



Tribunal Regional Eleitoral
do Rio Grande do Sul



SISTEMA ELETRÔNICO DE VOTAÇÃO E DE APURAÇÃO

SEGURANÇA DA INFORMAÇÃO E FISCALIZAÇÃO PELA SOCIEDADE



Tribunal Regional Eleitoral
do Rio Grande do Sul

SISTEMA ELETRÔNICO DE VOTAÇÃO E DE APURAÇÃO

SEGURANÇA DA INFORMAÇÃO E FISCALIZAÇÃO PELA SOCIEDADE

ABRIL/2022

As Eleições Gerais de 2022 são o novo desafio da Justiça Eleitoral brasileira.



Desembargador Jorge Luís Dall'Agnol

Embora o problema do nosso século seja muito maior do que escolher os representantes políticos, é durante as eleições que colocamos em xeque questões essenciais sobre cultura política, educação e informação, ou, melhor dizendo, atualmente, os maiores desafios são sobre a desinformação.

Há alguns anos, quando os novos meios de comunicação não passavam de um sonho nas mentes de homens de gênio, acreditava-se que, se houvesse algum dia algo como a Internet, ninguém teria sequer a chance de ser mal-informado, pois todo o conhecimento do mundo estaria confortavelmente disponível a qualquer um. Evoluímos e parece que as expectativas foram frustradas. O que menos esperávamos é exatamente o que se tornou realidade e o excesso de informação converteu-se prejudicial no século em que tudo passou a ser *fast*.

Entretanto, a responsabilidade por uma má escolha política não pode ser tratada como a descuidada escolha de uma refeição rápida do final de semana. A má digestão de escolhas políticas ruins dura muito mais do que alguns dias, podendo ter impacto superior a 4 anos e com consequências muito mais graves. E, por isso, o excesso de informação, quando direcionado a colocar em dúvida ou a alterar o comportamento do eleitorado, é tão desastroso para uma democracia.

Desse modo, um dos maiores desafios neste novo ambiente de excesso de informação passou a ser produzir-se materiais educativos/informativos que não sejam apenas úteis, mas que antes e, sobretudo, sejam lidos. Na sociedade em que se espera que refeições fiquem prontas em 5 minutos, para que sejam ingeridas em tempo ainda menor, proporcionar conhecimento sobre eleições e tecnologia cuja alienação por parte do eleitorado pode gerar consequências por anos, torna-se muito mais que importante. Passa a ser essencial.

Tendo tudo isso em mente, a Comissão de Enfrentamento à Desinformação do TRE-RS em parceria com a Coordenadoria de Gestão da Informação (COGIN) produziu a presente cartilha sobre o Sistema Eletrônico de Votação e sobre o que um eleitor precisa saber para entender e fiscalizar o processo eleitoral brasileiro, no que diz respeito às urnas eletrônicas e todos os sistemas e procedimentos que a circundam.

Trata-se de um texto leve, com a apresentação de muitos conceitos técnicos que podem servir de tábua de salvação, útil quando se perceber que alguém esteja tentando afogá-lo no mar de desinformações sobre o tema.

Sua leitura pode ser feita aos poucos, por temas, bem como pode servir de material de consulta quando surgir aquela dúvida pontual. O tempo de leitura é sempre inferior ao de uma refeição do tipo fast, mas providenciamos que o material esteja carregado de bons nutrientes, aptos a fazer com que nossa democracia prospere, forte e saudável.

Esperamos que esta cartilha seja muito mais do que apenas útil. Esperamos que ela seja lida e compartilhada por todos que tenham interesse em transformar cidadãos - de meros eleitores a agentes da democracia, que divulgam a verdade sobre o sistema e sobre o seu funcionamento.

Fica o meu convite. Saboreiem informação de qualidade. Leiam e compartilhem. Garantam a todos os amigos e familiares os bons nutrientes da boa informação e evitem a intoxicante desinformação.

Desejo a todos uma excelente leitura, muitas reflexões e um profícuo processo eleitoral para as eleições de 2022.

Desembargador Jorge Luís Dall’Agnol,

Presidente da Comissão de Enfrentamento à Desinformação do TRE-RS

CONTEÚDO

INTRODUÇÃO	7
UM PROCESSO EM CONSTANTE EVOLUÇÃO.....	9
ASPECTOS JURÍDICOS DO SISTEMA.....	10
DE VOTAÇÃO INFORMATIZADO	10
RESOLUÇÃO TSE Nº 23.673/2021	10
URNA ELETRÔNICA E SEU <i>SOFTWARE</i>	12
ASSINATURA DIGITAL, REGISTRO DIGITAL.....	13
DO VOTO - RDV E <i>HASH</i>	13
AUDITORIA EXTERNA NO DESENVOLVIMENTO	15
DA PROGRAMAÇÃO DOS SISTEMAS	15
TESTE PÚBLICO DE SEGURANÇA	16
LACRAÇÃO DOS SISTEMAS	18
INSTALAÇÃO DO PROGRAMA E CONECTIVIDADE DAS URNAS	21
CRIOGRAFIA	22
VERIFICAÇÃO DOS SISTEMAS ELEITORAIS NA CERIMÔNIA DE GERAÇÃO DE MÍDIAS ...	23
MECANISMOS DE FISCALIZAÇÃO DOS	24
SISTEMAS ELEITORAIS.....	24
TESTE DE INTEGRIDADE DAS URNAS ELETRÔNICAS	26
ZERÉSIMA E VOTOS EM <i>BACKUP</i>	28
VOTAÇÃO COM IDENTIFICAÇÃO BIOMÉTRICA DO ELEITOR	29
REGISTRO DIGITAL DO VOTO (RDV)	30
GRAVAÇÃO DOS DADOS E EMISSÃO DO BU	31
TRANSMISSÃO DOS VOTOS	32
APURAÇÃO DOS RESULTADOS	33

INTRODUÇÃO

A ideia de uma máquina de votar não é nova no Brasil. O art. 58, § 15º do Código Eleitoral de 1932, nosso primeiro Código Eleitoral, aprovado pelo Decreto-Lei nº 21.076, de 24 de fevereiro de 1932, regulava o procedimento antes mesmo da existência de um protótipo de urna, prova da vocação tecnológica da Justiça Eleitoral.

Código Eleitoral de 1932

Art. 58, § 15º: Nas seções eleitorais onde se use a máquina de votar, serão observadas estas regras:

- a) o voto é dado na máquina, dispensando-se a cédula;*
- b) é obrigatório o registro dos candidatos até cinco dias antes da eleição;*
- c) a máquina estará preparada de modo que cada eleitor não possa votar, no primeiro turno, em mais de um nome, e só o possa, no segundo, até o número de lugares a preencher.*

Entre a previsão legal de uma máquina de votar e a transformação da ideia em realidade se passaram muitos anos. A primeira urna não foi eletrônica, era um projeto mecânico, de 35 kg, concebido em 1958 por Sócrates Puntel, que funcionava por meio de algumas teclas e duas régua. Contudo, em razão de suas dimensões, nunca teria sido utilizada.



Por todo o período em que utilizamos a votação por meio de cédulas de papel, várias foram as modalidades de fraudes realizadas. A necessidade de se criar um método ou procedimento para garantir a lisura do pleito e dos seus resultados tornou-se uma meta nacional.

Com a reabertura democrática, foi dado o primeiro passo nesse sentido quando, em 1986, a Justiça Eleitoral deu início ao processo de digitalização das eleições, realizando o cadastramento informatizado de milhões de eleitores.

Em 1994 ocorreu no Tribunal Superior Eleitoral a primeira totalização de eleições gerais feitas por um computador central. Em 1995, enfim, surge o primeiro protótipo de urna eletrônica brasileira, uma iniciativa que mudaria para sempre a nossa democracia. Em 1996 tivemos as primeiras eleições utilizando urnas eletrônicas e, em 2000, pela primeira vez na história, tivemos uma eleição completamente informatizada, em todas as suas etapas.

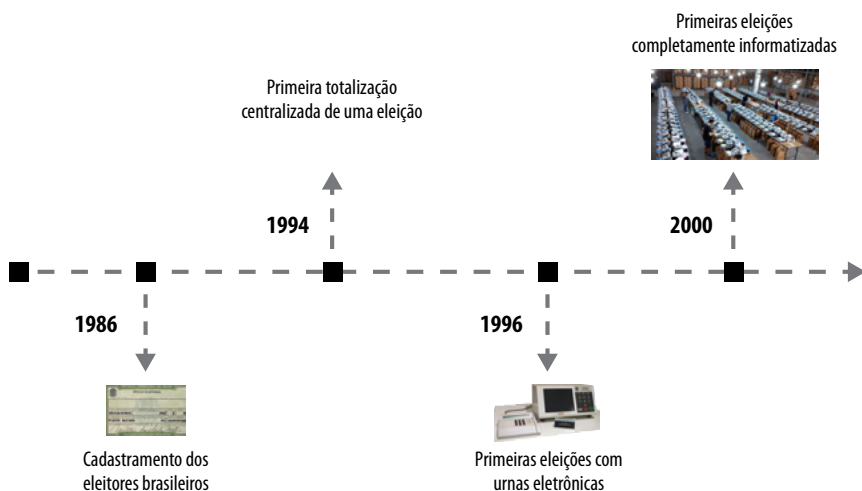
UM PROCESSO EM CONSTANTE EVOLUÇÃO



Desde a nossa primeira eleição utilizando urnas eletrônicas até os dias atuais, muitas coisas mudaram. O processo evoluiu muito. O processo eletrônico de votação evoluiu para ser informatizado em todas as suas fases, ainda assim, é regido por regras compreensíveis a qualquer um do povo, transparentes e completamente auditável.

Para responder às dúvidas mais comuns sobre o Sistema Eletrônico de Votação brasileiro apresentamos este material, o qual esperamos que sirva para dissuadir as principais desinformações sobre o assunto.

Linha do tempo - informatização do processo eleitoral



ASPECTOS JURÍDICOS DO SISTEMA DE VOTAÇÃO INFORMATIZADO

Os aspectos relacionados aos procedimentos de fiscalização e auditoria do sistema eletrônico de votação são regidos atualmente pela Res. TSE nº 23.673/2021. Essa Resolução é responsável por detalhar por quem, como e quando o processo, em todas as suas etapas, poderá ser fiscalizado para garantir transparência e lisura aos resultados das eleições brasileiras.

RESOLUÇÃO TSE Nº 23.673/2021

Em que pese ser repleta de informações técnicas, muitas vezes inacessíveis para a maioria dos eleitores, há um ponto essencial na Resolução TSE



23.673/2021 que não deveria fugir ao conhecimento de nenhum cidadão brasileiro. Ele diz respeito às instituições que, por lei, são fiscais naturais do processo, as quais têm o dever de acompanhar amplamente o processo eleitoral em eleições gerais ou municipais.

Resolução TSE. 23.673/2021

Art. 6º Para efeito dos procedimentos previstos nesta Resolução, salvo disposição específica, são consideradas entidades fiscalizadoras, legitimadas a participar das etapas do processo de fiscalização:

- I - Partidos Políticos, federações e coligações;*
- II - Ordem dos Advogados do Brasil;*
- III - Ministério Público;*
- IV - Congresso Nacional;*
- V - Supremo Tribunal Federal;*
- VI - Controladoria-Geral da União;*
- VII - Polícia Federal;*
- VIII - Sociedade Brasileira de Computação;*
- IX - Conselho Federal de Engenharia e Agronomia;*
- X - Conselho Nacional de Justiça;*
- XI - Conselho Nacional do Ministério Público;*
- XII - Tribunal de Contas da União;*
- XIII - Forças Armadas;*
- XIV - Confederação Nacional da Indústria, demais integrantes do Sistema Indústria e entidades corporativas pertencentes ao Sistema S;*
- XV - Entidades privadas brasileiras, sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao TSE; e*
- XVI - Departamentos de tecnologia da informação de universidades credenciadas junto ao TSE.*

Assim, qualquer um que queira questionar o processo eleitoral brasileiro pode se aproximar das instituições listadas acima e apresentar suas dúvidas e pedidos de providências, além de, é claro, fazer isso diretamente à Justiça Eleitoral.

URNA ELETRÔNICA E SEU SOFTWARE



A preparação do programa que rodará na urna eletrônica dura praticamente um ciclo inteiro entre eleições: encerrada a apuração de um plei-

O trabalho para manter o sistema é ininterrupto

to, a STI (Secretaria de Tecnologia da Informação) do TSE começa a planejar as mudanças que deverão ser implementadas na próxima votação. O obje-

tivo é atualizar o programa para atender novas demandas por segurança, sugestões de melhoria colhidas ao longo do processo eleitoral findo e instruções normativas do próprio tribunal (resoluções do TSE).

ASSINATURA DIGITAL, REGISTRO DIGITAL DO VOTO - RDV E HASH

Tais procedimentos para a aferição da segurança do processo eleitoral não são os únicos mecanismos desenvolvidos pela Justiça Eleitoral. A urna eletrônica utiliza o que há de mais moderno quanto às tecnologias de criptografia, assinatura digital e resumo digital dos votos.

Toda essa tecnologia é utilizada pelo *hardware* e pelo *software* da urna eletrônica para criar uma cadeia de confiança, garantindo que somente o programa desenvolvido pelo TSE, gerado durante a Cerimônia de Lacração dos Sistemas Eleitorais, possa ser executado nos equipamentos devidamente certificados pela Justiça Eleitoral.

Qualquer tentativa de executar *software* não autorizado na urna eletrônica resulta no bloqueio do seu funcionamento. De igual modo, tentativas de executar o *software* oficial em um *hardware* não certificado resultam no cancelamento da execução do aplicativo.

Res. TSE nº 23.673/2021

Art. 2º, I - assinatura digital: é uma forma eletrônica de garantir a autenticidade de um documento ou sistema. Para isso, são utilizadas operações matemáticas com algoritmos de criptografia assimétrica que atestam sua origem. A criptografia assimétrica faz uso de pares de chaves: chaves públicas, que podem ser amplamente disseminadas; e chaves privadas, que são conhecidas apenas pelo proprietário;

...

Art. 2º, XI - Registro Digital do Voto (RDV): arquivo gerado pela urna eletrônica, no qual os votos são gravados separados, por cargo, e ordenados aleatoriamente;

...

Art. 2º, XII - resumo digital (hash): pequena sequência de caracteres gerada por um cálculo matemático a partir de um conjunto de dados (arquivos, relatórios), que permite identificá-los de forma inequívoca. Qualquer alteração no arquivo original implica a geração de novo resumo digital.

A URNA ELETRÔNICA É VULNERÁVEL A ATAQUES EXTERNOS?

A urna eletrônica não é vulnerável a ataques externos, pois ela funciona de forma isolada, sem qualquer *hardware* ou *software* que possibilite sua conexão de forma que não seja local. Vale destacar que o sistema operacional Linux contido na urna é preparado pela Justiça Eleitoral de forma a não incluir nenhum mecanismo de *software* que permita a conexão com redes ou o acesso remoto. Além disso, as mídias utilizadas pela Justiça Eleitoral para a preparação das urnas e gravação dos resultados são protegidas por técnicas modernas de assinatura digital.

Não é possível a um atacante modificar qualquer arquivo presente nessas mídias.

AUDITORIA EXTERNA NO DESENVOLVIMENTO DA PROGRAMAÇÃO DOS SISTEMAS

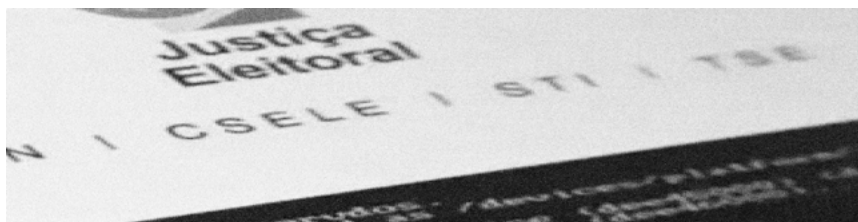
Conforme o Calendário Eleitoral estabelecido para cada pleito, nos 12 meses anteriores às eleições, todas as fases de especificação e de desenvolvimento dos *softwares* são acom-

panhadas por técnicos indicados pelos partidos políticos, pela Ordem dos Advogados do Brasil (OAB), pelo Ministério Público Eleitoral (MPE) e por pessoas autorizadas em resolução específica, podendo eles inspecionar todos os códigos-fonte do programa utilizado pelas urnas eletrônicas e apresentar sugestões.

A principal meta deste acompanhamento é conferir se o *software* funciona para aquilo que foi desenvolvido: registrar e contar votos corretamente. Até 2020, o prazo para os fiscais acessarem o código-fonte era de apenas 6 meses. Isso mudou.

NOVIDADE:

as entidades fiscalizadoras terão, a partir de **12 meses** antes do 1º turno, acesso ao código fonte dos sistemas desenvolvidos pelo TSE.



TESTE PÚBLICO DE SEGURANÇA



6ª edição

Realizado desde 2009, com o objetivo de identificar e corrigir eventuais vulnerabilidades relacionadas à violação da integridade ou do anonimato dos votos de uma eleição, o Teste Público de Segurança (TPS) abre os sistemas eleitorais para que investigadores tentem quebrar as barreiras de segurança do processo de votação, executando planos de ataque aos componentes externos e internos da urna eletrônica.

Assim, entre novembro e dezembro do ano anterior à eleição, o TSE promove o evento, ocasião em que especialistas em Tecnologia e Segurança da Informação têm liberdade para colocar os mecanismos de segurança da urna à prova, a fim de que sejam identificadas eventuais vulnerabilidades.

O TPS visa a fortalecer a transparência, a confiabilidade e a segurança da captação e da apuração dos votos, além de propiciar melhorias ao processo eleitoral. Em maio do ano seguinte em que

Realizado desde 2009, com o objetivo de identificar e corrigir eventuais vulnerabilidades relacionadas à violação da integridade ou do anonimato dos votos de uma eleição, o

Teste Público de

Segurança (TPS) abre os sistemas eleitorais para

que investigadores tentem quebrar as barreiras

de segurança do processo de votação, executando

planos de ataque aos componentes externos e

internos da urna eletrônica.

Assim, entre novembro e dezembro do ano

anterior à eleição, o TSE promove o evento, ocasião

em que especialistas em Tecnologia e Segurança

da Informação têm liberdade para colocar os

mecanismos de segurança da urna à prova, a fim

de que sejam identificadas eventuais vulnerabi-

lidades.

O TPS visa a fortalecer a transparência, a confi-

abilidade e a segurança da captação e da apuração

dos votos, além de propiciar melhorias ao pro-

cesso eleitoral. Em maio do ano seguinte em que

MATURIDADE



O evento demonstra a maturidade e confiança nas eleições informatizadas brasileiras.

TRANSPARÊNCIA



Acesso à informação para diversas instituições e qualquer cidadão brasileiro.

PARTICIPAÇÃO



Trabalho participativo junto à sociedade. Aberto a críticas e sugestões.

COLABORAÇÃO



Trabalho participativo junto à sociedade. Aberto a críticas e sugestões.

o TPS é realizado, as correções são confirmadas em uma nova rodada de avaliações com os mesmos participantes.

Março 21

Divulgação do resultado final da confirmação do Teste Público de Segurança para as eleições 2022.

30.5.2022

O Teste Público de Segurança de 2021 (TPS 2021), foi a sexta edição do evento, ocorreu entre 22 e 26 de novembro de 2021, na sede do TSE, em Brasília/DF, tendo como foco buscar a colaboração da sociedade brasileira para o aperfeiçoamento do sistema eletrônico de votação utilizado nas eleições do país.

Todas as informações sobre o TPS podem ser encontradas em:

<http://www.justicaeleitoral.jus.br/tps/>.

LACRAÇÃO DOS SISTEMAS



Até 20 dias antes do pleito, é realizada Cerimônia de Lacração dos Sistemas Eleitorais, que é pública e conta com a participação dos partidos políticos, do MPE e da OAB. O ato, que acontece nas dependências do TSE, serve para 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. Ou seja: serve para garantir que o *software* que será compilado para fins de instalação

Uma vez lacrado, garante-se que qualquer software diferente do oficial usado nas eleições, torna os resultados nulos.

nas urnas é exatamente o mesmo cujo desenvolvimento foi acompanhado e avaliado pelas entidades.

Para todo o conjunto de *software* produzido durante a Cerimônia de Lacração dos Sistemas Eleitorais são geradas assinaturas digitais e resumos digitais. Caso haja qualquer suspeição quanto à autenticidade do *software* da urna eletrônica as assinaturas digitais e os resumos digitais podem ser conferidos e validados por aplicativos desenvolvidos pelo TSE e, também, por partidos políticos, pelo MPE e pela OAB.

Em resumo, o que é apresentado na cerimônia:

- a versão final dos sistemas eleitorais;
- os códigos-fonte e executáveis;
- os manuais;
- a documentação.

Res. TSE nº 23.673/2021

Art. 19. Uma vez concluídos e até 20 (vinte) dias antes das eleições, os sistemas eleitorais e os programas de verificação desenvolvidos pelas entidades fiscalizadoras serão lacrados, mediante apresentação, compilação, assinatura digital e guarda das mídias pelo TSE na Cerimônia de Assinatura Digital e Lacração dos Sistemas, cujos procedimentos terão duração mínima de 3 (três) dias.

Res. TSE nº 23.673/2021

Art. 2º, IX - lacração dos sistemas: procedimento executado na Cerimônia de Assinatura Digital e Lacração dos Sistemas que consiste na gravação dos programas assinados em mídia não regravável e em posterior acondicionamento desta em envelope assinado fisicamente e guardado em cofre do Tribunal Superior Eleitoral (TSE).

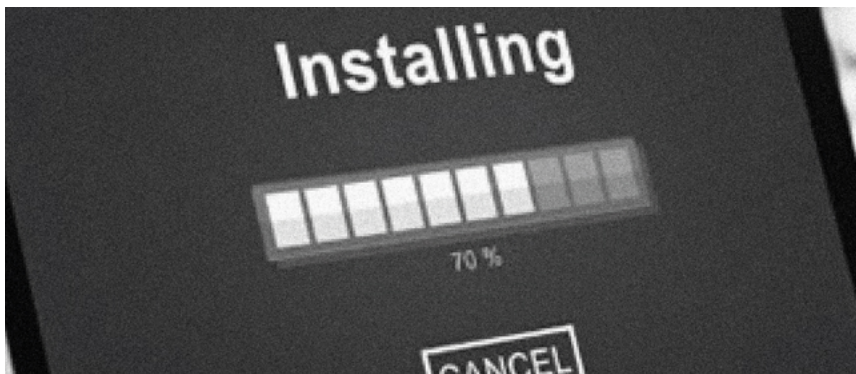
Res. TSE nº 23.673/2021

*Art. 5º A fiscalização dos sistemas eleitorais ocorrerá de acordo com os seguintes momentos e mecanismos:
I - durante o desenvolvimento, a compilação, a assinatura digital, e a lacração dos sistemas eleitorais, mediante:*

É possível que o alguém altere os *softwares* das urnas para fraudar uma eleição?

Os fiscais acompanham a produção dos vários códigos-fonte que serão utilizados no respectivo ano eleitoral. Ao final do processo, esses códigos são lacrados. Isso significa dizer que, em uma reunião solene, todos os participantes podem fazer uma espécie de foto do código. Se, durante o processo eleitoral, for provado que existe uma urna ou demais *softwares* utilizando um código-fonte diferente daquele que foi lacrado, torna-se nulo o resultado do pleito. Isso torna o evento de suma importância para os fiscais e interessados no processo eletrônico de votação.

INSTALAÇÃO DO PROGRAMA E CONECTIVIDADE DAS URNAS



Após a realização da Cerimônia de Lacração dos Sistemas Eleitorais, em geral 20 dias antes do pleito, as urnas começam a ser preparadas nos TRES e nas Zonas Eleitorais para o dia da votação. Em audiência pública, presidida pelo Juiz Eleitoral e que conta com a participação dos representantes do MPE e da OAB, é feita a instalação do *software*, das informações dos candidatos da circunscrição e dos eleitores da respectiva seção e são inseridos os cartões de memória que receberão uma cópia dos votos que serão apurados.

*Cada um das mais de 470 mil urnas eletrônicas
são preparadas uma a uma, manualmente,
uma vez que elas são incapazes de funcionar em rede.*

CRIPTOGRAFIA



A criptografia digital é um mecanismo de segurança para o funcionamento dos programas computacionais. Como os dados são codificados e embaralhados, torna-se impossível o acesso por pessoas não autorizadas. Nos programas da urna, da transmissão, da recepção e da totalização dos votos, são utilizados algoritmos proprietários de cifração simétrica e assimétrica, de conhecimento exclusivo do TSE.

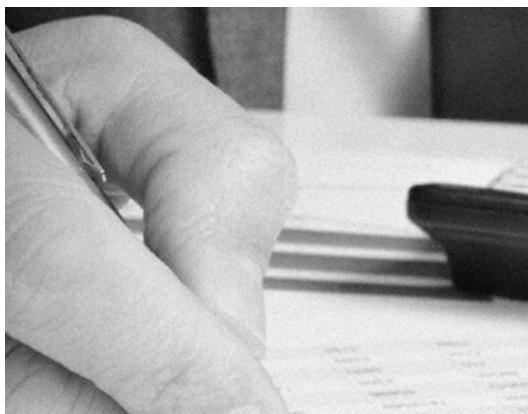
recepção e da totalização dos votos, são utilizados algoritmos proprietários de cifração simétrica e assimétrica, de conhecimento exclusivo do TSE.

Dessa forma, o boletim de urna (BU) é criptografado de forma segmentada, assinado digitalmente e transmitido. Na recepção dos dados pelos tribunais eleitorais, existe a decriptografia, que é o processo pelo qual são recuperados os dados previamente criptografados, isto é, eles são desembaralhados. É, igualmente, um mecanismo de segurança para o funcionamento dos programas computacionais.

No recebimento do boletim de urna ocorre:

- a validação da compatibilidade da chave pública de assinatura digital do boletim de urna com a chave privada do programa totalizador (se a urna não for reconhecida, o resultado não recebido pelo sistema);
- a decriptografia do boletim de urna de forma segmentada;
- a leitura do boletim de urna decriptografado;
- o armazenamento do boletim de urna criptografado e decriptografado.

VERIFICAÇÃO DOS SISTEMAS ELEITORAIS NA CERIMÔNIA DE GERAÇÃO DE MÍDIAS



Durante a cerimônia de geração de mídias, momento em que os dados relativos ao processo eleitoral em disputa são copiados para cartões de memória para que, posteriormente, sejam instalados nas urnas, há mais uma possibilidade de fiscalização e auditoria.

Nesta fase, conforme dispõe o Art. 36 da Res. TSE nº 23.673/2021, as entidades fiscalizadoras poderão verificar a integridade de todos os sistemas envolvidos no processo de geração das mídias, devendo solicitar à autoridade responsável pelo evento os pedidos que entender necessários.

Além disso, qualquer cidadão ou cidadão presente poderá reportar eventual irregularidades observada no processo, por escrito, ao juízo eleitoral ou autoridade competente sem, no entanto, fazer contato direto com técnicos e servidores durante o exercício de suas atividades.

Com isso, nesta fase, afasta-se a possibilidade de qualquer tentativa de cópia de dados produzidos por terceiros ou de instalação de *softwares* não originais nas urnas.

MECANISMOS DE FISCALIZAÇÃO DOS SISTEMAS ELEITORAIS

A evolução do sistema eleitoral eletrônico brasileiro trouxe a necessidade de cada vez mais transparência ao processo. Com isso, para possibilitar que todos os interessados possam acompanhar, fiscalizar e auditar todas as etapas, a Res. TSE nº 23.673/2021 trouxe algumas novidades, inclusive novos mecanismos de fiscalização.

Segundo o art. 5º da citada resolução, existem oito mecanismos de fiscalização solenes dos sistemas eleitorais, senão vejamos:

I - durante o desenvolvimento, a compilação, a assinatura digital, e a lacração dos sistemas eleitorais, mediante;

II - durante as cerimônias destinadas à geração de mídias e preparação das urnas eletrônicas;

III - durante a cerimônia destinada à verificação da integridade e autenticidade dos sistemas eleitorais instalados no TSE;

IV - na audiência destinada à verificação dos sistemas destinados à transmissão de BUs;

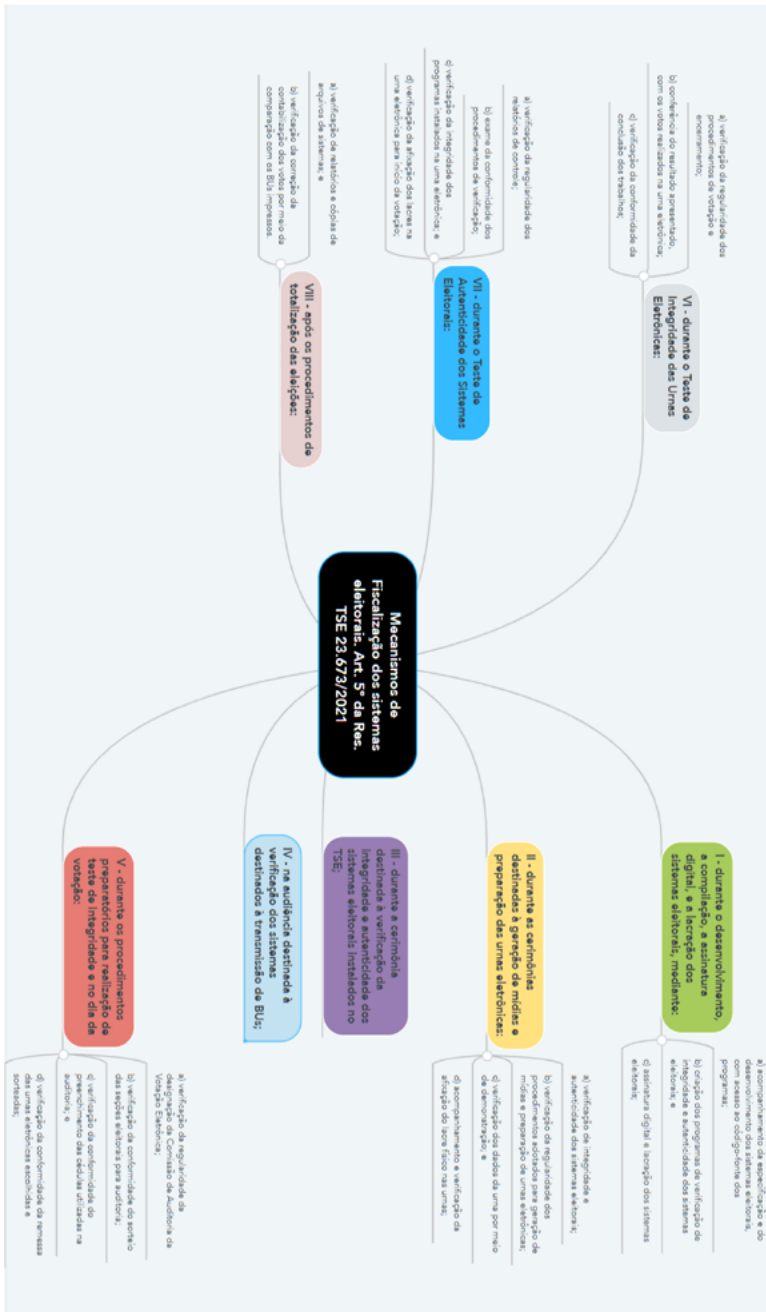
V - durante os procedimentos preparatórios para realização de teste de integridade e no dia da votação;

VI - durante o Teste de Integridade das Urnas Eletrônicas;

VII - durante o Teste de Autenticidade dos Sistemas Eleitorais;

VIII - após os procedimentos de totalização das eleições.

Veja mais detalhes pelo infográfico na página a seguir.



TESTE DE INTEGRIDADE DAS URNAS ELETRÔNICAS

Aqui devemos recordar sobre a cerimônia de lacração dos sistemas. No sábado anterior ao dia das eleições de primeiro e segundo turnos, qualquer urna do país poderá ser escolhida ou sorteada para que, publicamente, seja testado se nela está instalado o mesmo *software* que foi lacrado e se os seus resultados serão condizentes com o esperado.

Pela resolução, finalizada a escolha ou o sorteio das seções eleitorais destinadas ao teste de Integridade das Urnas Eletrônicas, a presidência da Comissão de Auditoria da Votação Eletrônica comunicará imediatamente o resultado ao juízo eleitoral da zona correspondente à seção escolhida ou sorteada. Esse, por sua vez, providenciará o transporte da urna até o local indicado

Cabe destacar que esse procedimento, tradicionalmente, era chamado de Votação Paralela pelo Art. 66, §6º, da Lei 9.504/97, contudo, a resolução ampliou os testes a serem realizados, tornando o evento ainda mais completo e transparente, razão pela qual o nome adequado, a partir de agora, passa a ser teste de autenticidade dos sistemas e de integridade das urnas eletrônicas.

Res. TSE nº 23.673/2021

Art. 53. Os tribunais regionais eleitorais realizarão, por amostragem, no dia da votação:
II - a verificação de autenticidade e integridade dos sistemas instalados nas urnas, nos termos do Capítulo VI desta Resolução, em cada unidade da Federação, nas seções eleitorais escolhidas ou sorteadas de acordo com o disposto na Seção III do presente capítulo.

Res. TSE nº 23.673/2021

Art. 34. Nas verificações dos sistemas eleitorais a serem realizadas no âmbito dos TREs ou das zonas eleitorais, a pessoa representante da entidade fiscalizadora informará se utilizará o programa de verificação de autenticidade e integridade da JE ou programa próprio, nos termos do art. 15 desta Resolução.

Res. TSE nº 23.673/2021

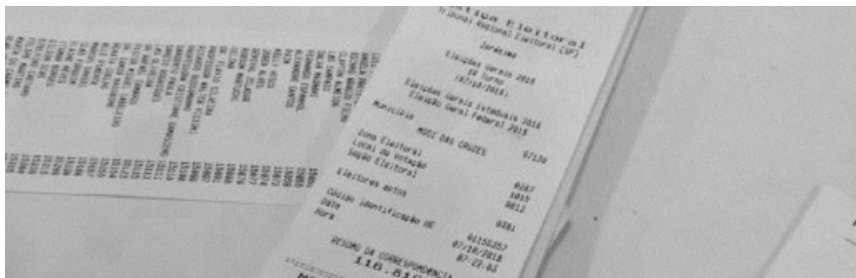
Art. 5º A fiscalização dos sistemas eleitorais ocorrerá de acordo com os seguintes momentos e mecanismos:

V - durante os procedimentos preparatórios para realização de teste de integridade e no dia da votação.

Seria possível a urna saber que está sendo testada?

Existe uma teoria de que as urnas poderiam descobrir que estão sendo testadas e, a partir disso, não manifestar o comportamento fraudulento para o qual teria sido programada. Contudo, não podemos nos esquecer que as urnas são equipamentos preparados para realizar determinadas atividades. Qualquer ação ou omissão realizada pela urna precisa de um código previamente instalado em seu sistema. Se os programas estão disponíveis para todas as entidades fiscalizadoras analisar e testar, esconder rotinas que detectam testes seria extremamente difícil para qualquer agente malicioso.

ZERÉSIMA E VOTOS EM *BACKUP*



No dia de votação, os componentes das mesas receptoras de votos e/ou justificativas começam seus trabalhos com a impressão da zerésima, que é o relatório emitido pela urna, antes da votação, que discrimina a identificação do equipamento e comprova que nele estão registrados todos os candidatos, e que nenhum deles computa voto, ou seja, que a urna tem zero voto.

A emissão desse documento é acompanhada por fiscais dos partidos. Durante todo o dia, os votos são computados em duas memórias internas — uma delas pode ser removida caso seja preciso substituir a urna.

Como funciona a impressão da Zerésima?

Após as 7h30 do dia da eleição, a urna eletrônica é ligada. Na presença dos mesários e fiscais de partidos políticos, é emitido em cada seção eleitoral um relatório denominado “zerésima”, que contém toda a identificação daquela urna e comprova que nela estão registrados todos os candidatos com zero voto. Após a assinatura do presidente da seção e dos fiscais presentes, esse relatório passa a compor a documentação da seção eleitoral.

VOTAÇÃO COM IDENTIFICAÇÃO BIOMÉTRICA DO ELEITOR

Com a adoção da tecnologia de identificação por meio dos dados biométricos, os eleitores mal notaram as mudanças na hora de votar. Isso porque a urna com leitor biométrico informatizou um procedi-



mento operacional: a liberação da urna, habilitando a votação a partir da leitura corporal individualizada do eleitor (impressões digitais), deixa de ser feita pelos mesários, aumentando sobremaneira a segurança do voto e a lisura do processo eleitoral.

Ainda, é importante destacar que a automatização desse procedimento elimina em elevado percentual a possibilidade de equívocos na habilitação pelos mesários de pessoa homônima ou diversa do eleitor que se apresentou para votar (por exemplo, ao utilizar a régua para ler e digitar o número da inscrição eleitoral no terminal da urna, o Presidente de Mesa insere o número contido na linha imediatamente abaixo do caderno de votação).

Vale frisar que o novo modelo de urna para as eleições 2022 conta com terminal do mesário com tela totalmente gráfica, sem teclado físico. E agora com superfície sensível ao toque.

REGISTRO DIGITAL DO VOTO (RDV)

O registro digital do voto, ou arquivo de votos, foi criado em 2003, possibilitando a recuperação dos votos para recontagem eletrônica a qualquer tempo, além de acrescentar segurança e transparência ao processo eleitoral.

O RDV, como é chamado, consiste na inserção, de forma aleatória, do voto de cada eleitor, assinado digitalmente pela urna eletrônica, em uma tabela de tamanho igual à da quantidade de eleitores da seção eleitoral.

A assinatura digital de cada voto, obtido mediante a aplicação de sistema de criptografia baseada em tecnologia de chaves assimétricas, conhecido como infraestrutura de chaves públicas, garante a identidade ou autenticação da urna registradora daquele registro digital e até o sigilo daquele registro.

Não há possibilidade de identificar o eleitor, uma vez que os votos, à medida que vão sendo registrados, são depositados aleatoriamente na urna eletrônica, impedindo qualquer vinculação entre o voto e o eleitor.

O arquivo é criptografado e possui cópia de segurança na urna.

GRAVAÇÃO DOS DADOS E EMISSÃO DO BU



Ao final da votação, o boletim de urna com a apuração dos votos de uma seção, carinhosamente chamado por nós de “BU”, transforma-se em documento público. O resultado de cada boletim pode ser facilmente confrontado com aquele

publicado pelo TSE na internet, seja pela conferência do resultado de cada seção eleitoral, seja pela conferência do resultado da totalização final. Esse é um procedimento amplamente realizado pelos partidos políticos e coligações há muito tempo e que também pode ser feito pelo eleitor, inclusive utilizando-se do app “Boletim na Mão”, desenvolvido pelo TSE e disponibilizado no Google Play e na App Store.

Após ser gerado o boletim de urna (BU), com todos os votos da seção, os dados são gravados de forma criptografada em cartões de memória chamados de “mídias de resultado”. Esses dispositivos são removidos e lacrados em um envelope específico contido no material dos mesários, seguindo para o local de transmissão dos votos (em geral, o Cartório Eleitoral) acompanhados de duas cópias impressas do BU.

Vale ressaltar que para muitos municípios, a participação da Justiça Eleitoral no pleito termina neste momento, pois, os próprios partidos se organizam para que eles mesmos totalizem o resultado das eleições, somando todos os BUs do município.

TRANSMISSÃO DOS VOTOS

As mídias de resultado são encaminhadas para um centro de transmissão, que pode ser o próprio Cartório Eleitoral (via de regra), o local de recepção de materiais para apuração ou a sede do TRE. Em locais de difícil acesso, a transmissão pode ser feita até por satélite. O envio dos dados é realizado em rede privada, exclusiva da Justiça Eleitoral, sendo inacessível para quaisquer tipos de invasores (*hackers*).

Os locais de transmissão são publicados no site do TRE cinco dias antes da eleição.

Todos os dados que alimentam a urna eletrônica, assim como todos os resultados produzidos, são protegidos por assinatura digital. Não é possível modificar os dados de candidatos e eleitores presentes na urna, por exemplo. Da mesma forma, não é possível modificar o resultado da votação contido no boletim de urna ou o registro das operações feitas pelo *software* (log) ou mesmo o arquivo de Registro Digital do Voto (RDV), entre outros arquivos produzidos pela urna, uma vez que todos estão protegidos pela assinatura digital.

Nos TREs, os dados são checados para garantir que eles vieram da mesma urna onde a mídia de resultado estava inserida. Os sistemas também verificam se os dados foram gerados pelo mesmo *software* que passou pelos testes de segurança e auditoria, que conta com assinatura digital.

APURAÇÃO DOS RESULTADOS



Após a impressão dos boletins de urna, uma mídia (pendrive) contendo o resultado é gravada de forma criptografada e assinada digitalmente. Quando chega ao servidor central para a totalização dos votos primeiramente é verificada a assinatura digital. Se a assinatura digital for válida, está garantido que aquele resultado foi gerado pela urna eletrônica que foi preparada para aquela seção eleitoral, ou seja, garante-se a integridade e a autenticidade do resultado.

Após essa verificação da assinatura digital, o boletim de urna é decifrado e várias verificações de consistências são feitas. Caso qualquer inconsistência seja confirmada – como divergência na totalidade de votos e o número de eleitores que compareceram –, ou a assinatura digital seja inválida, o boletim de urna é automaticamente descartado.

COMISSÃO DE ENFRENTAMENTO
À DESINFORMAÇÃO

SECRETARIA JUDICIÁRIA
COGIN - SEPG



Tribunal Regional Eleitoral
do Rio Grande do Sul

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: 137e8c1e - bd4bf760 - 00d8560c - dc5f1033