutica, do Instituto Nacional de Pesquisas Espaciais e do Ministério das Comunicações. Nos anos seguintes, o órgão ganhou uma grande expertise no tema, todavia, houve a concentração das informações no TSE. Em que pese haver auditorias e testes de segurança, os resultados dessas avaliações são controlados ou mesmo realizados pela JE, de forma que a sociedade depende quase absolutamente da JE como fonte de informações sobre a votação eletrônica.

Assim, entendemos que a atuação do controle externo poderia atender às diretrizes relacionas à transparência e à accountability do processo, além de identificar e avaliar riscos de fraudes no processo, reduzindo a assimetria de informações. O TCU poderia atuar, por meio de auditoria, para verificar o hardware e o software utilizados na votação eletrônica, na recontagem dos votos a partir dos RDV gerados pelas urnas eletrônicas e verificando, ao final das eleições, a integridade dos equipamentos, buscando evidências da materialização de eventuais riscos de fraudes nos dispositivos.

Para que essas auditorias possam ocorrer, seria desejável a realização de levantamento prévio que avaliasse a viabilidade desses trabalhos em especial pela necessidade de desenvolvimento de aplicativos que possam interagir com as urnas eletrônicas para permitir a coleta dos RDV, bem como a verificação da integridade e da autenticidade

do software nos equipamentos. Também, nesse levantamento, deveria ser definida uma estratégia para a verificação in loco das urnas eletrônicas, a qual poderia ocorrer por meio de auditoria coordenada com Tribunais de Contas Estaduais, em especial nos estados com depósito de urnas em vários municípios.

Possivelmente, caso o TCU realizasse esse papel de organização independente e competente auditando a votação eletrônica, haveria uma demanda da sociedade para manter o conjunto de auditorias nas eleições gerais, que ocorrem a cada dois anos, bem como nas eleições suplementares que acontecem quando candidatos eleitos em eleições majoritárias são cassados pela JE. Dessa forma, o tribunal poderia prever em seu planejamento estratégico essa atuação nas eleições.

Destaca-se, ainda, que as auditorias propostas neste trabalho correspondem a uma possibilidade de atuação do controle externo frente à votação eletrônica. Podendo outros estudos definir auditorias diversas ou mesmo buscar definir como entidade de fiscalização independente organizações do setor privado, que poderiam realizar esse trabalho de auditoria externa.

Assim foram analisadas boas práticas internacionais relacionadas à votação eletrônica, comparando-as com a legislação eleitoral, o que permitiu a definição de auditorias que poderiam ser realizadas pelo controle externo para assegurar a confiabilidade e a segurança das eleições. As ações de fiscalização propostas iriam garantir que os votos dos eleitores são devidamente coletados e contados, e buscaria verificar a materialização de fraudes nas urnas eletrônicas. Os objetivos específicos deste trabalho foram atingidos com a descrição de diretrizes internacionais relacionadas à votação e eletrônica e de processos de trabalho da JE no referencial teórico, bem como com a definição de auditorias e a sugestão de um calendário para a execução das ações de fiscalização na parte de discussão de resultados do presente trabalho.

5.1 Resposta à questão problema

A presente monografia teve como objetivo geral analisar o uso da votação eletrônica de modo a responder a seguinte questão problema: **Quais ações um órgão independente poderia utilizar na votação eletrônica para assegurar que os votos dos eleitores são devidamente registrados e totalizados pela Justiça Eleitoral?**

A resposta a esta questão foi apresentada a partir da descrição de três auditorias que em conjunto trariam uma asseguração razoável que os votos dos eleitores seriam registrados e gravados na urna eletrônica com integridade e segurança; que a totalização de votos realizada pela JE estaria correta certificando os resultados da votação com a recontagem dos votos a partir dos RDV das urnas eletrônicas; e que as urnas eletrônicas permaneceriam fisicamente íntegras não havendo arquivos estranhos ou adulterados no dispositivo.

5.2 Sugestões de estudos futuros

O tema não foi esgotado nesta pesquisa, a qual pode ser continuada por meio de estudos futuros. A seguir, algumas questões que podem ser objeto de investigação e aprofundamento:

- Há possibilidade de analisar os BU para que a partir das informações dos locais de votação e dos resultados das seções eleitorais se obtivessem padrões que pudessem identificar fraudes?

- Quais vantagens e desvantagens na utilização do voto impresso como trilha de auditoria frente aos riscos de adulteração ou subtração dos registros impressos?

Referências Bibliográficas

ANGELINI, F.; MILONE, G. Estatística Geral. São Paulo: Atlas, 1993.

ARANHA, D. F. et al. Execução de código arbitrário na urna eletrônica brasileira. Anais do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), Outubro 2018. 57-70. Disponível em: <http://portaldeconteudo.sbc.org.br/ index.php/sbseg/article/view/4243/4174>. Acesso em: 4 jan. 2019.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Normas de Auditoria do Tribunal de Contas da União, revisão junho de 2011. Brasília: TCU, 2011. Disponível em: <https://portal.tcu.gov.br/controle-externo/normas-e-orientacoes/normas-de-fiscalizacao/ nat.htm>. Acesso em: 18 dez 2018.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Resolução-TCU n. 246/2011. Regimento Interno do Tribunal de Contas da União. Brasília: TCU, 2012. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D7BC0B4014 D7E1FB1A622B4>. Acesso em: 18 de dezembro de 2018.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Portaria-Segecex n. 24/2018. Aprova o Roteiro de Levantamento com vistas a orientar a condução da fiscalização prevista no art. 238 do Regimento Interno a cargo das unidades técnicas do TCU. Brasília: TCU, 2018a. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId= 8A81881F65AAE41501660DA0750900D4. Acesso em: 19 dez. 2018.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Referencial de combate a fraude e corrupção: aplicável a órgãos e entidades da Administração Pública. 2ª. ed. Brasília: TCU, 2018b. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp? fileId=8A81881E66FA07210167099C7DE52B8F>. Acesso em: 28 nov. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Edital de Licitação-TSE n. 106/2017. Brasília. 2017a. Anexo IIA - Locais de armazenamento. Disponível em: <http://www.tse.jus.br/silic/pages/internet/licitacao/licitacoes-concluidas>. Acesso em: 19 dez. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Resolução n. 23.550/2017. Brasília. 2017b. Disponível em: < http://www.tse.jus.br/legislacao-tse/res/2017/RES235502017.html >. Acesso em: 18 dez. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Resolução n. 23.552/2017. Brasília. 2017c. Disponível em: < http://www.tse.jus.br/legislacao-tse/res/2017/RES235522017.html >. Acesso em: 18 dez. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Resolução n. 23.554/2017. Brasília. 2017d. Disponível em: < http://www.tse.jus.br/legislacao-tse/res/2017/RES235542017.html >. Acesso em: 18 dez. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Resolução n. 23.555/2017. Brasília. 2017e. Disponível em: < http://www.tse.jus.br/legislacao-tse/res/2017/RES235552017.html >. Acesso em: 18 dez. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Glossário Eleitoral. Brasília: TSE, 2018a. Disponivel em: <http://www.tse.jus.br/eleitor/glossario/glossario-eleitoral>. Acesso em: 18 dez. 2018.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Código eleitoral anotado e legislação complementar. 13ª Edição. ed. Brasília: TSE, 2018b. 1200 p.

BRASIL. TRIBUNAL SUPERIOR ELEITORAL. Seminário no TSE debate mitos e verdades sobre a urna eletrônica. You Tube, 2018c. Disponivel em: <https://www.youtube. com/watch?v=t21m-H24jD8>. Acesso em: 20 dez. 2018.

CONSELHO DA EUROPA. Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. Council of Europe. Estraburgo, p. 23. 2017a. Disponível em: < https://rm.coe.int/1680726c0b%20>. Acesso em 13 set. 2018.

CONSELHO DA EUROPA. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting. Council of Europe. Estraburgo, p. 7. 2017b. (CM/Rec(2017)5). Disponível em: < https://rm.coe.int/0900001680726f6f>. Acesso em 13 out. 2018.

CONSELHO DA EUROPA. Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for evoting. Council of Europe. Estraburgo, p. 19. 2017c. (CM/Rec(2017)5). Disponível em: <http://rm.coe.int/ 090000168071bc84>>. Acesso em 13 out. 2018.

GOLDSMITH, B.; RUTHRAUFF, H. Implementing and Overseeing Electronic Voting and Counting Technologies. Washington: [s.n.], 2013. 310 p. Disponível em: <https://www.ndi.org/sites/default/files/Implementing_and_Overseeing_Electronic_Voting_ and_Counting_Technologies.pdf >>. Acesso em 13 out. 2018.

GOMES, A. R. Auditoria Baseada em Risco. Instituto Serzedello Corrêa. Brasília. 2017. Notas de aula.

HOQUE, Z. (Ed.). Methodological Issues in Accounting Research: Theories, Methods and Issues. Londres: Spiramus Press, 2006.

INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE. Use of E-Voting Around the World, 2015. Disponivel em: <https://www.idea.int/newsmedia/media/use-e-voting-around-world>. Acesso em: 13 out. 2018.

INTOSAI - INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS. ISSAI 100. Tradução de TCU. Viena: [s.n.], 2006.

MARCELO, A.; PEREIRA, M. A arte de hackear pessoas. Rio de Janeiro: Brasport, 2005.

NATIONAL AUDIT OFFICE. A practical sampling guide. Londres: [s.n.], 2001. Disponivel em: <https://www.nao.org.uk/wp-content/uploads/2001/06/SamplingGuide.pdf>. Acesso em: 20 dez 2018.

NETO, A. A. D. C. Fundamentos de auditoria do setor público. Brasília. 2017. Notas de aula.

PRANDINI, M.; RAMILLI, M. A Model for E-voting Systems Evaluation Based on International Standards: Definition and Experimental Validation. E-Service Journal, Bloomington, 8, n. 3, 2012. 42–72.

SILVA, E. L. D.; MENEZES, E. M. Metodologia da pesquisa e elaboração de dissertação. 4. ed. rev. atual. ed. Florianópolis: UFSC, 2005. 138 p. Disponível em < https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_diss ertacoes_4ed.pdf >. Acesso em: 13 out. 2018.

SOUZA, M. B. M. Manual para apresentação do trabalho acadêmico e técnico-científico. 2. ed. ed. Brasília: Edições Câmara, 2010. 147 p. Disponível em < http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/1923/manual_%20 trabalho_academico _souza_2ed.pdf?sequence=1>. Acesso em: 13 out. 2018.

U.S. ELECTION ASSISTANCE COMMISSION. Voluntary Voting System Guidelines Version 1.1. Silver Spring, MD: [s.n.], v. 1 Voting System Performance Guidelines, 2015a. Disponível em <https://www.eac.gov/assets/1/28/VVSG.1.0_Volume_1.PDF>. Acesso em 13 out. 2018.

U.S. ELECTION ASSISTANCE COMMISSION. Voluntary Voting System Guidelines Version 1.1. Silver Spring, MD: [s.n.], v. 2 National Certification Testing Guidelines, 2015b. Disponível em < https://www.eac.gov/assets/1/28/VVSG1.0Vol.2.PDF>. Acesso em 13 out. 2018.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE. Federal Information System Controls Audit Manual (Fiscam). Washignton: [s.n.], 2009 Disponível em < https://www.gao.gov/assets/80/77142.pdf>. Acesso em 4 jan. 2019.

VAN DE GRAAF, J. O mito da urna: desvendando a (in)segurança da urna eletrônica. versão 1.1. ed. Belo Horizonte: [s.n.], 2018 Disponível em < https://inscrypt.dcc.ufmg.br/wpcontent/uploads/2017/11/o-mito-da-urna-1-1.pdf >. Acesso em 13 out. 2018.

Instituto Serzedello Corrêa

Missão

Aprimorar a Administração Pública em benefício da sociedade por meio do controle externo

Visão

Ser referência na promoção de uma Administração Pública efetiva, ética, ágil e responsável

TRIBUNAL DE CONTAS DA UNIÃO

tcu.gov.br/isc