O que é Desinformação e como enfrentá-la:

um guia da Justiça Eleitoral de Santa Catarina

2ª Edição

Justiça Eleitoral

Dados Internacionais de Catalogação na Publicação (CIP)
Tribunal Regional Eleitoral de Santa Catarina - Biblioteca Des. José Rocha F. Bastos

B823q

Brasil. Tribunal Regional Eleitoral de Santa Catarina.
O que é desinformação e como enfrentá-la [recurso eletrônico]: um guia da Justiça Eleitoral de Santa Catarina / Tribunal Regional Eleitoral. - 2.ed. - Dados eletrônicos (137 páginas). - Florianópolis : Tribunal Regional Eleitoral, 2025.
Versão eletrônica (EPUB).
Modo de acesso : Internet e intranet.
Disponível, também, em formato impresso.

1.Direito Eleitoral - Brasil 2.Desinformação - Eleições 3.Fake news - Eleições 4.Processo eleitoral - segurança 5.DeepFake I.Brasil.Tribunal Regional Eleitoral de Santa Catarina. II.Título.

CDU 342.8:342.72

Ficha catalográfica elaborada pela bibliotecária Jociane Gonçalves CRB-14/827

TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA

Rua Esteves Júnior, 68 - Centro
Florianópolis - SC - CEP 88015-130
Fone: (48) 3251-3700
Site: www.tre-sc.jus.br

Equipe de edição

Coordenação
Juiz Márcio Schiefler Fontes
Presidente do Comitê Gestor do Programa Permanente de Enfrentamento à Desinformação

Conteúdo
Grupo de Apoio Técnico ao Comitê Gestor do Programa Permanente de Enfrentamento à Desinformação
Denise Goulart Schlickmann (SA) - Coordenadora
Karine Borges de Liz (SEEJESC) - Secretária
Adriana Martins Ferreira Festugatto (94ª ZE - Chapecó)
Augusto Gil Chaves Boal (STI/CSC)
Carlos Eduardo Justen (67ª ZE - Santo Amaro da Imperatriz)
Daniel da Rosa Vargas (AEPE)
Edmar Sá (ADG-GI)
Ivete Ana Araldi (SA)
João Sebastião de Andrade (STI/CEL) e
Maurílio Luiz Hoffmann da Silva (ASCOM)

Editoração e Design Gráfico
Assessoria de Comunicação Social (ASCOM)
Mateus Victor de Oliveira

TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA

Presidente
Des. Carlos Alberto Civinski

Vice-Presidente e Corregedor Regional Eleitoral
Des. Carlos Roberto da Silva

Juízes Titulares
Adilor Danieli
Sergio Francisco Carlos Graziano Sobrinho
Marcelo Pizolati
Victor Luiz dos Santos Laus

Juízes Substitutos
Denise de Souza Luiz Francoski
Jaime Machado Júnior
Ana Cristina Ferro Blasi
Rudson Marcos
Márcio Schiefler Fontes
Filipe Ximenes de Melo Malinverni
Luiza Cesar Portella

Procurador Regional Eleitoral
Claudio Valentim Cristani

Diretor-Geral
Gonsalo Agostini Ribeiro

Composição
Outubro/2025

SUMÁRIO

1 INTRODUÇÃO

1. INTRODUÇÃO

Este guia do Tribunal Regional Eleitoral de Santa Catarina, em um contexto desinformativo – seja pela intenção de desinformar, seja pela ingênua disseminação de notícias descontextualizadas ou irreais – tão visível e presente, é fruto de meses de trabalho e pretende trazer a lume, de forma didática e ampla, a compreensão do que seja desinformação, desde seu termo mais popularmente divulgado, qual seja, *fake news*, até sua disseminação em formas tecnologicamente mais reais e sofisticadas, como a *deepfake*.

O fenômeno da desinformação afeta indistintamente toda a sociedade, em quase todas as suas áreas de conhecimento. Percorre desde os afazeres diários típicos até alcançar o universo da comunicação, próprios do que hoje se denomina mundo digital. O conteúdo que ora se apresenta não busca, contudo, apenas conceituar, mas efetivamente informar, a partir da compreensão de que a boa informação é o instrumento mais eficaz para coibir a desinformação.

Assim, tem-se aqui um conjunto cuidadosamente organizado de ferramentas que possam servir à depuração do que seja a informação íntegra, introduzindo as mais modernas ferramentas e técnicas de checagem disponíveis. Paralelamente, o guia também apresenta os *sites* e agências de verificação de fatos disponíveis no Brasil, assim como ferramentas *online* com essa mesma finalidade, no propósito de contribuir e oferecer ao público caminhos práticos de aferição de fatos.

Para além disso, não é novidade que a própria Justiça Eleitoral e mesmo o processo eleitoral brasileiro têm sido, nos últimos anos, alvos recorrentes da manifestação do fenômeno da desinformação, a exigir pronta e preventiva resposta, de que é efetivo exemplo o Programa Permanente de Enfrentamento à Desinformação, cujos principais fundamentos e linhas de atuação são expostos neste trabalho.

Assim, com o propósito de mitigar a propagação de toda sorte de informações falsas, sobretudo quando verificadas condutas potencialmente ilícitas, é que foram organizadas neste trabalho todas as informações disponíveis sobre segurança do processo eleitoral e auditorias do sistema eletrônico de votação. Tais informações contemplam desde o surgimento da urna eletrônica, perpassando os aspectos de segurança na sua produção, de segurança tecnológica, de transparência nos procedimentos e formas pelas quais a própria sociedade pode verificá-los.

A Justiça Eleitoral de Santa Catarina espera, com este guia, participar dos esforços que concorrem, no Brasil e em todo o mundo democrático, para colocar luz e foco nos desafios que impõem as novas tecnologias aos valores sempre caros da liberdade de expressão e do Estado Democrático de Direito.

MUNDO DIGITAL 2

2. MUNDO DIGITAL

Vivemos numa época de alto desenvolvimento tecnológico e acessível para a maioria das pessoas.

A internet dá acesso a inúmeras fontes de informação, possibilitando a democratização/difusão de conhecimento, da cultura, e permitindo a livre expressão do pensamento. Nesse contexto de amplo acesso a uma multiplicidade de informações, a sua integridade é requisito para que as pessoas possam tomar decisões com liberdade e segurança.

Os telefones celulares tornaram-se computadores portáteis permanentemente conectados à internet, a partir dos quais podemos realizar uma série de ações com apenas alguns toques: desde acessar uma conta bancária e redes sociais, gravar e publicar fotos e vídeos, mandar e receber mensagens, ouvir música, assistir a filmes e vídeos, e muito mais!

O acesso à tecnologia e a facilidade em produzir e compartilhar conteúdos têm um aspecto muito positivo em nossas vidas, mas também apresentam riscos. Por isso é muito importante entender como funciona esse "mundo digital" e como nos comportar nele.

A inteligência artificial incorporada aos aplicativos analisa nosso comportamento na internet e com base nessa análise faz sugestões de conteúdo personalizadas de acordo com as preferências identificadas pelos algoritmos. Assim, cada pessoa tem seu próprio "mundo digital" e fica limitada à sua "bolha" de informações.

O objetivo da criação de um mundo digital próprio é manter as pessoas conectadas. Por isso o conteúdo oferecido busca atender às preferências demonstradas durante o uso dos aplicativos. Mas receber sempre o mesmo tipo de conteúdo pode acabar reduzindo a percepção de mundo, a tolerância e o respeito à diversidade.

Quer saber mais sobre algoritmos? Clique aqui.

É preciso entender que esse conteúdo digital direcionado faz parte de um modelo de negócio onde os produtores de conteúdo são remunerados de acordo com a atenção que recebem dos usuários das mídias sociais. E nessa busca por atenção, frequentemente os conteúdos produzidos têm forte apelo emocional, visando aumentar o engajamento e, consequentemente, a remuneração recebida. Infelizmente, gerar e propagar desinformação são estratégias frequentemente adotadas na chamada Economia da atenção.

Outra característica desse mundo moderno é a rapidez com que as informações são recebidas e compartilhadas. Antes de compartilhar, é fundamental parar por um momento para analisar se a informação recebida é confiável (íntegra, verdadeira, contextualizada). Compartilhar desinformação causa inúmeros problemas a pessoas e instituições. Assim, é preciso ter cuidado e ser responsável. Com esse cuidado também se evitam golpes virtuais, cada vez mais comuns.

A integridade da informação é tão importante que a Organização das Nações Unidas (ONU) expediu recomendações para reforçá-la, visando salvaguardar os Objetivos de Desenvolvimento Sustentável (ODS):

> A promoção da integridade da informação envolve capacitar as pessoas para exercerem o seu direito de procurar, receber e transmitir informações e ideias de todos os tipos e de terem opiniões sem que haja interferência. Em um ambiente de informação digital cada vez mais complexo, isso significa permitir que os indivíduos naveguem em espaços de informação com segurança, privacidade e liberdade.[1]

Quando falamos em desinformação, duas expressões são muito utilizadas: *fake news* e *deepfakes*. A seguir vamos entender o que são *fake news* e *deepfakes*, conteúdos que se propagam facilmente no ambiente digital, conhecer *sites*, ferramentas e técnicas de checagem úteis para enfrentar os desafios do mundo digital.

[1] https://brasil.un.org/*sites*/*default*/*files*/2024-07/ONU_PrincipiosGlobais IntegridadeDaInformacao_20240624.pdf

3

O QUE SÃO *FAKE NEWS* E *DEEPFAKES*?

3. O QUE SÃO *FAKE NEWS* E *DEEPFAKES*?

3.1. Informação íntegra X desinformação

Você já percebeu que quanto mais informações corretas e claras estão disponíveis no nosso dia a dia, fica mais fácil para tomar boas decisões?

Isso vale para situações simples como, por exemplo, saber pela previsão do tempo se irá chover ou não e, se for o caso, levar um guarda-chuva ao sair de casa. E vale também para decisões muito importantes, como é a de escolher as pessoas que irão governar o município, o estado e o país.

Por isso, é muito importante entender o fenômeno da desinformação, pois ele afeta a qualidade das informações que iremos levar em conta em nossas decisões.

A disseminação de desinformação, ainda chamada por alguns de *fake news*, consiste no uso de técnicas de comunicação para induzir o receptor da mensagem ao erro ou provocar uma falsa percepção da realidade por meio da ocultação de informações, minimização da importância de fatos ou dados, modificação do sentido de textos, falas, imagens ou, ainda, mudança de contexto de declarações.

A prática de levar as pessoas ao engano por meio de informações falsas, distorcidas ou fora de contexto é coisa bem antiga. Basta lembrar da história do Cavalo de Tróia.

Mas se isso é coisa antiga, por que se fala tanto sobre isso hoje em dia? Já em 2018 a Comissão Europeia publicou amplo relatório sobre desinformação e *fake news* e, mais recentemente, em 2025, o governo do Reino Unido lançou orientações sobre desinformação *online* e ameaças de IA para candidatos e autoridades eleitorais. Anteriormente, em 2023, o Reino Unido já havia produzido um guia específico sobre o tema intitulado Defendendo a democracia.

Porque com a tecnologia e a popularização das redes sociais ficou muito mais fácil e rápido espalhar esse tipo de conteúdo fraudulento. O que antes era feito de boca em boca e levava dias ou meses, agora, com a tecnologia, atinge milhares de pessoas num espaço de tempo muito reduzido. Por isso a desinformação é um fenômeno que afeta o mundo inteiro, e não apenas o Brasil.

E o mais perigoso: até que seja esclarecida uma notícia falsa, os prejuízos à sociedade podem ser enormes, a ponto de comprometer a segurança e a integridade das pessoas envolvidas.

3.2. O que é *fake news*?

Como dito, *fake news* não é um assunto recente e nem se refere a apenas uma área da vida das pessoas. Também é um tema que passou a ser muito estudado nos últimos tempos. Por tudo isso, é possível encontrarmos várias definições de *fake news*, dependendo do ponto de vista que se está analisando.

Por exemplo, quando estamos tratando de eleições, a parte do Direito que regula tudo o que se refere a elas é o Direito Eleitoral. E para o Direito Eleitoral, conforme ensina o professor Diogo Rais, *fake news* é o "conteúdo enganoso com potencial lesivo".

Uma *fake news* pode ser espalhada de muitas formas. Pode ser por meio de uma matéria escrita de jornal, um meme no *WhatsApp*, um vídeo, um áudio, uma foto, etc. Ou seja, a mensagem enganosa pode ter muitos formatos.

Entendendo melhor:

- O que significa "enganoso": o que uma *fake news* faz, em resumo, é distorcer a realidade, levando ao engano sobre ela. A pessoa acha que aquele conteúdo com o qual ela está tendo contato é totalmente verdadeiro, quando não é. Isso porque uma notícia até pode ser verdade, mas quando é retirada do seu contexto, ou seja, quando é distorcida de alguma forma, acaba levando a pessoa ao erro. Por isso, nem toda *fake news* é uma mentira descarada. Ela pode ser apenas uma meia-verdade. E é aí que mora o perigo.

- O que quer dizer "com potencial lesivo": significa que estamos diante de uma *fake news* quando a mensagem fraudulenta/enganosa que ela traz pode acarretar algum tipo de prejuízo (lesão) ou ameaça de prejuízo a algo que é protegido pelas leis e pelo Direito. Exemplo: quando um *show* é de graça para a população, mas pessoas aproveitadoras espalham que estão vendendo camarotes ou lugares especiais para quem se dispuser a pagar[2].

Qual o motivo das *fake news* influenciarem tanto as pessoas?

Existem vários motivos, mas provavelmente o principal é a dimensão emocional das *fake news* na vida das pessoas.

Durante um bom tempo se acreditou que as pessoas, no geral, tomavam suas decisões, desde as mais pequenas até as de maiores consequências, baseadas na razão. Isto é, o mundo seria percebido sem se deixar levar pelas emoções como raiva, medo, paixão, alegria, contentamento, tristeza, etc.

[2] Essa situação aconteceu no Rio de Janeiro no show da Lady Gaga em 3 de maio de 2025.

Porém, pesquisas recentes têm demonstrado que as pessoas, sem se dar conta disso, fazem suas escolhas, formam suas opiniões e tomam suas atitudes com base muito mais no que sentem e como sentem, ou seja, se guiam mais pela emoção do que pela razão para viver no mundo.

E o que isso tem a ver com *fake news*?

Muita coisa! As emoções são um dos pontos centrais das *fake news*.

É também por meio delas que um conteúdo enganoso passa a ser aceito como real, pois as pessoas deixam de raciocinar sobre o que estão vendo ou sabendo de algum modo para se deixar levar pelas emoções que elas provocam. Com isso, uma mensagem enganosa que foi divulgada com o objetivo de prejudicar alguém ou alguma instituição ganha muito mais força para passar como verdade, tornando bem mais difícil convencer uma pessoa do contrário.

Isso se liga a um outro assunto importante: *saber a diferença entre fato e opinião*.

Fato é um dado da realidade. É algo que existe ou está no mundo independentemente da posição, crença ou opinião que uma pessoa ou um grupo de pessoas possa ter em relação a ele.

Exemplo: a cor do céu, a existência da gravidade, etc.

Já a opinião é o julgamento pessoal que cada um faz sobre o que observa dos fatos que toma conhecimento. A opinião está ligada à maneira de pensar, de julgar e de ver de cada ser humano. Por isso se diz que é algo muito pessoal, pois está ligado diretamente aos valores e às emoções que cada pessoa escolhe para si na vida.

Exemplo: alguém pode achar que a cor do céu seria bem melhor se fosse lilás ao invés de azul. A cor do céu é um fato, sua preferência ou não por essa cor é uma opinião.

Ou, ainda, vamos imaginar a seguinte situação:

Está fazendo 29 graus hoje na cidade de Florianópolis. É um **fato**! Qualquer um pode medir com um termômetro.

Opinião 1: Que calor terrível!

Opinião 2: Que delícia essa temperatura, adoro dias assim!

Percebam, a temperatura continua sendo a mesma, mas cada pessoa sente e interpreta a seu modo.

Percebeu como são situações diferentes?

Mostrado dessa forma as coisas parecem simples, não é?

E até seriam não fosse um detalhe importante: a presença dos vieses em nossas vidas. Principalmente o viés de confirmação.

Viés de confirmação: às vezes *fake news* tem mais a ver com vaidade do que com verdade.

Vieses são atalhos mentais, ou seja, é um tipo de recurso mental que os seres humanos utilizam há milênios para facilitar o seu dia a dia. Eles nos ajudam a tomar decisões rápidas. Isso tem seu lado bom e também o ruim:

- **O lado bom:** quando bem utilizado economiza nosso tempo e nossa energia na condução de decisões simples do nosso cotidiano. Exemplo: a chance de se encontrar um mesmo produto com preço mais barato é maior em ruas de comércio popular do que em lojas de *shoppings*;

- **O lado ruim:** como o raciocínio é muito simplificado, acaba que distorções e erros de julgamento acontecem. Exemplo: supor que toda loja de comércio popular sem exceção vende produtos mais baratos que lojas de *shoppings*. Nem sempre é assim.

Há vários tipos de vieses. Mas um dos que mais tem relação com *fake news* é o chamado viés de confirmação.

Viés de confirmação é quando a pessoa lida com as informações que toma conhecimento de forma seletiva, de modo que essas informações irão confirmar crenças e emoções fortemente presentes nela. Ou seja, quando se dá mais valor às informações que confirmam no que se acredita àquelas que questionam o que acreditamos.

E por que isso importa?

Porque se não percebemos que estamos deixando esse viés agir, há grandes chances de confundir opinião com fato. E aí começam os mal-entendidos e até a disseminação de desinformação.

A diferença está em como lidamos com esse viés. Ao se perceber que o que se estava acreditando ser verdade não o é realmente, é frequente não admitir a falha. Por isso se diz que às vezes *fake news* tem mais a ver com vaidade do que com verdade dos fatos em si.

Na verdade, uma *fake news* muitas vezes se assemelha a uma roupa confortável, pois se molda às crenças e aos sentimentos das pessoas. E a realidade, via de regra, pode ser desconfortável às vezes.

3.3. O que é *deepfake*?

Provavelmente você já ouviu falar em *deepfake*, mas será que entende o que esse termo realmente significa?

Deepfake é uma tecnologia baseada em **inteligência artificial** que permite criar vídeos, áudios e imagens falsos que parecem muito reais. Com ela, é possível fazer com que uma pessoa pareça dizer ou fazer algo que nunca disse ou fez: o rosto de uma pessoa pode ser substituído pelo de outra; a boca de uma pessoa falando pode ser ajustada a uma faixa de áudio diferente da original (sincronização labial), e, ainda, uma voz pode ser "copiada" para dizer outras coisas (clonagem de voz).

Quer ver exemplos disso? Clique aqui e aqui.

Parece coisa de filme, né?

E de fato é: essa técnica já foi usada de forma criativa no cinema, na publicidade e até em vídeos de humor. Mas, quando cai nas mãos erradas, pode virar uma arma perigosa: pode ser usada para enganar pessoas, espalhar *fake news*, destruir reputações e até manipular eleições.

Por que devemos nos preocupar?

Imagine ver um vídeo de um ator famoso falando algo polêmico ou fazendo algo reprovável... mas depois descobrir que ele nunca disse ou fez aquilo. Isso pode confundir as pessoas e prejudicar a imagem desse ator, que pode perder oportunidades de trabalho em consequência.

Como se proteger das *deepfakes*?

Desenvolver o olhar crítico e saber identificar sinais de manipulação digital é essencial. Aqui vão algumas dicas simples para você aprender a detectar *deepfakes*:

- **Observe o piscar dos olhos:** muitas vezes, o piscar pode parecer artificial ou não acontecer com a frequência natural.
- **Preste atenção no áudio:** o som da fala acompanha os movimentos labiais? Há sincronia?
- **Note a textura da pele:** principalmente na bochecha e na testa; se estiver estranha ou "plástica" demais, desconfie!
- **Fique de olho na luz:** a iluminação do rosto pode estar diferente do restante do corpo ou do ambiente.

Quer aprender mais?

Assista a um vídeo rápido que explica o que são *deepfakes* e como identificá-las.

Desafio prático: qual rosto é real?

Que tal testar suas habilidades? Acesse o *site* *Which Face is Real?* e tente descobrir qual rosto é de uma pessoa real e qual foi criado por inteligência artificial. Parece fácil? Nem sempre é!

4 FERRAMENTAS

E TÉCNICAS DE CHECAGEM

4. FERRAMENTAS E TÉCNICAS DE CHECAGEM

Antes de compartilhar um texto, uma imagem, um áudio ou um vídeo recebido – por mais urgente e impactante que o conteúdo possa parecer –, é fundamental parar e analisar se a informação recebida é confiável (íntegra, verdadeira, contextualizada).

A seguir são apresentadas algumas ferramentas e técnicas de checagem de textos, imagens e vídeos que podem ajudar nessa análise.

4.1. Introdução à checagem

Por que checar? *Fake news* e *deepfakes* manipulam a opinião pública e distorcem a percepção da realidade, podendo prejudicar pessoas e instituições.

O que vamos aprender? Métodos, manuais e ferramentas digitais para verificar a autenticidade de fontes, datas, linguagem e conteúdos visuais.

Abordagem prática: Método de cinco passos: **verificar fonte**, **data**, **linguagem**, **consistência e tecnologia**, adaptado para checagem rápida e eficaz.

4.2. Checagem de textos

Passo a passo para verificar textos

- **Verificar a fonte:**

1. Confirme se o *site* ou perfil é confiável e pertence a um veículo de imprensa reconhecido. Desconfie de *sites* desconhecidos ou perfis anônimos.
2. Ferramentas como Who.is ajudam a investigar a origem e o histórico de domínios.

Exemplo: um *site* informa que um furacão atingirá o Estado e causará muita destruição. Verifique se o domínio é recente ou ligado a fontes duvidosas.

- **Confirmar a data:**

1. Cheque se a notícia é atual ou está sendo reutilizada fora de contexto.
2. Utilize a busca avançada do Google (ferramentas > período personalizado) para encontrar a data original da publicação.

Exemplo: uma notícia de 2022 sobre chuvas torrenciais pode ser republicada em 2025 como se fosse nova.

- **Analisar a linguagem:**

1. Desconfie de manchetes sensacionalistas ou textos com erros ortográficos e gramaticais.

Exemplo: títulos com **“ESCÂNDALO!”** ou **“VOCÊ NÃO VAI ACREDITAR!”** buscam atrair cliques, não informar.

Checar a consistência:

1. Compare a informação com veículos confiáveis e oficiais. Veículos estabelecidos seguem padrões jornalísticos, e o TSE oferece informações oficiais sobre o processo eleitoral.
2. Consulte portais confiáveis e agências de checagem (no **item 5.1** deste guia você vai conhecer algumas).

Cuidado com redes sociais: Plataformas de redes sociais podem amplificar boatos.

Usar tecnologia:

1. Utilize a ferramenta de análise de textos.
2. Insira o texto ou a URL da notícia para avaliar a probabilidade de desinformação com base em padrões linguísticos.

Dica: combine a análise da ferramenta com sua própria avaliação para maior precisão.

4.3. Checagem de imagens

- **Pesquisa reversa de imagens:** utilizar ferramentas como *Google* Imagens ou *Google Lens*, *TinEye* ou *Yandex* para encontrar a origem da imagem e verificar se ela foi manipulada.
- Análise de cores, luzes, sombras, listras, dedos, perspectiva, etc.
- Repare nas mãos dos personagens, as quais muitas vezes possuem defeitos e distorções.
- **Contexto da imagem:** a legenda e a descrição da imagem correspondem ao que ela realmente mostra?

4.4. Checagem de vídeos

- **Análise da fonte:** verificar a credibilidade do canal/perfil que publicou o vídeo.
- **Pesquisa por trechos do vídeo:** utilizar ferramentas de busca para encontrar outras versões do vídeo e verificar se ele foi manipulado.
- **Análise da qualidade do vídeo:** verificar se há sinais de manipulação (ex: áudio fora de sincronia, rostos borrados).
- Ao passar a mão com os dedos abertos em frente ao rosto caso seja uma chamada ao vivo, a chance disso não ser possível com *deepfake* é alta e, caso o faça, há grande chance de distorção.

5 CHECANDO FATOS

5. CHECANDO FATOS

5.1. *Sites* e agências de checagem de fatos no Brasil

Antes de repassar uma notícia, pesquise para saber se ela é verdadeira e confiável.

A checagem da veracidade de informações divulgadas nas mídias sociais é fundamental para garantir a integridade das informações e reduzir a desinformação e seus efeitos nocivos.

Várias instituições fazem checagem de notícias, sobre os mais variados assuntos, e publicam os resultados em seus *sites*. Dentre elas, destacam-se:

- A Agência Lupa é uma plataforma de combate à desinformação que atua em jornalismo e educação midiática. No *site* dessa agência você encontra um repositório de notícias checadas e verificações, além de matérias sobre algoritmos, mídias, redes sociais, plataformas, tecnologias de informação e *big techs*, que ajudam a entender como é a vida 100% conectada na internet, seus riscos e suas oportunidades.

- Aos Fatos é uma organização jornalística voltada à investigação de desinformação e à checagem de notícias.

- A Boatos.org é uma organização jornalística com foco na checagem de notícias e educação midiática.

- A Checamos AFP é o departamento da agência de notícias AFP (*Agence France Presse*) de checagem de notícias potencialmente danosas.

- O Projeto Comprova, liderado pela Abraji (Associação Brasileira de Jornalismo Investigativo), investiga conteúdos suspeitos e, em resposta, produz conteúdos explicativos e contextualizados, visando manter a integridade da informação.

- O *site* E-farsas é um dos pioneiros na checagem de notícias.

- O Estadão Verifica analisa conteúdos "virais" potencialmente danosos que circulam em mídias sociais.

- O *site* Fato ou Fake publica notícias "virais" verificadas, com a ferramenta utilizada.

- O UOL Confere dedica-se ao esclarecimento de fatos e à checagem de notícias com grande potencial de causar danos.

- A Justiça Eleitoral mantém o *site* Fato ou Boato, que reúne notícias de cunho eleitoral checadas e esclarecimentos sobre desinformações que se propagam especialmente em período eleitoral.

- Informação confiável (oficial e verdadeira) sobre as eleições você encontra no *site* da Justiça Eleitoral.

5.2. Ferramentas *online* de checagem

Foram reunidos numa planilha as principais ferramentas de checagem de imagens, vídeos e textos, além de *sites* das agências de checagem de notícias. Nesta planilha (**ANEXO I**) você tem uma variedade de recursos úteis para enfrentar a desinformação.

5.3. Guia prático de checagem de fatos

Ao receber um texto, uma imagem, um áudio ou um vídeo por aplicativo de mensagem (como *WhatsApp* ou *Telegram*) ou pelas mídias sociais (como *Instagram*, *Facebook*, *TikTok*, *X*), antes de compartilhar siga estes passos para verificar se a notícia é verdadeira ou falsa:

Analise com atenção

- **Qual a fonte da notícia?** O *site*/perfil ou a pessoa é confiável e costuma divulgar informações corretas? Conhecer a credibilidade da fonte é importante.

- **Observe o tom da notícia:** o texto tem título sensacionalista ou alarmista, usa letras maiúsculas, exclamações, muitos adjetivos, possui erros gramaticais, não indica claramente a fonte? O áudio, a imagem ou o vídeo é chocante ou impactante? Tem senso de urgência? Notícias sensacionalistas geralmente querem apenas captar o seu "clique".

- **Qual sentimento a notícia provoca?** A manipulação de sentimentos (medo, ódio, raiva, curiosidade, pena/comiseração) é comum em notícias falsas. Desconfie de notícias que apelam para suas emoções.

- **Observe bem as imagens e os vídeos para identificar alguma manipulação ou montagem:** falta de sincronia entre som e imagem, textura da pele "plástica", piscar de olhos e movimentos "mecânicos", podem indicar manipulação.

- **Solicita compartilhamento?** Querer "viralizar" é um indicativo de conteúdo falso e enganoso.

Pesquise

- Verifique a data: a notícia é recente ou foi republicada fora do contexto? Um texto, um fato ou uma imagem de outra época ou de outro evento podem causar confusão. Por exemplo, uma notícia verdadeira sobre a ocorrência de fortes chuvas em uma região do país, republicada anos depois como sendo atual pode causar uma apreensão desnecessária nas pessoas. Uma informação fora de contexto leva à interpretação errada dos fatos.

- Pesquise o texto da notícia no *Google*, e organize o resultado por ordem cronológica para descobrir a data de publicação original.

- Use a pesquisa reversa de imagens para encontrar a imagem original e verificar seu contexto. Você pode usar *Google* Imagens ou *Google Lens*, *TinEye* ou *Yandex*. Na planilha (**ANEXO I**) você encontra várias ferramentas que podem ser usadas para verificar notícias e esclarecer fatos.

- Verifique se a notícia foi publicada em outros *sites* ou mídias sociais confiáveis, com conteúdo semelhante. Uma notícia parcial ou fora de contexto pode se tornar uma desinformação.

- Vá direto à fonte oficial da informação: o *site* oficial do órgão público, da empresa ou da instituição é a fonte da informação íntegra e verdadeira.

- Pesquise nas agências de checagem (como Agência Lupa, Aos Fatos, Boatos.org, Checamos AFP, Comprova, E-farsas, Estadão Verifica, Fato ou Fake, UOL Confere e Fato ou Boato). O fato já pode ter sido checado e esclarecido.

Denuncie

- Os aplicativos de mensagem e as mídias sociais possuem meios de denunciar conteúdos e perfis falsos. Recebeu *fake news*, denuncie!

- Quando a desinformação for sobre eleições, utilize o Sistema de Alertas de Desinformação Eleitoral (SIADE).

- Você pode denunciar notícias falsas também na página do Ministério Público Federal (MPF).

- Só compartilhe informações após checá-las. Evite propagar boatos, mesmo que pareçam convincentes.

5.4. Saiba mais (*links* úteis)

- Guia prático CNJ.
- Minicurso Aprenda a identificar boatos nas redes.
- Inteligência Artificial: o básico para entendê-la.
- Dicas para verificar conteúdos e não espalhar desinformação.
- Cartilha de Segurança para Internet.
- Dicas rápidas de segurança digital.
- Educamídia: Educação midiática e IA.
- *E-books* Educom.

6 ENFRENTAMENTO À DESINFORMAÇÃO ELEITORAL

6. ENFRENTAMENTO À DESINFORMAÇÃO ELEITORAL

O enfrentamento à desinformação tem sido um dos maiores desafios da Justiça Eleitoral nos últimos anos. Isso porque a disseminação crescente de notícias falsas, descontextualizadas ou manipuladas acarreta a formação de opiniões distorcidas quanto à integridade do sistema eletrônico de votação utilizado no país.

Uma importante fonte de consulta, como já visto, para se obter informações de qualidade é a página Fato ou Boato, onde são esclarecidas dezenas de teorias conspiratórias e notícias falsas relacionadas à segurança do sistema eleitoral brasileiro.

6.1. Programa Permanente de Enfrentamento à Desinformação

A Justiça Eleitoral possui Programa específico e permanente de enfrentamento à desinformação (PPED).

Iniciado no Tribunal Superior Eleitoral, também o Tribunal Regional Eleitoral de Santa Catarina o instituiu e passou a atuar de forma sistêmica no enfrentamento à desinformação.

O escopo do PPED é a redução dos efeitos prejudiciais da desinformação relativa à Justiça Eleitoral e aos seus integrantes, ao sistema eletrônico de votação, ao processo eleitoral e aos seus diversos participantes. Os conteúdos desinformativos relativos a pré-candidatas(os), candidatas(os), partidos políticos, coligações e federações fogem ao escopo do programa, exceto quando possam afetar negativamente a integridade, a credibilidade e a legitimidade do processo eleitoral.

Em 2022 o TSE instituiu também o Programa de Fortalecimento da Imagem da Justiça Eleitoral (PROFI), com o objetivo de estimular a confiança social na idoneidade do processo eleitoral e na imparcialidade, no profissionalismo e na fundamentalidade da Justiça Eleitoral.

Na página do Programa de enfrentamento à desinformação estão reunidos os conteúdos referentes aos dois programas, como o relatório de ações e resultados, o guia básico de enfrentamento à desinformação, o programa de fortalecimento institucional a partir da gestão da imagem da Justiça Eleitoral, notícias, boletins, lista de instituições parceiras, além de vídeos informativos.

Em março de 2024 o TSE inaugurou o Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia (CIEDDE) que, juntamente com órgãos públicos e entidades privadas, especialmente plataformas de redes sociais e serviços de mensagens, atua no enfrentamento à desinformação e aos discursos de ódio, discriminatórios e antidemocráticos no âmbito eleitoral. O CIEDDE também atua na promoção da educação para a cidadania, os valores democráticos e os direitos digitais.

Uma das principais ferramentas do PPED é o Sistema de Alertas de Desinformação Eleitoral (SIADE), que possibilita a qualquer pessoa relatar fatos notoriamente inverídicos ou descontextualizados com potencial de prejudicar o equilíbrio do pleito ou a integridade do processo eleitoral.

Inclusive a página Fato ou Boato foi criada com o objetivo de esclarecer informações sobre o processo eleitoral e estimular a verificação da veracidade de informações por meio da divulgação de notícias checadas, recomendações e conteúdos educativos. Essa iniciativa integra o Programa Permanente de Enfrentamento à Desinformação e reúne os conteúdos verificados por agências de checagem parceiras, além de orientações para a identificação de notícias falsas.

6.2. E se for caso de denúncia?

O que fazer se, devido à gravidade do caso, for necessário fazer uma denúncia? Veja quais meios estão disponíveis para a denúncia.

Sistema de Alertas de Desinformação Eleitoral (SIADE) e aplicativo Pardal

Como vimos, na página do TSE você encontra o SIADE, um canal da Justiça Eleitoral para apurar desinformações referentes diretamente às eleições. Para registro de denúncia, é necessário escolher uma das categorias de desinformação, fundamentadas na Resolução TSE n. 23.610/2019, e informar o *link* da publicação do fato relatado.

Os fatos informados no SIADE são analisados quanto ao enquadramento no escopo do Programa Permanente de Enfrentamento à Desinformação e, em caso positivo, são encaminhados às plataformas digitais. Se houver indício de crime eleitoral, são encaminhados às instâncias competentes: Ministério Público Eleitoral (MPE) e Polícia Federal (PF). Na hipótese de o fato relatado restringir-se às municipalidades, é feito o encaminhamento ao Tribunal Regional Eleitoral (TRE) competente.

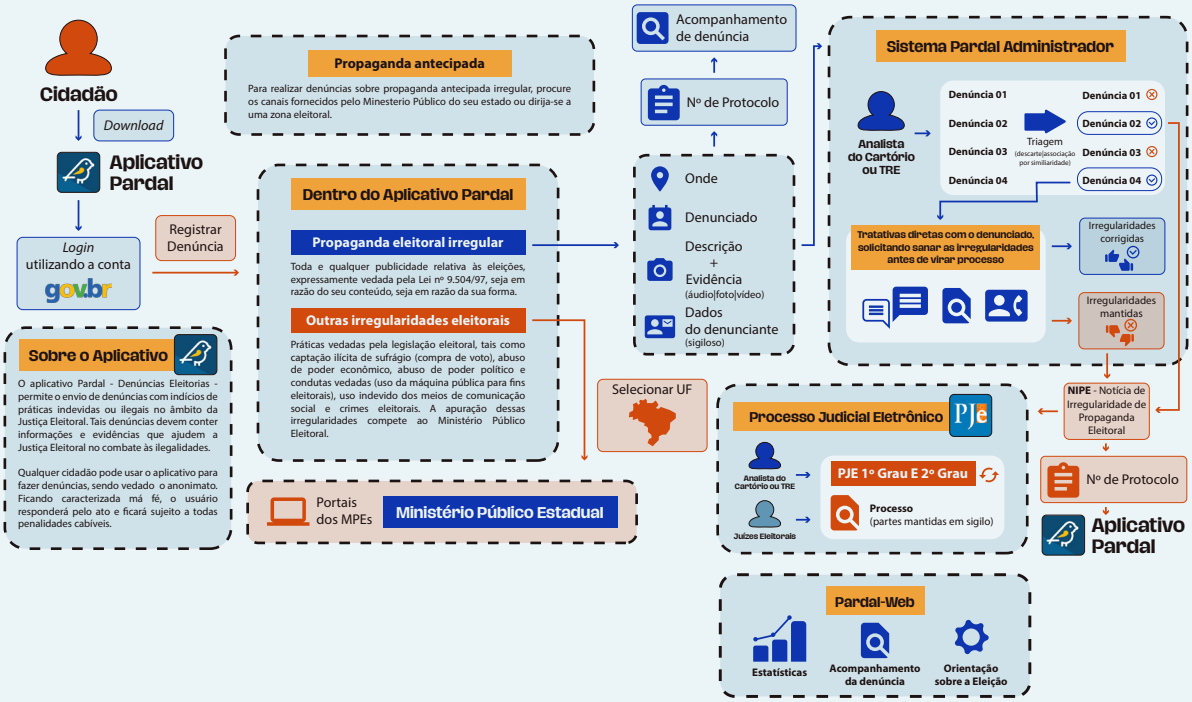
No SIADE você também vai encontrar, além dos vários assuntos relacionados a possíveis denúncias, as decisões já tomadas pela Justiça Eleitoral em cada um dos temas relacionados.

Já o aplicativo Pardal Móvel serve para o encaminhamento de denúncias relativas à propaganda eleitoral irregular, e pode ser baixado na loja de aplicativos de qualquer *smartphone*.

Por meio desse aplicativo a denúncia pode ser encaminhada ao SIADE, quando envolver desinformação, ou para o Ministério Público Eleitoral, quanto tratar de crime eleitoral ou outros ilícitos eleitorais.

Entenda como funciona o Pardal:

Figura 1 - Visão Gráfica do Aplicativo Pardal



Fonte: Adaptado de TSE (2025).

Página do Ministério Público Federal (MPF)

Outra possibilidade para encaminhar denúncias ou relatar irregularidades sobre as eleições é por meio da página do Ministério Público Federal (MPF). Naquele órgão trabalham Procuradores da República que cuidam desse tipo de matéria.

E como fazer o encaminhamento de denúncias ao MPF?

É simples: basta acessar o endereço eletrônico do MPF, e ali encontrar a página MPF Serviços. Nela existe a opção Denúncias onde pode ser informado irregularidade ou fato ilícito (conta gov.br acesso bronze).

Plataformas de redes sociais e de mensageria

Você pode denunciar perfis falsos e conteúdos enganosos e desinformativos diretamente nas plataformas de redes sociais ou nos aplicativos de mensageria.

A seguir seguem exemplos de algumas das desinformações mais comuns em época eleitoral, com os devidos esclarecimentos.

6.3. Esclarecendo algumas desinformações

Veja algumas das principais desinformações veiculadas e seus respectivos esclarecimentos:

Desinformação: Urna eletrônica é vulnerável a ataques externos pela internet.

Esclarecimento: Essa é uma das alegações mais frequentes, mas é completamente infundada. A urna eletrônica é projetada para operar sem qualquer tipo de conexão à internet, seja por cabo, *wi-fi* ou *bluetooth*. Esse isolamento é uma medida de segurança essencial para protegê-la de invasões cibernéticas. A Justiça Eleitoral tem reiteradamente desmentido essa alegação, mas ela persiste, possivelmente como uma estratégia para gerar desconfiança no sistema.

Desinformação: *Software* da urna pode ser manipulado e o código-fonte não é transparente.

Esclarecimento: Essa alegação também é falsa. O desenvolvimento do *software* da urna é de responsabilidade exclusiva do Tribunal Superior Eleitoral (TSE), com a participação de especialistas de diversas entidades desde 1995. O código-fonte do *software* eleitoral é aberto para inspeção por representantes de partidos políticos, do Ministério Público, da Ordem dos Advogados do Brasil (OAB), da Polícia Federal e de outras entidades, garantindo a transparência do processo.

Desinformação: Falta de comprovante impresso torna o sistema não auditável.

Esclarecimento: Ao contrário do que se alega, a urna eletrônica brasileira possui diversos mecanismos de auditoria que garantem a verificação da integridade do processo eleitoral em diferentes etapas. Esses mecanismos incluem o Registro Digital do Voto (RDV), o *Log* da Urna Eletrônica, auditorias pré e pós-eleitorais, auditoria do código-fonte, lacração dos sistemas, tabela de correspondência, lacre físico, auditoria de votação (votação paralela) e oficialização dos sistemas.

Desinformação: Urna eletrônica pode ser programada para favorecer candidatos.

Esclarecimento: Essa é uma alegação que surge frequentemente em períodos de polarização política. A Justiça Eleitoral tem se dedicado a desmentir essas informações, como a alegação de que a urna desbloquearia um candidato secreto se o eleitor pressionasse a tecla 5. Essas narrativas exploram a desconfiança no resultado eleitoral, mas não possuem qualquer fundamento.

Desinformação: Fraude nos resultados das eleições.

Esclarecimento: Essa categoria engloba diversas alegações falsas, como ataques à credibilidade do TSE e de outras autoridades eleitorais, questionando sua imparcialidade e integridade. Também inclui narrativas falsas sobre os resultados das eleições e a contagem de votos, muitas vezes disseminadas logo após a divulgação dos resultados, alegando, por exemplo, que um candidato teria obtido uma porcentagem de votos diferente daquela divulgada oficialmente.

Desinformação: Sistema do TSE foi invadido por *hackers*.

Esclarecimento: Essa *fake news* busca atribuir a manipulação do processo eleitoral a atores externos, como *hackers* estrangeiros. Teorias da conspiração envolvendo interferência estrangeira são veiculadas, apelando a sentimentos nacionalistas e sendo usadas para justificar derrotas eleitorais. No entanto, não há evidências que corroborem essas alegações.

Desinformação: Mesários podem votar no lugar de eleitores faltosos.

Esclarecimento: Essa alegação é falsa. O mesário só pode liberar a urna para votação quando o eleitor está presente, apresenta um documento original com foto e informa a data de nascimento. A liberação sem biometria é apenas uma alternativa para casos em que a identificação digital falha, mas sempre com a presença física do eleitor.

Desinformação: Urnas já vêm com votos inseridos antes da eleição.

Esclarecimento: Esse boato é desmentido pela Justiça Eleitoral. Antes do início da votação, cada urna imprime a "zerésima", um relatório que comprova que ela está com zero votos registrados. Esse documento pode ser acompanhado por qualquer pessoa presente na seção eleitoral.

Desinformação: Urnas eletrônicas não são auditáveis.

Esclarecimento: Essa é uma alegação comum, mas incorreta. As urnas eletrônicas são auditáveis em diversas etapas. O Tribunal Superior Eleitoral (TSE) realiza procedimentos como o Teste Público de Segurança (TPS), disponibiliza o código-fonte para inspeção de entidades fiscalizadoras e emite o Boletim de Urna, que permite a conferência dos votos.

Desinformação: Voto nulo ou branco para um dos cargos anula a votação para outro cargo.

Esclarecimento: Essa é uma narrativa falsa que busca gerar confusão entre os eleitores. O voto nulo ou branco para um cargo eletivo (como vereador, prefeito, governador ou senador) não anula os votos para outros cargos, como o de presidente. Cada cargo é considerado de forma independente na urna eletrônica.

A seguir são apresentadas informações a respeito da urna eletrônica e de todos os sistemas e procedimentos de segurança e de auditoria envolvidos no processo eleitoral.

SEGURANÇA DO PROCESSO ELEITORAL E AUDITORIAS

7. SEGURANÇA DO PROCESSO ELEITORAL E AUDITORIAS[3]

7.1. Como surgiu a urna eletrônica?

Afinal, a urna eletrônica é segura? Essa é uma dúvida frequente, principalmente durante o período eleitoral. Mas nos últimos anos, com a popularização das redes sociais e das desinformações que por elas circulam, essa pergunta transformou a urna em alvo de diversas teorias conspiratórias.

Por isso, é necessário compreender os mecanismos e processos que tornam a votação brasileira segura.

Retrospectivamente, verifica-se que o processo eleitoral brasileiro vem se desenvolvendo no sentido de ampliar a segurança na votação e garantir o sigilo do voto, permitindo aos brasileiros escolherem livremente seus candidatos, de forma a inibir coerções e fraudes.

Em 1986, a Justiça Eleitoral realizou o recadastramento de eleitores, iniciando o processo de informatização dos dados do cadastro eleitoral: os fichários e os dados sem interligação cederam lugar a um banco de dados informatizado. Esse foi o primeiro passo para impedir fraudes. Antes, os partidos registravam eleitores no momento da votação e, com isso, falsidades na identificação do eleitor eram comuns, como a utilização de documentos de pessoas falecidas para votar.

[3] Conteúdo adaptado do curso Segurança do Processo Eleitoral e Auditoriais - 2024.

Contudo, os processos de votação e apuração permaneceram em formato analógico, ou seja, por meio de cédulas, que dependiam da contagem manual dos votos. Além de demorado, esse processo dava margem a erros na contagem, seja por falha humana, por má-fé ou por preenchimento dúbio da cédula de votação por eleitoras e eleitores. Em uma eleição municipal, em que poucos votos são capazes de definir o resultado, os erros na contagem poderiam alterar completamente o resultado.

É preciso salientar que as fraudes não se restringiam às eleições municipais. Um caso emblemático aconteceu nas eleições de 1994, quando eram disputados os cargos de Deputado Estadual e Deputado Federal. À época, na 25ª Zona Eleitoral do Rio de Janeiro, responsável pela zona oeste da cidade, 90% das urnas de lona apresentaram resultados corrompidos. Foi necessário trocar a equipe de escrutinadores e reforçar a fiscalização, em uma apuração que perdurou por 13 dias.

Você sabia? O pesquisador Jairo Nicolau conta como era o sistema eleitoral brasileiro antes da informatização[4]:

> "A fraude era generalizada, ocorrendo em todas as fases do processo eleitoral (alistamento dos eleitores, votação, apuração dos votos, e reconhecimento dos eleitores)."
>
> "Os principais instrumentos de falsificação eleitoral foram o bico de pena e a degola."

Como era a votação por cédulas?

Curiosidade: conheça as cédulas.

Na votação por cédulas, devido à interferência humana, a possibilidade de fraude era muito presente. Dessa forma, o processo eleitoral era vulnerável a falhas, intencionais ou não. Além disso, como as pessoas que contavam os votos (escrutinadores) faziam esse trabalho manualmente, o processo de apuração poderia levar dias ou semanas para ser concluído.

[4] NICOLAU, Jairo. A história do voto no Brasil. Rio de Janeiro: Jorge Zahar, 2002, p. 34.

Na apuração por cédulas, outro problema acontecia com frequência: o escrutinador não entendia o que foi escrito pelo eleitor. Por exemplo, confundia o número 5 com o número 8. Assim, a cada cédula mal preenchida, qualquer dúvida que houvesse sobre a real intenção do eleitor gerava uma discussão entre os fiscais dos partidos e os escrutinadores, que podia se arrastar por muito tempo. E, muitas vezes, essa discussão resultava na anulação de votos e, por vezes, da urna inteira.

Figura 2 - Tipos de fraudes nas eleições

Fonte: Adaptado de TSE (2025).

Tipos de fraudes nas eleições por meio de cédulas de papel

Cometidas pelo eleitor:

Antes da votação:

- Sumiço de urnas

Antes de chegar aos locais de votação, as urnas oficiais eram substituídas por outras repletas de cédulas preenchidas.

- Roubo das urnas

Antes de chegar aos locais de votação, as urnas oficiais eram roubadas e, assim, inviabilizava-se a votação em determinadas seções eleitorais.

Durante a votação:

- Voto pré-preenchido

As cédulas do estoque de segurança das seções eleitorais eram roubadas e, então, preenchidas e inseridas nas urnas.

- Voto "formiguinha"

O eleitor recebia a cédula do mesário, entrava na cabina de votação e, em vez de preenchê-la e depositá-la, guardava a cédula em branco e colocava um papel qualquer na urna de lona. O organizador da fraude, que estava fora da seção, recebia a cédula oficial, assinalava os candidatos desejados e a entregava para outro eleitor. Esse eleitor depositava a cédula já preenchida, pegava outra em branco e a entregava para o organizador, que repetia o processo fraudulento à exaustão.

- Uma pessoa votando no lugar de outra

O eleitor apresentava documento falso para se identificar na seção eleitoral e votar. Dessa forma, era possível que uma mesma pessoa votasse mais de uma vez em mais de uma seção eleitoral. Era possível, até mesmo, votar em nome de pessoas já falecidas.

Cometidas pelo escrutinador:

Durante a apuração:

- Registro da apuração da urna no mapa eleitoral

Os votos eram registrados em mapas eleitorais após serem contados. A fraude ocorria de duas maneiras: a pessoa que informava os números da apuração para serem registrados no mapa eleitoral (escrutinador) "cantava os votos", ou seja, "falava em voz alta" números errados para serem registrados no mapa; a outra maneira era a pessoa responsável por escrever os votos no mapa registrar valores diferentes dos votos cantados.

- Preenchimento dos votos em branco

No momento da votação, os votos eram marcados com caneta azul. Na apuração, utilizava-se caneta vermelha para identificar as cédulas apuradas. Nesse momento, ao se deparar com votos em branco, o apurador os preenchia com caneta azul.

- Nome e número diferentes

As cédulas que continham apenas o nome do candidato eram preenchidas, pelo escrutinador, com o número de outro candidato. Com isso, os votos eram anulados, pois não se tornava possível identificar, com segurança, para qual candidato o voto havia sido consignado.

Você sabia?

Já aconteceu de cédulas voarem da mesa onde acontecia a apuração por causa de um ventilador ligado.

Também já aconteceu de acharem cédulas no bolso de escrutinadores, e até mesmo o incrível caso do escrutinador que engoliu a cédula.

A evolução da urna eletrônica

A urna eletrônica surgiu, então, para sanar essas inconformidades. Foi nas eleições de 1996 que 57 cidades brasileiras utilizaram, pela primeira vez, a urna eletrônica. Nessa primeira fase, a urna já emitia um boletim após o encerramento do pleito, permitindo saber o resultado da votação em cada uma das seções eleitorais.

No **pleito de 1998**, 537 municípios (eleitorado superior a 40.500 eleitores), totalizando 61.111.922 eleitores, votaram pelo sistema eletrônico, em 166.937 urnas. Em Santa Catarina foram 13 municípios e 4.462 equipamentos.

O progressivo desenvolvimento do voto informatizado atingiu seu ápice nas eleições municipais de 1º **de outubro de 2000**, quando o processo foi estendido, com sucesso, a todos os municípios do Brasil. Nesse ano, 100% do eleitorado valeu-se da urna eletrônica para a votação, em 353.737 equipamentos. A partir daí, todas as eleições subsequentes foram realizadas por meio do sistema informatizado.

Mas as inovações não pararam por aí. A cada eleição, a urna eletrônica e os processos que envolvem a votação incorporam novas tecnologias e conceitos da segurança da informação, sempre acompanhando a evolução tecnológica.

As eleições brasileiras servem de modelo para todo o mundo, não apenas pelos mecanismos de segurança empregados, mas especialmente por permitir que todo o processo seja acompanhado pela sociedade, prestando um serviço transparente, eficiente e ágil. Enfim, **segurança** e **transparência** são os princípios que norteiam a atuação da Justiça Eleitoral.

Atenção!

O processo eletrônico de votação possui **mais de 30 barreiras de segurança**, que vão além do *software* e do *hardware* da urna, pois envolvem todos os processos ligados a essa grande empreitada que é a eleição.

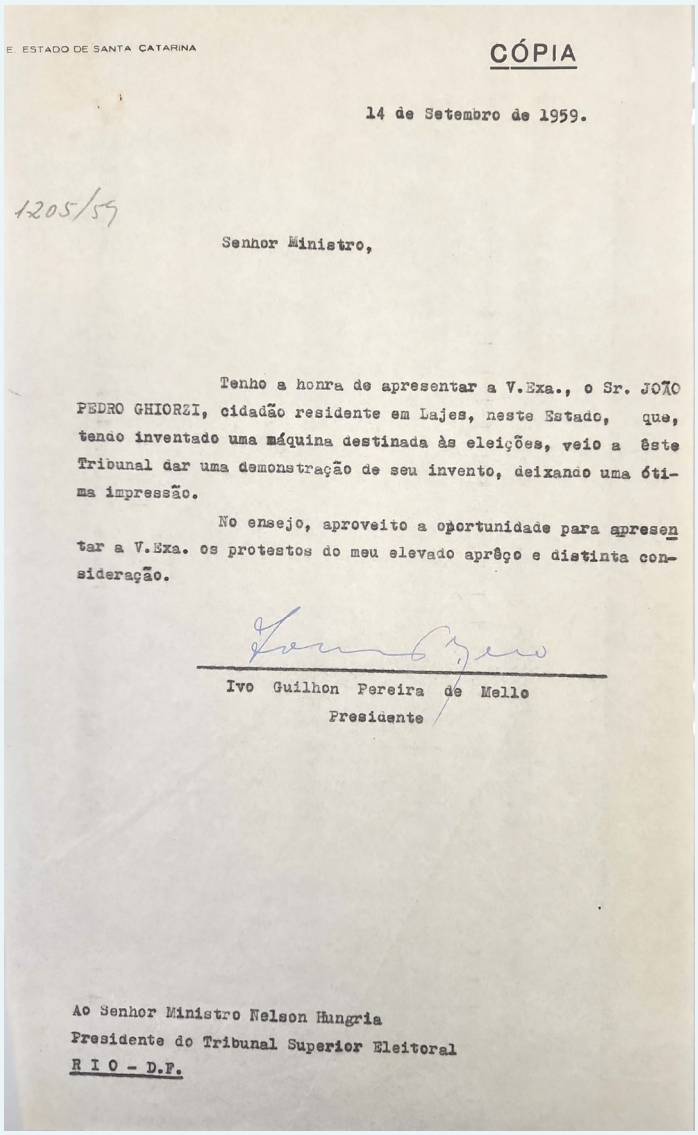
Curiosidades históricas

O interesse em facilitar a votação e prevenir fraudes em eleições é mais antigo do que pode parecer!

Em Santa Catarina, no ano de 1959, um cidadão do município de Lages veio até o TRE-SC para demonstrar seu invento: "uma máquina destinada às eleições".

O senhor João Pedro Ghiorzi parece ter convencido a equipe do Tribunal, a ponto de o presidente à época, Des. Ivo Guilhon Pereira de Mello, enviar ofício ao presidente do TSE relatando a "ótima impressão" causada pela invenção.

Figura 3 - Ofício ao presidente do Tribunal Superior Eleitoral



E. ESTADO DE SANTA CATARINA

CÓPIA

14 de Setembro de 1959.

1205/59

Senhor Ministro,

Tenho a honra de apresentar a V.Exa., o Sr. JOÃO PEDRO GHIORZI, cidadão residente em Lajes, neste Estado, que, tendo inventado uma máquina destinada às eleições, veio a êste Tribunal dar uma demonstração de seu invento, deixando uma ótima impressão.

No ensejo, aproveito a oportunidade para apresentar a V.Exa. os protestos do meu elevado aprêço e distinta consideração.

Ivo Guilhon Pereira de Mello
Presidente

Ao Senhor Ministro Nelson Hungria
Presidente do Tribunal Superior Eleitoral
R I O - D.F.

Fonte: TRE-SC (1959).

Mas foi na década de 1990 que ocorreu o primeiro evento oficial da Justiça Eleitoral em que foram utilizadas exclusivamente a votação e a apuração eletrônicas. Trata-se do plebiscito para emancipação do distrito de Cocal do Sul do município de Urussanga, ocorrido em 31 de março de 1991. Abaixo, veja como era a tela para votação na consulta plebiscitária:

Figura 4 - Tela para votação na consulta plebiscitária

Fonte: TRE-SC (1991).

Como se vê, a busca por um sistema de votação totalmente informatizado é antiga. Com o passar do tempo, muitas ações contribuíram para essa conquista. A cada inovação no processo de votação, escreve-se parte dessa história!

7.2. Segurança na produção

Fabricação, certificação e autenticação da urna eletrônica

A segurança das urnas eletrônicas já começa antes mesmo da sua produção. Inicia-se na elaboração do edital de aquisição, onde já são definidos os requisitos mínimos de seguranças que devem ser atendidos. O tipo de aquisição é concorrência na modalidade técnica e preço, e durante a fase técnica as empresas concorrentes entregam um modelo de engenharia que já possui os requisitos de segurança necessários para que a comissão de avaliação técnica verifique se a concorrente possui a capacidade de produção de uma urna eletrônica segura.

O *hardware* é produzido pela empresa vencedora da licitação, mas com uma série de restrições e controles por parte da Justiça Eleitoral. Já os sistemas são desenvolvidos integralmente pelo TSE.

Nos projetos de *hardware* e *software* da urna eletrônica, há um fator crucial de segurança: eles são **dedicados exclusivamente à eleição**, ou seja, a urna possui somente os mecanismos necessários para a votação e apuração, não sendo possível utilizá-la para qualquer outro fim.

Para melhor compreensão, leia o texto abaixo, produzido pela Unidade Técnica[5] do TSE e adaptado pelo TRE-SC.

Fabricação

A empresa que vence a licitação deve fabricar as urnas conforme as **especificações técnicas determinadas pelo TSE**. Além disso, técnicos da Justiça Eleitoral acompanham o processo de produção para garantir que todos os requisitos de qualidade e segurança sejam atendidos.

As empresas Unisys, Diebold/Procomp e Positivo já foram as responsáveis pela fabricação da urna eletrônica.

Por questões de segurança, as urnas saem de fábrica podendo executar apenas o *software* de certificação que é desenvolvido pelo TSE, e somente as teclas BRANCO e CORRIGE estão habilitadas.

Após a fabricação, as urnas eletrônicas são auditadas pelos técnicos da Justiça Eleitoral. Elas são separadas em lotes. As urnas dos primeiros lotes são todas verificadas e, a partir do momento em que há uma estabilidade na aceitação desses lotes, passa-se a fazer auditoria por amostragem.

Somente após serem aprovados nas auditorias técnicas é que os lotes de urnas eletrônicas serão enviados para os locais de armazenamento de cada TRE.

[5] Seção de Gestão de Certificação Digital/Coordenadoria de Tecnologia Eleitoral/Secretaria de Tecnologia da Informação (SGCD/COTEL/STI)

Certificação

Para cada urna fabricada, o TSE emite um certificado digital correspondente, **atestando que ela é um equipamento oficial da Justiça Eleitoral**. Portanto, a urna eletrônica apenas é reconhecida como um equipamento da Justiça Eleitoral após a certificação e somente passará a executar os demais *softwares* desenvolvidos pelo TSE a partir desse momento.

Mas como é realizado esse processo de certificação?

Quando as urnas são recebidas em seus locais de armazenamento, são instalados os "certificados digitais" emitidos pela Autoridade Certificadora (AC) da Justiça Eleitoral. São inseridas na urna eletrônica uma mídia com o programa de certificação e outra com os certificados digitais. O certificado digital é enviado para o *chip* de segurança, que é um processador à parte responsável por auditar a urna eletrônica.

Estes certificados são gerados para cada urna eletrônica, a partir de requisições feitas em sua fabricação e enviadas à Autoridade Certificadora. **Em urnas que não estejam certificadas não é possível executar os sistemas eleitorais**.

Uma autoridade certificadora é um ente confiável para certificar um determinado processo digital.

A AC da Justiça Eleitoral foi criada usando equipamentos e políticas de segurança similares aos utilizados por autoridades subordinadas à Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Autenticação

Após a certificação, ocorre o processo de autenticação. Nele, os **certificados digitais instalados nas urnas são validados**, ou seja, é verificado se eles realmente foram emitidos pela Justiça Eleitoral.

Para ilustrar, seria como um cartório de registro carimbando e assinando um documento após a conferência da assinatura de alguém que tem ali sua "firma" reconhecida.

Atualizações de *firmware*

Firmware é uma classe específica de *software* que executa a configuração e o controle dos componentes de *hardware*. Basicamente, é um programa de computador que faz o *hardware* funcionar.

O *firmware* é encontrado, praticamente, em qualquer eletrodoméstico com certa tecnologia, como fornos de micro-ondas, televisores, tocadores de DVD, dentre outros. Ele garante o básico do funcionamento desses equipamentos. É por causa dele que, por exemplo, um micro-ondas possui a função de contagem regressiva do tempo de cozimento.

Agora, vamos entender como isso funciona na urna eletrônica. Em cada urna, há **quatro dispositivos eletrônicos de segurança** que, entre outras funcionalidades:

- asseguram que os certificados digitais estão armazenados corretamente;
- possibilitam a assinatura digital de dados e *softwares*, bem como sua respectiva verificação;
- cifram (ou seja, codificam) as comunicações entre a placa-mãe da urna e seus periféricos mais críticos – teclado do eleitor, terminal do mesário e impressora;

A partir dos modelos mais novos da urna eletrônica, UE2020 e UE2022, o leitor biométrico passou a ser o periférico crítico a ter suas comunicações codificadas, ao invés do terminal do mesário.

Em cada um desses dispositivos, está gravado o *firmware*, que implementa essas funcionalidades. Ou seja: cada urna eletrônica recebida após sua fabricação possui uma versão inicial de *firmware*. Em caso de necessidade, esse *firmware* pode ser atualizado. Essas atualizações são disponibilizadas como versões novas do *firmware*, assinadas digitalmente pelo TSE. Uma atualização só é aceita pela urna eletrônica caso a verificação da assinatura digital seja bem-sucedida.

Geração da chave de *kernel*

Primeiramente, assim como usamos os sistemas operacionais nos computadores (*Windows*, *Mac OS X*, *Linux*, etc), a urna eletrônica também utiliza um sistema operacional. Trata-se de um sistema próprio, chamado "UENUX", que o TSE desenvolveu tendo como base o sistema *Linux*.

Já o *kernel* é como se fosse a versão mais básica de um sistema operacional. Por analogia, seria como o cérebro de um computador, responsável pela ligação entre o *hardware* (parte física) e o *software* (parte lógica). Assim que a urna é ligada, o *kernel* é acionado e detecta todo o *hardware* e o que ela precisa para funcionar (microterminal, módulo impressor, placa de vídeo, etc). Depois que o UENUX é carregado, o *kernel* assume a função de organizar tudo o que acontece: gerenciar processos, arquivos, dispositivos periféricos, etc.

A geração da chave de *kernel* consiste, portanto, na geração de uma chave de criptografia que é usada para decifrar o sistema da urna eletrônica (UENUX). Em outras palavras, a geração dessa chave de segurança garante que **somente o sistema UENUX seja decifrado na urna eletrônica**. Qualquer tentativa de utilização de outro sistema será frustrada.

Assim como a certificação, esse procedimento é requisito para que as urnas eletrônicas executem os sistemas eleitorais.

Desenvolvimento dos sistemas

Todos os sistemas utilizados nas urnas eletrônicas – para os processos de votação, apuração e totalização – são integralmente desenvolvidos pelo TSE.

Antes e depois de assinados digitalmente e lacrados, os sistemas são testados por várias equipes: pela própria equipe de desenvolvimento, por equipe dedicada no TSE e pelos TREs.

Além disso, para garantir a legitimidade do processo eleitoral, os sistemas passam por auditorias de entidades fiscalizadoras. Esse assunto será detalhado no item 7.4, "Transparência nos procedimentos", mas não há como falar sobre o desenvolvimento dos sistemas sem falar do papel dessas entidades.

Disponibilização dos códigos-fonte

Para começar, **a partir de 12 meses antes do 1º turno das eleições**, a Justiça Eleitoral abre a possibilidade de as entidades fiscalizadoras acessarem o código-fonte dos programas, em ambiente controlado no TSE. Lá, elas podem acompanhar as fases de especificação e desenvolvimento dos sistemas eleitorais pela equipe técnica do Tribunal.

Anteriormente, esse prazo era de 6 meses antes do 1º turno das eleições, tendo sido ampliado no ano de 2021.

Em 2022, o TSE ampliou a **disponibilização dos códigos-fonte dos sistemas eleitorais**, de forma que algumas entidades fiscalizadoras possam fazer a inspeção em suas próprias dependências, dispensando-se o comparecimento no TSE.

O objetivo da publicação dos códigos-fonte dos *softwares* eleitorais é ampliar seu acesso para a comunidade acadêmica e especializada, a fim de aumentar a confiabilidade no processo eletrônico de votação, bem como receber contribuições para a melhoria do *software*. Trata-se da medida 5, prevista no Plano de ação para ampliação da transparência do Processo Eleitoral.

Espera-se que a iniciativa proporcione conhecimento e debate nos meios acadêmicos e especializados, de modo a gerar repercussão na sociedade civil e reduzir a propagação das chamadas *fake news* e de notícias especulativas.

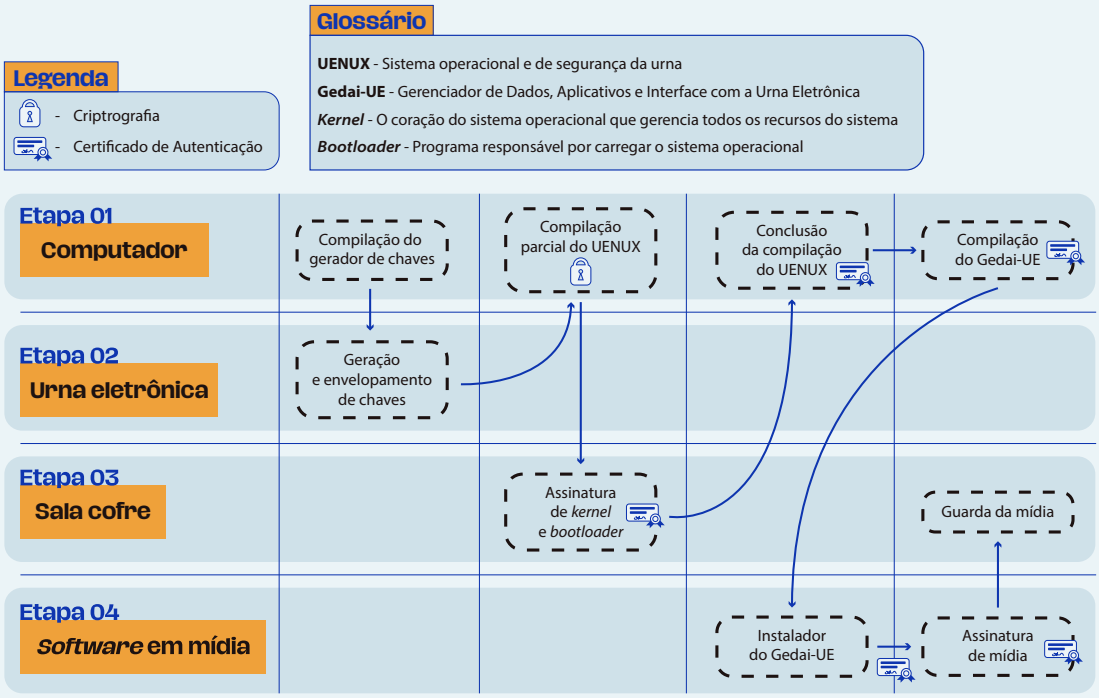
Cerimônia de Assinatura Digital e de Lacração dos Sistemas

A **versão final dos sistemas** é apresentada nesta cerimônia, que ocorre aproximadamente um mês antes das eleições. Além disso, essas versões finais são assinadas digitalmente e lacradas fisicamente. Basicamente, os sistemas passam pelas seguintes etapas:

1. **Apresentação**.
2. **Compilação**.
3. **Assinatura digital**: os representantes do TSE assinam digitalmente os programas, bem como as entidades fiscalizadoras que demonstrarem interesse.
4. **Lacração**: guarda das mídias pelo TSE.

Para entender melhor, veja um resumo dessas etapas, tomando o Sistema Gedai-UE como exemplo:

Figura 5 - Resumo das etapas da Cerimônia de Assinatura Digital e Lacração dos Sistemas



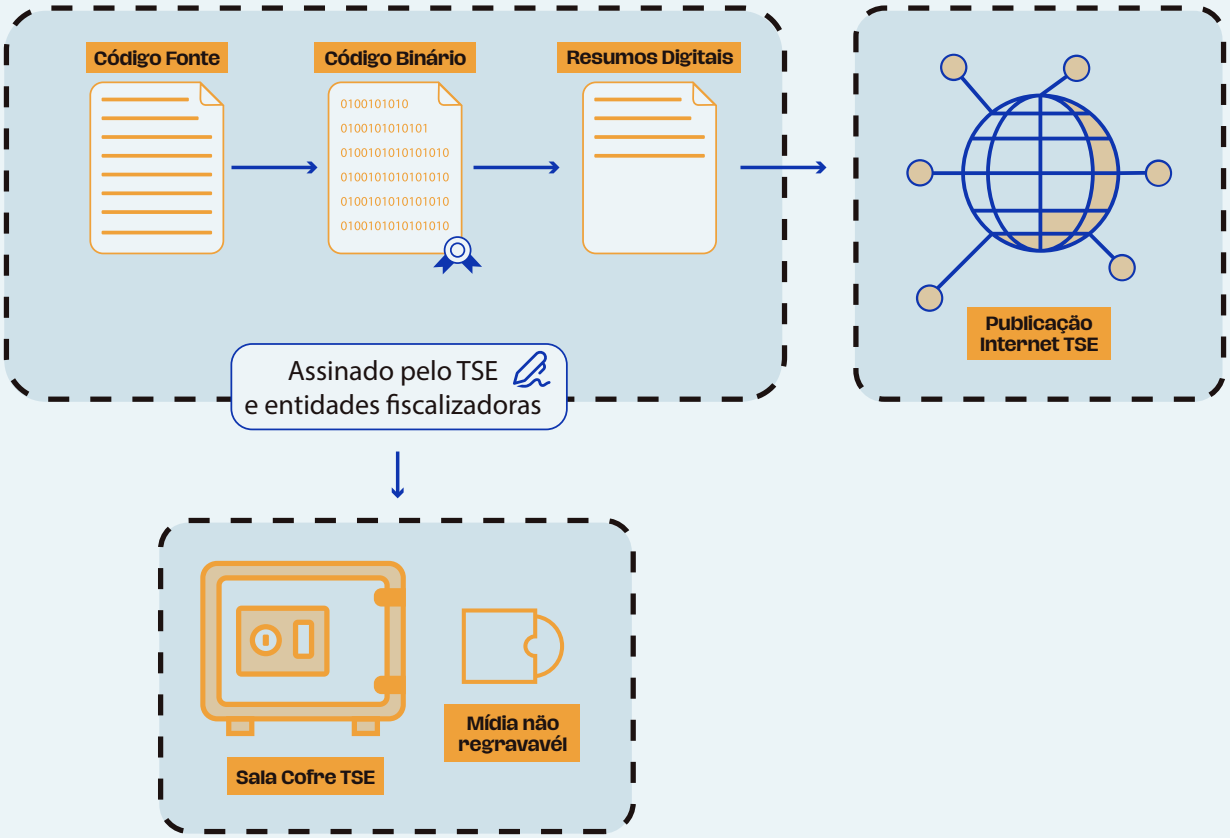
Fonte: Adaptado de TSE (2025).

Após a compilação e a assinatura digital, são calculados os resumos digitais (*hashes*) de todos os programas-fonte, programas executáveis, arquivos fixos dos sistemas, arquivos de assinatura digital e chaves públicas. As cópias desses resumos digitais são entregues aos representantes das entidades presentes na cerimônia, bem como publicadas na página do TSE.

Nesta cerimônia, além dos sistemas eleitorais, também os programas de verificação desenvolvidos pelas entidades fiscalizadoras são apresentados, compilados, assinados digitalmente e lacrados.

Entenda resumidamente como ocorre esse procedimento de assinatura e lacração dos sistemas:

Figura 6 - Resumo do procedimento de assinatura e lacração dos sistemas



Fonte: Adaptado de TSE (2025).

O que acontece se for descoberto um erro em um sistema que já havia sido assinado digitalmente e lacrado?

Será necessário relatar essa ocorrência às entidades fiscalizadoras e a nova versão do sistema precisará passar novamente pelos procedimentos de apresentação, compilação, assinatura digital e lacração.

Teste Público de Segurança (TPS)

Além das auditorias internas e externas, um importante evento para melhorias no desenvolvimento dos sistemas é o Teste Público de Segurança (TPS).

Nele, os mecanismos de segurança da urna eletrônica são postos à prova: o TSE abre o código-fonte dos programas eleitorais para que especialistas, previamente inscritos para o procedimento, realizem tentativas de violação, buscando por possíveis problemas. Em alguns casos, inclusive, várias barreiras de segurança são desativadas para que os investigadores possam executar seus planos.

Basicamente, a urna eletrônica é submetida a *hackers*, que tentam violar suas barreiras de segurança.

Uma vez identificados problemas ou fragilidades, eles serão resolvidos antes da realização das eleições. O TSE realiza as correções e convida novamente os investigadores para executarem novo teste e verificarem se a vulnerabilidade foi corrigida.

O TSE é precursor na realização desse procedimento, que tem o objetivo de fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos, bem como propiciar melhorias no processo eleitoral.

O primeiro teste de segurança ocorreu em 2009; a segunda edição, em 2012.

A Resolução TSE n. 23.444/2015 tornou periódica a realização do TPS nos sistemas eleitorais, determinando que eles sejam realizados antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.

Após essa Resolução, foram realizadas mais cinco edições: em 2016, 2017, 2019, 2021 e 2023. Durante a elaboração deste guia está em andamento o TPS edição 2025.

Para mais informações sobre o TPS, visite o *site* Teste Público de Segurança da Urna e consulte o guia Teste público de segurança da urna: guia para jornalistas.

7.3. Segurança tecnológica

Métodos de proteção dos dados

A votação com a urna eletrônica foi um grande avanço para a lisura do processo eleitoral e a rapidez na apresentação dos resultados. Em contrapartida, por se tratar de um conjunto de sistemas computacionais, é essencial garantir a segurança dos dados.

Para tanto, os sistemas eleitorais e a urna eletrônica utilizam métodos de segurança aplicados no mundo inteiro para o tráfego de dados. São eles: criptografia, *hash* e assinatura digital.

Como você perceberá, o grande diferencial desses mecanismos na esfera eleitoral é a sua aplicação em **várias camadas e vários níveis de segurança**. Quer saber mais?

Recomenda-se a leitura do art. 2º da Resolução TSE n. 23.673/2021 para conhecer os conceitos de vários termos que serão mencionados nesta etapa do curso.

Veja o vídeo sobre criptografia.

Criptografia

Em síntese, criptografia é a técnica para cifrar um texto, de forma a impedir a sua interpretação por terceiros, ou seja, é um mecanismo de proteção do conteúdo da mensagem.

A criptografia foi utilizada desde tempos remotos em operações militares, políticas e diplomáticas. Hoje, além desses usos seculares, também é usada para a proteção de dados informatizados, incluindo os da urna eletrônica.

Mas onde ela é utilizada na urna?

- **Imagem do kernel do UENUX**: o UENUX é o sistema operacional da urna eletrônica. A proteção criptográfica impede a sua execução fora da UE.
- **Chaves da urna**: a criptografia garante que as chaves sejam usadas somente na urna eletrônica. Além disso, só quem possui as chaves consegue ler os dados.
- **Sistema de arquivos da urna**: a criptografia resguarda contra a cópia indevida.
- **Biometrias dos eleitores**: são criptografadas e decifradas somente na urna.
- **Boletim de urna**: é criptografada a parte do BU que possui os resultados da seção eleitoral e só pode ser decifrada pelo Sistema de Totalização.
- **Registro Digital do Voto (RDV)**: arquivo em que os votos são gravados por ordenação lexicográfica dentro de cada cargo (ordenação pelo número do candidato), dessa forma preservando o sigilo do voto. Utiliza criptografia com AES-CBC 256 bits durante a votação (veja um exemplo da força da criptografia AES clicando aqui).

Saiba mais sobre a criptografia utilizada nos Boletins de Urna!

"A criptografia digital é um mecanismo de segurança para o funcionamento dos programas computacionais. Como os dados tornam- se embaralhados, eles ficam inacessíveis a pessoas não autorizadas.

O Tribunal Superior Eleitoral usa algoritmos proprietários de cifração simétrica e assimétrica, de conhecimento exclusivo do TSE.

O boletim de urna é criptografado de forma segmentada, assinado digitalmente e transmitido.

Além da criptografia, existe a descriptografia, que é o processo pelo qual são recuperados os dados previamente criptografados, isto é, eles são desembaralhados. É 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 Totalizador;
- a descriptografia do BU de forma segmentada;
- a leitura do BU descriptografado;
- o armazenamento do BU criptografado e descriptografado."

Fonte: TSE.

Hash ou resumo digital

Qualquer arquivo digital, seja um programa ou banco de dados, forma um conjunto de caracteres (letras, números, sinais, etc.) que pode ser bastante extenso. Então, é possível aplicar uma função matemática para criar um outro grupo de caracteres que "resume" o conteúdo do arquivo original. O nome desse conjunto gerado é **código *hash*** ou **resumo digital**.

Para que tenha utilidade, a função algorítmica que calcula (ou gera) o *hash* deve dificultar ao máximo que dois arquivos diferentes tenham o mesmo resumo digital. Mais importante ainda: a função deve garantir que arquivos semelhantes tenham *hashes* claramente distintos, **permitindo a rápida verificação de arquivos alterados**.

Observe, no exemplo a seguir, como a alteração de um único caractere (de "T" para "t") gerou um *hash* completamente diferente:

Figura 7 - Exemplo na alteração de caractere

Conjunto de caracteres	Resumo digital ou *hash*
TSE	90083b903950e09c7e3152ff016d1d416696b03665ac5696298f23ab7e5660545c5adba65ecfb46710d88aa85222fecaa4617474fd4b30e2737e04acd36e54cf
tSE	6338fcf67f4ef34686d2b2eb65b8c265e23d920e508d638ae7e5540f9f4e75062f1988c10f53e5adc307d48993f390e4120b4d2e117a3ef503055ab7a35add92

Fonte: Adaptado de TSE (2025).

Na cerimônia de lacração dos sistemas, são gerados *hashes* que serão usados para verificar a **integridade** e **autenticidade** dos sistemas oficiais da eleição instalados em qualquer urna ou computador da Justiça Eleitoral. Qualquer mudança neles, por mínima que seja, deixaria rastros e poderia ser identificada ao se confirmarem os *hashes*.

Na prática, o que é conferido?

Os aplicativos de verificação exibirão ou imprimirão os *hashes* dos arquivos dos sistemas eleitorais, que deverão ser conferidos visualmente com os *hashes* publicados no *site* do TSE, na página Resumos digitais (*hashes*) dos sistemas eleitorais. Como cada sistema é composto por uma série de arquivos, são vários resumos digitais para conferir.

Veja um exemplo: abaixo há a imagem do relatório impresso pelo aplicativo Verificador Pré e Pós-Eleição (VPP), onde aparecem os *hashes* dos arquivos estáticos (executáveis, bibliotecas de aplicações e do sistema operacional) contidos em uma urna eletrônica. Esses *hashes* podem ser comparados com os publicados na página do TSE.

Figura 8 - Comparação de *hashes* na página do TSE

Fonte: Adaptado de TRE-SC (2025).

Ficou interessado nessa conferência?

Consulte os resumos digitais dos sistemas das eleições de 2024.

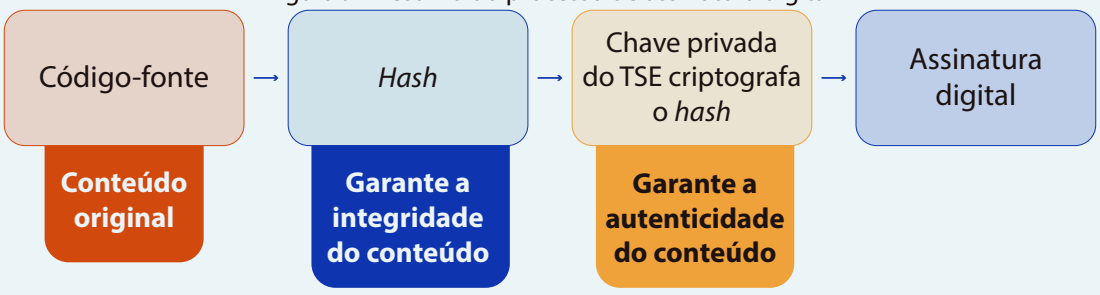
Assinatura Digital

A **assinatura digital** é uma forma de garantir a autoria e o conteúdo de um arquivo digital. Ela proporciona a mesma segurança que uma assinatura feita à mão. Para implementá-la, utiliza-se a combinação de uma função de *hash* com um mecanismo de criptografia com chave assimétrica.

A chave assimétrica é baseada em dois tipos de chaves de segurança: as públicas, que podem ser amplamente divulgadas; e as privadas, que devem ser conhecidas apenas pelo proprietário. Elas são usadas para cifrar mensagens e verificar a identidade de um usuário.

Uma vez assinado um arquivo, é impossível que outra pessoa assine o mesmo arquivo fazendo-se passar pelo signatário original. Assim, se o TSE e outras entidades assinarem digitalmente um arquivo, qualquer tentativa de alteração será detectada na conferência da assinatura digital.

Figura 9 - Resumo do processo de assinatura digital



Fonte: Adaptado de TSE (2025).

Como a assinatura digital é utilizada nos sistemas eleitorais?

Todos os **dados que integram o sistema da urna**, que a alimentam ou são produzidos por ela são protegidos por assinatura digital e não podem ser modificados.

Quanto aos **aplicativos da urna**, todos possuem assinaturas digitais e resumos digitais, que são verificados pelo *kernel* da urna antes da sua execução. As assinaturas e *hashes* servem para garantir que os sistemas usados na urna foram os mesmos assinados durante a Cerimônia de Lacração dos Sistemas Eleitorais.

Também os **dados que alimentam a urna**, como dados de eleitores e de candidatos, são protegidos por assinatura digital, para garantir que se mantenham íntegros e autênticos.

Ainda, os **arquivos de resultado da votação** possuem assinatura de *software* e de *hardware*. A assinatura em *hardware* consiste na atribuição de uma chave de assinatura diferente para cada urna eletrônica. Essa assinatura possibilita conferir se o resultado da votação foi mesmo gerado na urna de determinada seção eleitoral. Somente após essa verificação é que os dados serão decifrados e totalizados.

Também há outros dados que utilizam a assinatura digital, como os *logs* de operações feitas na urna, o registro digital do voto (RDV), entre outros.

Como a assinatura digital é utilizada na urna eletrônica?

Cada urna gera seis pares de chaves assimétricas, ou seja, de combinações de códigos de segurança conhecidos pelo TSE e pelos programas da urna eletrônica.

Essas chaves ficam protegidas na memória do dispositivo. Apenas as chaves públicas são enviadas nas requisições dos certificados digitais. Já as chaves privadas nunca saem dos dispositivos de segurança de cada urna eletrônica; afinal, ninguém vai colocar uma senha num cofre e sair por aí divulgando a senha para todo mundo, não é mesmo?

Nas cerimônias públicas, que ocorrem em diversos momentos do processo eleitoral, as assinaturas digitais e os *hashes* podem ser conferidos e validados por aplicativos desenvolvidos pelo TSE e pelas entidades fiscalizadoras (partidos políticos, MP, OAB, etc).

Para mais informações sobre assinatura digital, acesse a Cartilha de Segurança para Internet.

Outros dispositivos de segurança

Além dos métodos mencionados, foram desenvolvidas soluções específicas de segurança para o processo eletrônico de votação. Essas soluções compreendem desde a **segurança lógica** (de sistemas) até a **segurança física** (ou seja, tangível, concreta), tanto de computadores da Justiça Eleitoral quanto da própria urna eletrônica. Saiba mais sobre os dispositivos de segurança utilizados pela Justiça Eleitoral no **ANEXO II.**

Sistema de Controle de Versões

Todos os sistemas da urna são mantidos em uma ferramenta de controle de versões. Com isso, é possível saber quais alterações foram realizadas, quando e quem as realizou.

A verificação dos sistemas utilizados ocorre nas diversas cerimônias do processo eleitoral (geração de mídias, preparação de urnas, conferência das urnas, etc) e, por isso, é uma informação relevante nas atas dessas cerimônias.

Log da urna

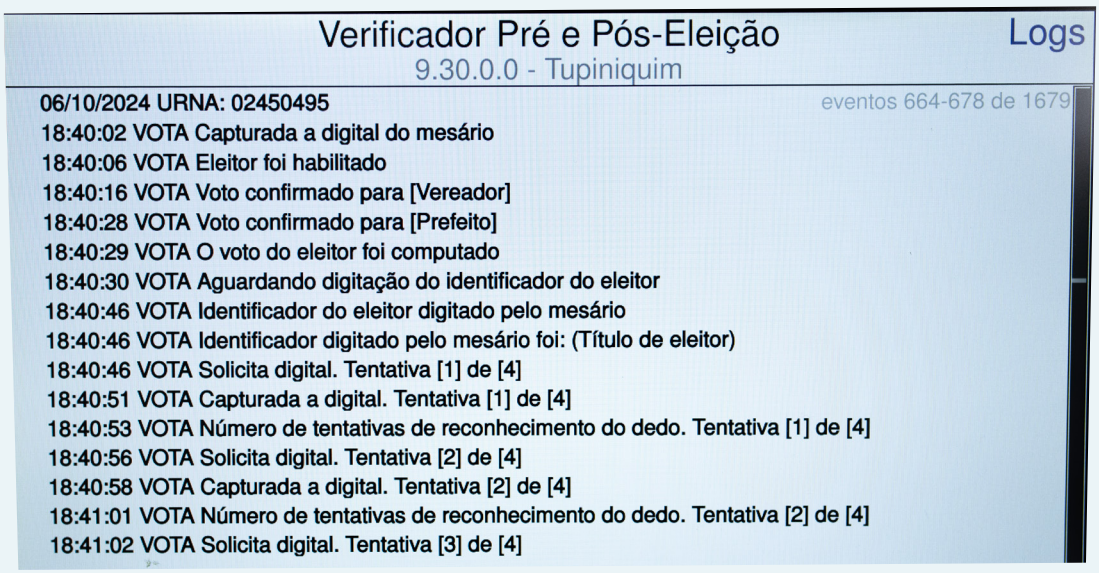
Todas as operações realizadas no *software* da urna eletrônica ficam registradas em ordem cronológica no arquivo de *log*. Com isso, é possível saber todo o histórico da urna, desde a sua preparação até o encerramento da votação.

São exemplos de operações registradas: aplicativos que foram executados, ajustes de data e hora, início e encerramento da votação, relatórios emitidos, procedimentos de contingência realizados, entre outros.

Além da segurança, os arquivos de *log* formam um valioso banco de dados para o TSE, utilizado para promover melhorias nos processos. É possível saber, por exemplo, a velocidade da votação, a dinâmica na utilização da biometria, o horário de impressão da zerésima, o horário de início da votação, etc.

O aplicativo Verificador Pré e Pós-Eleição (VPP), sobre o qual falaremos adiante, permite visualizar o *log* na tela da urna ou gravá-lo em uma mídia de resultado, conforme se vê nos exemplos abaixo.

Figura 10 - Exemplo de visualização do *log* na tela da urna eletrônica



Fonte: TRE-SC (2025).

Figura 11 - Relatório de *log* da urna gravado na MR (seção com biometria).

```
06/10/2024 16:22:54     INFO    02190993        VOTA    Capturada a digital. Tentativa [1] de [4]       15A8BC78C5DAF41C
06/10/2024 16:22:57     INFO    02190993        VOTA    Tipo de habilitação do eleitor [biométrica]     C8EDAD842116E48F
06/10/2024 16:22:57     INFO    02190993        VOTA    Eleitor foi habilitado  309C95BC4C7A9252
06/10/2024 16:23:07     INFO    02190993        VOTA    Voto confirmado para [Vereador] 85F97CBD53C7C242
06/10/2024 16:23:11     INFO    02190993        VOTA    Voto confirmado para [Prefeito] 3966060EC30442E0
06/10/2024 16:23:12     INFO    02190993        VOTA    O voto do eleitor foi computado 51AF9FF1BBF3EEA5
06/10/2024 16:23:13     INFO    02190993        VOTA    Aguardando digitação do identificador do eleitor        08107F23CD4C0924
06/10/2024 16:48:54     INFO    02190993        VOTA    Quantidade de memória livre [3.3 GB]    7509C6A2444B32A1
06/10/2024 16:48:54     INFO    02190993        VOTA    Espaço livre na MI [3.4 GB]     9ABB75A4C15B4579
06/10/2024 16:48:54     INFO    02190993        VOTA    Espaço livre na MV [350.7 MB]   79E256AA0D825AE9
06/10/2024 16:48:54     INFO    02190993        VOTA    Espaço utilizado na MI [14.6 MB]        D6F2AC8EF358D0EC
06/10/2024 16:48:54     INFO    02190993        VOTA    Espaço utilizado na MV [15.0 MB]        DB1AA1C198A1F2C5
06/10/2024 16:59:45     INFO    02190993        VOTA    Inspeção da urna iniciada       74DE84D8028BFA46
06/10/2024 16:59:53     INFO    02190993        VOTA    Inspeção da urna confirmada     9E7C97E738CFFAA2
06/10/2024 17:00:30     INFO    02190993        VOTA    Inspeção da urna terminada      9C198FFE777AF586
06/10/2024 17:00:30     INFO    02190993        VOTA    Aguardando digitação do identificador do eleitor        CB91FF3362D877FD
06/10/2024 17:00:43     INFO    02190993        VOTA    Operador indagado se todas as pessoas presentes votaram 2E964BEEEAE6BFD2
06/10/2024 17:00:46     INFO    02190993        VOTA    Todas as pessoas presentes já votaram? SIM      8B58431579D57822
06/10/2024 17:01:03     INFO    02190993        VOTA    Título digitado para encerramento: XXXXXXXXXXX AC352495B3211FA3
06/10/2024 17:01:05     INFO    02190993        VOTA    Procedimento de encerramento confirmado 1BFEE935C7F3A78C
06/10/2024 17:01:05     INFO    02190993        VOTA    Operador indagado se ocorrerá registro de mesários      6D81C21A8DBA5CBE
06/10/2024 17:01:10     INFO    02190993        VOTA    Operador confirmou para registrar mesários      AACFF33BBFF0B6A3
06/10/2024 17:01:10     INFO    02190993        VOTA    Registrando mesários após a votação     078D831FE7761E3E
06/10/2024 17:01:21     INFO    02190993        VOTA    Pedido de leitura da biometria do mesário XXXXXXXXXXX  C9D38C8BC8A31156
06/10/2024 17:01:26     INFO    02190993        VOTA    Mesário XXXXXXXXXXX é eleitor da seção D10567F24FD2508D
06/10/2024 17:01:26     INFO    02190993        VOTA    Mesário XXXXXXXXXXX registrado B70E506D974BACB0
06/10/2024 17:01:48     INFO    02190993        VOTA    Pedido de leitura da biometria do mesário XXXXXXXXXXX  2C1B74D441C8DF7C
06/10/2024 17:01:53     INFO    02190993        VOTA    Realizada a conferência da biometria do mesário 8487A7DD0C1D6EC4
06/10/2024 17:01:53     INFO    02190993        VOTA    Mesário XXXXXXXXXXX é eleitor da seção B34EA6DD9329A2A9
06/10/2024 17:01:53     INFO    02190993        VOTA    Mesário XXXXXXXXXXX registrado C6A8244881F783F2
06/10/2024 17:02:08     INFO    02190993        VOTA    Pedido de leitura da biometria do mesário XXXXXXXXXXX  83D841EF977CBBAA
06/10/2024 17:02:12     INFO    02190993        VOTA    Realizada a conferência da biometria do mesário 94E68AF75D8F2272
06/10/2024 17:02:12     INFO    02190993        VOTA    Mesário XXXXXXXXXXX é eleitor da seção 1377654510AC8657
06/10/2024 17:02:13     INFO    02190993        VOTA    Mesário XXXXXXXXXXX registrado 746573D95EC437B6
06/10/2024 17:02:26     INFO    02190993        VOTA    Pedido de leitura da biometria do mesário XXXXXXXXXXX  161BAD74B23BAD3E
06/10/2024 17:02:31     INFO    02190993        VOTA    Mesário XXXXXXXXXXX não é eleitor da seção      0B64EC6535E42328
06/10/2024 17:02:32     INFO    02190993        VOTA    Mesário XXXXXXXXXXX registrado 311A38C08DF9355F
06/10/2024 17:02:40     INFO    02190993        VOTA    Operador encerrou ciclo de registro de mesários 10D9F5C437E14B15
06/10/2024 17:02:40     INFO    02190993        VOTA    Inicio do Encerramento  65C84AA1412439A2
06/10/2024 17:02:42     INFO    02190993        VOTA    Gerando relatório [BU] [INÍCIO] 8BBC7E9E491E8DE1
06/10/2024 17:02:42     INFO    02190993        VOTA    Gerando relatório [BU] [TÉRMINO]        284DAA380F3EDB91

TRECHO DO ARQUIVO DE LOG DE URNA COM BIOMETRIA
TÍTULO DO MESÁRIO SUBSTITUÍDO POR XXXXXXXXXXX
```

Fonte: TRE-SC (2025).

Registro digital do voto (RDV)

O **Registro Digital do Voto** é uma espécie de tabela digital, criada pela Lei n. 10.740/2003, em substituição ao voto impresso. Lá, são armazenados todos os votos à medida em que são digitados no teclado da urna.

Como visto anteriormente, os votos serão gravados no arquivo RDV em ordenação lexicográfica dentro de cada cargo (ordenação pelo número do candidato).

Dessa forma, o RDV garante o sigilo e – assim como numa urna de lona tradicional, onde as cédulas de papel ficam embaralhadas – impossibilita a vinculação de cada cédula à pessoa que votou.

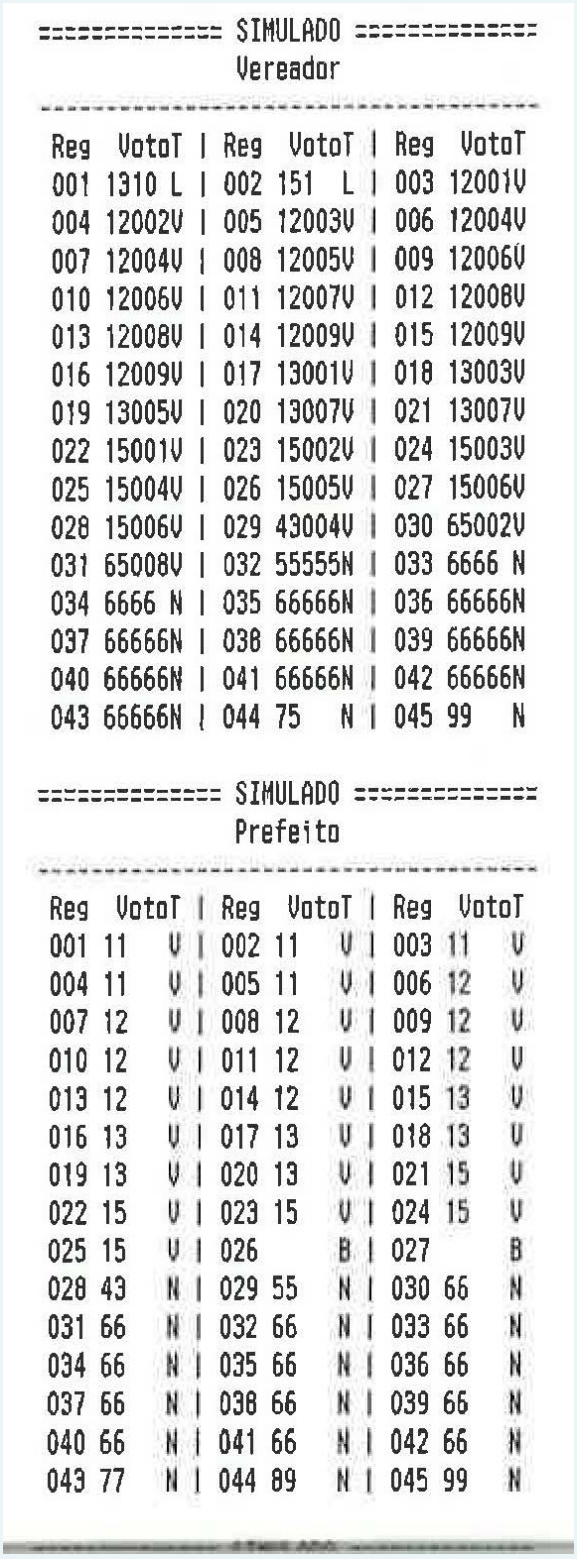
Até 2020, os arquivos de ***log*** e de **RDV** eram disponibilizados aos partidos políticos e às coligações partidárias para análise dos eventos ocorridos na urna eletrônica.

A partir de 2022, esses arquivos passaram a ser **disponibilizados na internet**.

Quer saber mais sobre o RDV? Recomenda-se a leitura da notícia no *site* do TSE: Registro Digital do Voto permite recontagem e amplia transparência do processo eleitoral.

Veja exemplo de relatório do RDV:

Figura 12 - Exemplo de relatório do RDV



```
============== SIMULADO ==============
                Vereador
---------------------------------------
 Reg  VotoT | Reg  VotoT | Reg  VotoT
 001 1310 L | 002 151  L | 003 12001V
 004 12002V | 005 12003V | 006 12004V
 007 12004V | 008 12005V | 009 12006V
 010 12006V | 011 12007V | 012 12008V
 013 12008V | 014 12009V | 015 12009V
 016 12009V | 017 13001V | 018 13003V
 019 13005V | 020 13007V | 021 13007V
 022 15001V | 023 15002V | 024 15003V
 025 15004V | 026 15005V | 027 15006V
 028 15006V | 029 43004V | 030 65002V
 031 65008V | 032 55555N | 033 6666 N
 034 6666 N | 035 66666N | 036 66666N
 037 66666N | 038 66666N | 039 66666N
 040 66666N | 041 66666N | 042 66666N
 043 66666N | 044 75   N | 045 99   N

============== SIMULADO ==============
                Prefeito
---------------------------------------
 Reg  VotoT | Reg  VotoT | Reg  VotoT
 001 11   V | 002 11   V | 003 11   V
 004 11   V | 005 11   V | 006 12   V
 007 12   V | 008 12   V | 009 12   V
 010 12   V | 011 12   V | 012 12   V
 013 12   V | 014 12   V | 015 13   V
 016 13   V | 017 13   V | 018 13   V
 019 13   V | 020 13   V | 021 15   V
 022 15   V | 023 15   V | 024 15   V
 025 15   V | 026      B | 027      B
 028 43   N | 029 55   N | 030 66   N
 031 66   N | 032 66   N | 033 66   N
 034 66   N | 035 66   N | 036 66   N
 037 66   N | 038 66   N | 039 66   N
 040 66   N | 041 66   N | 042 66   N
 043 77   N | 044 89   N | 045 99   N
```

Fonte: TRE-SC (2025).

Dispositivo de segurança em *hardware*

Você sabe como funciona a inicialização de um computador comum? O primeiro componente a entrar em operação é a BIOS, que faz verificações gerais (de vídeo, dispositivos, etc) e depois aciona outros programas, como o *Loader*, responsável pelo carregamento do sistema operacional. O problema é que um vírus pode se instalar na BIOS ou em qualquer um desses programas.

Para evitar isso, a urna eletrônica possui um **dispositivo físico, chamado *hardware* de segurança**, que é acionado antes da BIOS e que inicia a verificação de segurança dos módulos e sistemas que serão carregados na memória da urna, incluindo os programas de inicialização (BIOS, *bootloader* e *kernel*). Veja como funciona:

1. Ao ligar a urna, o *hardware* de segurança é o primeiro componente a funcionar.

2. Em seguida, ele verifica a BIOS: se está íntegra, se foi assinada pelo TSE e se não foi adulterada. Se tudo estiver correto, o *hardware* de segurança passa o comando para a BIOS.

3. A BIOS passa a verificar o *Loader*: se está íntegro e assinado pelo TSE; e só depois de confirmada a regularidade é que o *Loader* é acionado.

4. O *Loader* é responsável por acionar o sistema operacional (UENUX). Mas, antes de fazê-lo, verifica se está íntegro e assinado pelo TSE. Depois de verificado, o sistema operacional é carregado.

5. Continuam a ser feitas essas conferências sucessivamente com os demais programas. É o que se denomina **cadeia de segurança em *hardware***.

Você percebeu a diferença para um sistema computacional comum? Os sistemas da urna eletrônica apenas são acionados após serem verificados quanto à integridade e à assinatura do TSE, o que ocorre de forma encadeada.

Atenção!

É por conta dessa cadeia de segurança que a urna eletrônica executa **apenas** os *softwares* gerados durante a Cerimônia de Lacração e Assinatura Digital.

Eventual tentativa de executar *software* não autorizado bloqueia o funcionamento da urna. A situação oposta também não é possível: a execução do aplicativo é cancelada caso se tente executar o *software* oficial em *hardware* não certificado.

Barreiras físicas de segurança

Além de todos os mecanismos lógicos vistos até aqui, pode-se também enumerar algumas barreiras físicas que reforçam a segurança da urna eletrônica. Veja quais são:

- Uma **grossa camada de resina de epóxi** é aplicada nos dispositivos mais críticos da urna, de forma a evidenciar tentativas de acesso físico.

- **Lacres físicos** são colocados nas urnas eletrônicas para resguardar o acesso ao seu interior. Esses lacres são assinados pelo juiz da Zona Eleitoral e por demais autoridades, e colados nas urnas eletrônicas logo após sua configuração, durante a Cerimônia de Preparação das Urnas Eletrônicas. Cada urna recebe os lacres de uma cartela específica, com numeração própria, tornando possível a conferência. Além disso, qualquer tentativa de romper o lacre é facilmente detectada.

- A **disposição da urna** no momento da votação auxilia na fiscalização. Ou seja: a parte traseira da urna, onde ficam as portas das conexões, está voltada para quem fica na seção eleitoral (mesários, fiscais de partido, etc) e não para o eleitor. Para os eleitores, ficam acessíveis apenas o teclado e a tela da urna.

Como a urna se defende de ataques cibernéticos?[6]

A urna utiliza o que há de mais moderno em assinatura digital e criptografia para proteger o seu *software*, assim como os dados de eleitores, candidaturas e votos nela registrados.

No entanto, nos últimos anos, houve uma crescente exigência social para que o sistema eleitoral brasileiro seja compreendido pela população. Além de demandas justificáveis, infelizmente também surgiram questionamentos que são fruto de desinformação espalhada na internet. Por isso, é importante conhecer as perguntas mais comuns e como a Justiça Eleitoral previne problemas de segurança nas eleições.

A urna está conectada na internet?

Embora seja eletrônica, a urna funciona de forma isolada, ou seja, não possui nenhum mecanismo que possibilite sua conexão a redes de computadores, como a internet.

A urna não possui o *hardware* necessário para se conectar a uma rede e tampouco a qualquer forma de conexão com ou sem fio. O sistema operacional contido na urna é preparado pela Justiça Eleitoral de forma a não incluir nenhuma ferramenta que permita a conexão com redes ou o acesso remoto.

O único cabo que ela possui é o de energia e, se for necessário, ela poderá ficar ligada somente na bateria por mais de dez horas, por exemplo, caso falte energia da rede elétrica.

[6] Fonte: Seção de Voto Informatizado/Coordenadoria de Tecnologia Eleitoral/Secretaria de Tecnologia da Informação do Tribunal Superior Eleitoral (SEVIN/COTEL/STI/TSE).

E se alguém tentar alterar um *software* da urna?

Tudo começa na Cerimônia de Lacração, realizada no TSE, quando o *software* da urna recebe assinaturas digitais que o protegem de qualquer tipo de modificação. Todas as urnas possuem um dispositivo chamado "*hardware* de segurança" que valida as assinaturas do *software* que foram geradas na lacração. Isso garante que somente o *software* produzido pelo TSE e assinado na cerimônia possa ser utilizado pelas urnas.

Quando o *hardware* de segurança valida corretamente o *software* oficial que será usado na eleição, a luz de segurança do terminal do mesário fica com a cor verde. Quando o *software* não é autêntico, essa luz fica piscando e nenhum comando é executado. A urna não funciona se houver modificação do programa original.

E se alguém tentar alterar dados de candidatos ou de quem votou?

Todos os dados de eleitoras, eleitores, candidatas, candidatos e de configuração da eleição são assinados digitalmente. Com isso, um atacante não consegue fazer qualquer tipo de modificação nesses dados, seja nos computadores da Justiça Eleitoral, seja nas mídias ou seja diretamente na urna. Dados mais sensíveis, como os de biometria, são protegidos por criptografia e só podem ser abertos de forma segura na urna.

Existe alguma forma de quebrar o sigilo do voto?

Os votos na urna são gravados de forma embaralhada, criptografados e sem qualquer associação com os eleitores. Com isso, não é possível acessar os dados da urna para saber como cada pessoa votou.

Como são protegidos o boletim de urna e os resultados?

Os boletins de urna, assim como outros resultados produzidos pela urna, também são protegidos por assinatura digital. O *hardware* de segurança assina todos os arquivos gravados na memória de resultado, o que impede a modificação dos dados e permite ter a certeza sobre qual urna produziu os respectivos arquivos.

Para quem quiser se aprofundar no assunto, sugere-se a apresentação Segurança e Auditoria nas Eleições Brasileiras (TSE).

7.4. Transparência nos procedimentos

Entidades fiscalizadoras e momentos da fiscalização

Até agora, foram abordadas as tecnologias de proteção dos dados que ajudam a compreender os programas e aplicativos desenvolvidos pelo TSE para garantir a segurança da urna e de seus sistemas.

A partir deste momento, será verificado o aspecto da **transparência**. É para garanti-la que o processo eleitoral é **auditável** em todos os seus momentos: desde o desenvolvimento dos sistemas até o funcionamento da urna eletrônica em suas diversas etapas (preparatórias, no próprio dia da votação, e após a eleição).

Conforme o art. 5º da Resolução TSE n. 23.673/2021, a fiscalização dos sistemas eleitorais ocorrerá nos seguintes momentos:

- Durante o desenvolvimento, a compilação, a assinatura digital e a lacração dos sistemas eleitorais.
- Cerimônias de geração de mídias e preparação das urnas eletrônicas.
- Cerimônia de verificação da integridade e autenticidade dos sistemas eleitorais instalados no TSE.
- Audiência de verificação dos sistemas de transmissão de boletins de urna.
- Durante os procedimentos preparatórios para realização dos testes de integridade e de autenticidade no dia da votação.
- Durante o Teste de Integridade das Urnas Eletrônicas (antiga auditoria de funcionamento das urnas eletrônicas em condições normais de uso ou, simplesmente, "votação paralela").
- Durante o Teste de Autenticidade dos Sistemas Eleitorais, no dia da votação (antiga auditoria de funcionamento das urnas eletrônicas por meio da verificação dos sistemas).
- Após os procedimentos de totalização das eleições.

Então, inicialmente, ocorre a fiscalização no desenvolvimentos dos sistemas utilizados nas urnas e computadores da Justiça Eleitoral.

Além das auditorias serem feitas pela Justiça Eleitoral, as entidades fiscalizadoras também podem realizá-las. De acordo com o art. 6º da Resolução TSE n. 23.673/2021, são **entidades fiscalizadoras legitimadas** a participar do processo de fiscalização:

- Partidos políticos, federações e coligações;
- Ordem dos Advogados do Brasil;
- Ministério Público;
- Congresso Nacional;
- Controladoria-Geral da União;
- Polícia Federal;
- Sociedade Brasileira de Computação;
- Conselho Federal de Engenharia e Agronomia;
- Conselho Nacional de Justiça;
- Conselho Nacional do Ministério Público;
- Tribunal de Contas da União;
- Confederação Nacional da Indústria, demais integrantes do Sistema Indústria e entidades corporativas pertencentes ao Sistema S;
- Entidades privadas brasileiras, sem fins lucrativos, com notória atuação em fiscalização e transparência da gestão pública, credenciadas junto ao TSE; e
- Departamentos de tecnologia da informação de universidades credenciadas junto ao TSE.

Com o intuito de tornar mais transparente o processo eletrônico de votação, o TSE vem ampliando o rol de entidades fiscalizadoras a cada ano.

Para cientificar essas entidades sobre as datas das cerimônias e dos eventos, oportunizando a fiscalização, são publicados os **editais de convocação**, com a antecedência prevista na legislação.

Atenção!

Todos os procedimentos de verificação e auditoria devem ocorrer à vista de autoridades e fiscais presentes, sempre operados por técnicos da Justiça Eleitoral, conforme designação do TRE ou do juízo eleitoral.

Como visto, há muita gente envolvida na garantia de segurança do sistema de votação brasileiro em todas as suas etapas, cujos detalhes serão apresentados na sequência.

Aplicativos utilizados na fiscalização para verificação da integridade dos sistemas, tanto na urna eletrônica quanto nos computadores da Justiça Eleitoral

Para isso, poderá ser usado programa de verificação, **fornecido pelo TSE ou desenvolvido por entidade fiscalizadora**.

Conforme o art. 37, § 3º, da Resolução TSE n. 23.673/2021:

> Art. 37. Durante a Cerimônia de Preparação de Urnas, prevista na Resolução de Atos Gerais do Processo Eleitoral, as entidades fiscalizadoras poderão verificar a integridade e autenticidade dos sistemas eleitorais instalados em urnas eletrônicas.
>
> [...]
>
> § 3º A verificação da integridade e autenticidade dos programas da urna eletrônica será realizada nos locais de preparação das urnas mediante:
>
> I – utilização do programa de verificação de autenticidade dos programas da urna (AVPART), desenvolvido pelo Tribunal Superior Eleitoral;
>
> II – utilização do programa de Verificação Pré/Pós-Eleição (VPP) da urna eletrônica, desenvolvido pelo TSE; e
>
> III – utilização de programas de verificação de integridade e autenticidade dos sistemas eleitorais, desenvolvidos pelas entidades fiscalizadoras.
>
> [...]

Como segurança nunca é demais, existem também os **aplicativos de verificação dos programas verificadores**. O TSE utiliza esses aplicativos para verificar a autenticidade e as assinaturas dos próprios sistemas eleitorais e dos programas de verificação desenvolvidos pelas entidades fiscalizadoras.

Programas das entidades fiscalizadoras

De acordo com o art. 15 da Resolução TSE n. 23.673/2021:

> Art. 15. As entidades fiscalizadoras poderão desenvolver programas próprios de verificação, devendo, até 90 (noventa) dias antes da realização do primeiro turno das eleições, apresentar, para homologação, o seguinte material:
>
> I – códigos-fonte dos programas de verificação, que deverão estar em conformidade com a especificação técnica disponível na STI/TSE; e
>
> II – chave pública correspondente àquela que será utilizada pelos representantes na Cerimônia de Assinatura Digital e Lacração dos Sistemas.
>
> Parágrafo único. O Tribunal Superior Eleitoral, por sua Secretaria de Tecnologia da Informação, requisitará à entidade fiscalizadora as licenças de uso das ferramentas de desenvolvimento empregadas na construção do programa, se não as possuir, para uso e guarda até a realização das eleições. (Redação dada pela Resolução TSE n. 23.728/2024)

Os programas precisam ser apresentados dentro do prazo e estar em conformidade com as especificações técnicas para que sejam analisados e homologados pela Secretaria de Tecnologia da Informação do TSE (STI/TSE). Detectada qualquer falha de segurança ou problema no funcionamento dos programas de verificação, a STI/TSE informará a entidade fiscalizadora para que providencie o ajuste, submetendo-os a novos testes.

Cumpridos os requisitos necessários, os programas serão compilados, assinados digitalmente e lacrados na Cerimônia de Assinatura Digital e de Lacração dos Sistemas, juntamente com os sistemas eleitorais, para que sua autenticidade também possa ser conferida.

Atenção!

Não é permitida a gravação, na urna ou nos computadores da Justiça Eleitoral, de nenhum tipo de dado ou função pelos programas de verificação apresentados pelas entidades fiscalizadoras.

Mas a impressora da urna poderá ser utilizada para emitir relatórios, desde que a capacidade de papel disponível não fique comprometida.

Programas desenvolvidos pelo TSE

AVPART – Programa de Verificação de Autenticidade dos Programas da Urna

O AVPART permitirá:

- emissão do *hash* dos programas instalados nas urnas; e
- validação das assinaturas digitais dos arquivos da urna eletrônica. O procedimento de verificação com o AVPART é realizado:
  - na **cerimônia de preparação das urnas**; e
  - na **urna da seção eleitoral, no dia da votação, antes da emissão da zerésima** (caso a urna tenha sido sorteada na véspera da eleição).

VPP – Verificador Pré e Pós-Eleição

A Justiça Eleitoral disponibiliza o VPP para:

- conferência visual dos dados de pessoas candidatas e partidos;
- emissão do *hash* dos programas instalados durante a carga das urnas eletrônicas; e
- demonstração do processo de votação, a fim de aferir o correto funcionamento do equipamento.

Além da impressão dos *hashes* para conferência, o VPP disponibiliza outras opções, que variam de acordo com o momento em que o aplicativo estiver sendo executado e conforme o tipo de urna (seção ou contingência) onde está sendo executado.

O VPP pode ser executado em diferentes momentos:

- Antes do 1º turno – apenas **verificação pré-eleição**, em urna configurada para o 1º turno, antes da emissão da zerésima, como ocorre durante a cerimônia de preparação das urnas.
- Entre os dois turnos – **verificação pós-eleição do 1º turno e pré-eleição do 2º turno**, em urna já preparada para o 2º turno, antes da emissão da zerésima.
- Após o 2º turno – apenas **verificação pós-eleição do 1º ou 2º turno**.

VAP e VAD – Programas verificadores de autenticidade e das assinaturas digitais

Para verificação da autenticidade e da assinatura digital dos sistemas eleitorais, bem como dos programas de verificação desenvolvidos por entidades ou partidos, o TSE disponibiliza os aplicativos:

VAP – Verificador de Autenticidade dos Programas

Verifica a integridade dos sistemas instalados em microcomputadores, realizando o cálculo do *hash* dos arquivos dos sistemas eleitorais neles instalados. Saiba os sistemas que podem ser verificados pelo VAP:

- Subsistema de Instalação e Segurança (SIS);
- Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica – GEDAI-UE;
- *HotSwapFlash* (HSF);
- Transportador;
- JE-Connect.

VAD – Verificador da Assinatura Digital

Verifica a autenticidade das assinaturas digitais dos sistemas eleitorais no computador ou de programas desenvolvidos por entidades externas à Justiça Eleitoral.

> Esses aplicativos deverão ser instalados em computadores da Justiça Eleitoral com a última versão do Subsistema de Instalação e Segurança (SIS) e com a lista de certificados públicos mais recentes da Justiça Eleitoral.

Auditorias dos sistemas eleitorais e da urna eletrônica.

As auditorias podem ser realizadas para verificar a integridade dos sistemas e da urna eletrônica. É importante conhecê-las mais detalhadamente, separando-as pelo período em que acontecem durante o processo eleitoral: se antes das eleições, se durante a votação, ou após a eleição.

Antes das eleições:

Na cerimônia de geração de mídias

As mídias da eleição, que serão utilizadas na carga das urnas oficiais, são geradas em cerimônia pública, na qual os seguintes sistemas podem ser verificados:

- Subsistema de Instalação e Segurança (SIS);
- Sistema Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica – GEDAI-UE;
- *HotSwapFlash* (HSF).

Para isso, poderão ser utilizados os aplicativos do TSE (**VAP** e **VAD**) ou algum outro programa desenvolvido por entidade fiscalizadora.

Na cerimônia de preparação das urnas

Durante esta cerimônia, é **obrigatório**:

I - VPP

Realizar a demonstração de votação acionada pelo aplicativo Verificador Pré/Pós-Eleição (VPP) em pelo menos uma urna por Município da zona eleitoral.

II - AVPART

Verificar os sistemas instalados na urna pelo programa Verificador de Integridade e Autenticidade dos Sistemas Eleitorais (AVPART) em pelo menos uma urna de cada mídia de carga utilizada.

A verificação por amostragem será realizada em até 6% das urnas preparadas para cada zona eleitoral, escolhidas pelos representantes das entidades fiscalizadoras, de forma aleatória, entre as urnas de votação e as de contingência.

Poderão ser verificados todos os sistemas instalados nas urnas. Para tanto, devem ser utilizados os programas do TSE (**VPP** e **AVPART**), bem como podem ser utilizados os desenvolvidos pelas próprias entidades fiscalizadoras.

Verificação dos sistemas Transportador e JE-Connect

Na **antevéspera da eleição**, acontece mais uma possibilidade de fiscalização: em audiência, são checadas a integridade e a autenticidade dos sistemas destinados à transmissão dos Boletins de Urna – o Sistema Transportador e o JE-Connect –, que estão instalados nos microcomputadores.

Sistema Transportador: é o responsável pela leitura das mídias de resultado, que contêm os arquivos de urna, e pela transmissão desses arquivos lidos para o banco de dados da Justiça Eleitoral.

JE-Connect: é o aplicativo que recebe e transmite arquivos de BU de forma segura – a partir do próprio local de votação, por exemplo –, utilizando redes de comunicação ou mesmo computadores de parceiros da Justiça Eleitoral.

Verificação dos sistemas de totalização instalados no TSE

Na **véspera da eleição**, as entidades legitimadas poderão fiscalizar, no TSE, os sistemas relacionados à transmissão dos Boletins de Urna e sua totalização. São eles:

- Gerenciamento da Totalização;
- Receptor de Arquivos da Urna (REC-BU);
- InfoArquivos; e
- Transportador *WEB*.

> As verificações desses sistemas são **realizadas exclusivamente no TSE** por serem aplicações *web*, ou seja, que "rodam" (ou "são executadas") num computador servidor que, no caso, está localizado nas dependências desse Tribunal.

Estes são, resumidamente, os momentos de verificação que acontecem antes da votação, em ambientes da Justiça Eleitoral abertos às entidades fiscalizadoras.

Auditorias de funcionamento das urnas durante a votação

Os TREs realizam no dia da votação dois tipos de auditoria, ambas feitas por amostragem:

- **Teste de Integridade das Urnas Eletrônicas**, que verifica o funcionamento das urnas sob condições normais de uso (a obrigatoriedade desse teste consta na Lei n. 9.504/1997, art. 66, § 6º, com a denominação de "votação paralela"); e
- **Teste de Autenticidade dos Sistemas Eleitorais**, que, como o próprio nome diz, verifica a autenticidade dos sistemas eleitorais instalados nas urnas eletrônicas.

Essas auditorias acontecem por determinação legal e independem da solicitação de qualquer entidade.

O sorteio das seções eleitorais que participarão das duas auditorias ocorre sempre na **véspera da eleição** (sábado), em um mesmo evento. A Comissão de Auditoria da Votação Eletrônica, constituída pelo TRE, é responsável pelo sorteio e por organizar os trabalhos das auditorias.

No caso de ausência de entidades fiscalizadoras ou de a quantidade de seções escolhidas ser inferior ao número estabelecido nos artigos 58 e 59 da Resolução TSE n. 23.673/2021, será promovido um sorteio de forma a complementar o quantitativo.

No TRE-SC, a cerimônia é transmitida ao vivo para os Cartórios Eleitorais pela *intranet* e ao público externo pelo seu canal no *YouTube*.

Teste de Integridade das Urnas Eletrônicas

Este teste é um simulado da votação real, executado pelo TRE em ambiente controlado e filmado, para verificar o efetivo funcionamento da urna no dia da eleição. Ele tem como objetivo demonstrar que o voto em determinada(o) candidata ou candidato será devidamente computado a quem se destina, e não para outra pessoa.

Para isso, algumas urnas do interior e da Capital são selecionadas aleatoriamente por meio de sorteio público ou, opcionalmente, escolhidas pelas entidades fiscalizadoras presentes. O procedimento detalhado observa as etapas a seguir.

Figura 13 - Sorteio das urnas eletrônicas para auditoria

Fonte: TRE-SC (2008).

Na **véspera** da eleição, todas as urnas já estão configuradas e organizadas para distribuição aos locais de votação. Na manhã desse dia, é escolhido (pelas entidades fiscalizadoras presentes) e/ou sorteado (pela Comissão de Auditoria da Votação Eletrônica) um conjunto de urnas conforme as quantidades estabelecidas pelo TSE para aquela eleição, dependendo do total de seções eleitorais de cada Estado. Essas urnas são recolhidas e transportadas para o local onde será feita a auditoria. Na foto acima, você vê um sorteio sendo realizado.

Também na **véspera**, para cada seção escolhida ou sorteada, são preenchidas cédulas em papel, contendo votos para os diversos candidatos. A intenção é simular várias possibilidades de votação. Essas cédulas são, então, guardadas em urnas de lona lacradas.

No **dia da eleição**, a Comissão de Auditoria retira as cédulas de cada urna de lona. Uma a uma, mostra a cédula e seu conteúdo ao público, e depois efetua o registro desse voto na urna eletrônica que foi selecionada na véspera. O voto também é registrado em um sistema de controle. Concluída a votação, os votos totalizados no boletim de urna serão conferidos com aqueles registrados no sistema de controle, para comprovar que a urna contabiliza corretamente os votos (foto abaixo).

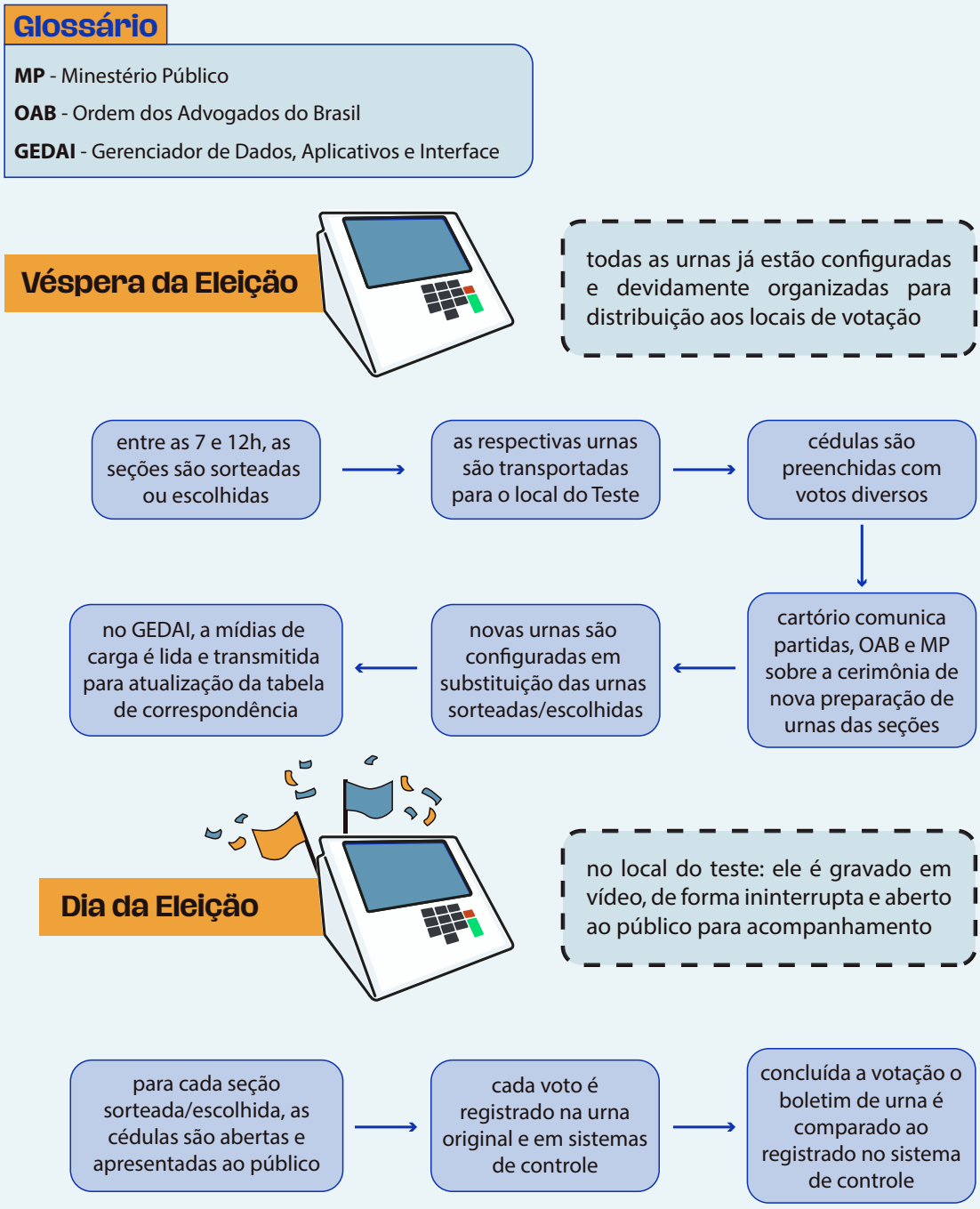
Figura 14 - Verificação da contabilidade correta dos votos nas urnas eletrônicas

Fonte: TRE-SC (2008).

A Justiça Eleitoral realiza Teste de Integridade com Biometria desde as eleições de 2024, em locais de votação designados.

O Teste de Integridade com Biometria é realizado mediante o emprego de biometria de eleitores voluntários em local próximo ao da votação.

Figura 15 - Fluxo de procedimentos do Teste de Integridade das Urnas Eletrônicas



Fonte: Adaptado de TRE-SC (2025).

Agora que você já conhece melhor a auditoria do funcionamento das urnas nas condições normais de uso, veja a outra auditoria realizada no dia da votação.

Teste de Autenticidade dos Sistemas Eleitorais

Esta auditoria é realizada na própria seção eleitoral, no dia da eleição, às 7 horas, antes da emissão da zerésima.

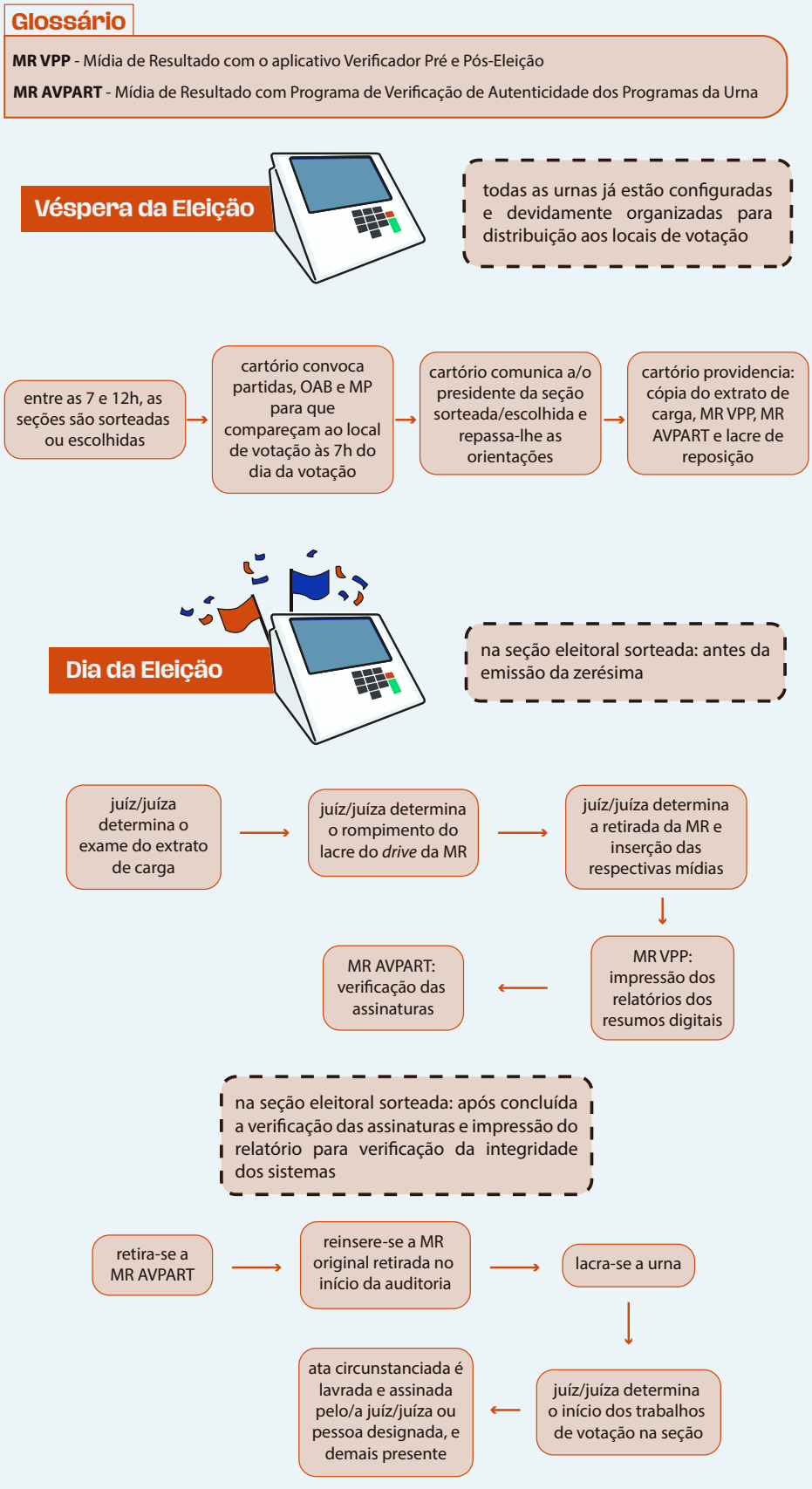
Como visto, a escolha e/ou o sorteio das urnas para esta auditoria é feito em conjunto com a escolha e/ou o sorteio das urnas destinadas à auditoria anteriormente comentada ("votação paralela").

Cabe à Comissão Eleitoral informar à autoridade eleitoral sobre a urna sorteada. A juíza ou o juiz convoca então os partidos políticos, assim como os representantes da OAB e do MP, para que compareçam ao local de votação pelo menos **uma hora antes do início da votação**.

Quem for presidente da seção eleitoral também receberá a informação sobre a auditoria que será realizada na urna.

Na seção eleitoral, será feita a verificação das assinaturas e dos resumos digitais pelos programas do TSE (AVPART e VPP), bem como por programa de verificação de entidade fiscalizadora, se apresentado. Desta forma, comprova-se a autenticidade dos programas da urna.

Figura 16 - Fluxo de procedimentos do Teste de Autenticidade dos Sistemas Eleitorais



Fonte: Adaptado de TRE-SC (2025).

Auditorias após a eleição

Durante todo o processo eleitoral, as entidades fiscalizadoras são convidadas a participar de cerimônias públicas e de eventos destinados à verificação dos sistemas de votação e da sua integridade. A Justiça Eleitoral dá, em muitas ocasiões, acesso para que as verificações sejam feitas.

No entanto, mesmo depois de todas essas oportunidades e já terminada a eleição, pode ser que as entidades fiscalizadoras ainda solicitem alguma verificação nos sistemas. Essa **verificação extraordinária dos sistemas eleitorais** após o pleito é possível, desde que sejam relatados fatos e apresentados indícios e circunstâncias que a justifiquem.

O prazo final para o pedido de verificação posterior à eleição se encerra 5 dias antes da data-limite para manutenção dos lacres das urnas e de liberação para desinstalação dos sistemas.

Podem ser verificados os sistemas instalados nas urnas eletrônicas, nos microcomputadores da Justiça Eleitoral e no equipamento servidor do TSE, aplicando-se, no que couber, as regras das auditorias realizadas antes das eleições.

Resumindo

Para retomar o que foi visto até agora e organizar as informações, veja abaixo uma tabela relativa às auditorias realizadas antes e depois da eleição, com o momento em que ocorre a fiscalização, onde é realizada, quais os sistemas verificados e os aplicativos utilizados, conforme a Resolução TSE n. 23.673/2021:

Figura 17 - Tabela relativa às auditorias realizadas antes e depois da eleição

Glossário

VAP - Aplicativo Verificador de Autenticidade dos Programas
VAD - Aplicativo Verificador da Assinatura Digital
SIS - Subsistema de Instalação e Segurança
HotSwapFlash (HSF) - Serviço utilizado pelo Sistema Gerenciador de Dados
JE-Connect - Ferramenta que viabiliza a transmissão do Boletim de Urna diretamente de alguns locais de votação

Fase / momento	Local	Sistemas que podem ser verificados	Aplicativos para verificação
Antes da eleição Cerimônia de Geração de Mídias (art. 36)	Cartório Eleitoral	Instalados em equipamentos da Justiça Eleitoral: ▶ SIS ▶ GEDAI ▶ *HotSwapFlash* (HSF)	▶ VAP ▶ VAD ▶ Verificador de partido/entidade
Antes da eleição Cerimônia de Preparação das Urnas (art. 37)	Local de preparação das urnas	▶ Urnas	▶ VPP ▶ AVPART ▶ Verificador de partido/entidade
Antevéspera do dia das eleições (art. 43)	Cartório Eleitoral	▶ Transportador ▶ JE-Connect	▶ VAP ▶ VAD ▶ Verificador de partido/entidade
Véspera do dia das eleições (art. 41)	TSE	▶ Gerenciamento da Totalização ▶ Receptor de arquivos de urna (REC-BU) ▶ InfoArquivos ▶ Transportado *WEB*	▶ VAP ▶ VAD ▶ Verificador de partido/entidade
Após as eleições (art. 52, I c/c arts. 36 e 43) (art. 52, II c/c art. 37)	Cartório Eleitoral	▶ SIS ▶ GEDAI ▶ *HotSwapFlash* (HSF) ▶ Urnas ▶ Transportador ▶ JE-Connect	▶ VAP ▶ VAD ▶ VPP ▶ AVPART ▶ Verificador de partido/entidade
Após as eleições (art. 52, III c/c art. 41)	TSE	▶ Gerenciamento da Totalização ▶ Receptor de arquivos de urna (REC-BU) ▶ InfoArquivos ▶ Transportador *WEB*	▶ VAP ▶ VAD ▶ Verificador de partido/entidade

Fonte: Adaptado de TSE (2025).

Disponibilização de dados pela Justiça Eleitoral

Até aqui, viu-se como se dá a fiscalização dos sistemas eleitorais nas urnas eletrônicas e também nos computadores utilizados pela Justiça Eleitoral durante todo o processo eleitoral.

Percebe-se que são diversas as oportunidades para que entidades e instituições verifiquem a autenticidade e integridade do funcionamento do sistema de votação brasileiro.

Ainda assim, prezando pela absoluta transparência, a Justiça Eleitoral pode também entregar dados, arquivos e relatórios para que os partidos façam sua análise. Durante a preparação das eleições e após, é normal que os partidos políticos solicitem dados dos sistemas eleitorais para que possam exercer a sua fiscalização.

Essas solicitações podem ocorrer em momentos diversos:

Arquivos referentes a eventos antes da eleição

As entidades fiscalizadoras têm até 100 dias corridos, contados a partir do dia do 1º turno das eleições, para solicitar:

- os arquivos de *log* do Gerenciador de Dados, Aplicativos e Interface com a Urna Eletrônica (GEDAI-UE); e
- os arquivos de dados alimentadores do Sistema de Gerenciamento da Totalização, referentes a pessoas candidatas, partidos políticos, coligações, federações, municípios, zonas e seções.

Arquivos referentes à votação e à totalização

No mesmo prazo (100 dias corridos, contados a partir do dia do 1º turno das eleições), as entidades também podem solicitar os seguintes relatórios e cópias dos arquivos de sistemas:

- arquivos de *log* do Transportador, do Receptor de Arquivos de Urna e do banco de dados da totalização;
- arquivos de imagens dos boletins de urna;
- arquivos de Registro Digital do Voto (RDV);
- arquivos de *log* das urnas;
- relatório de boletins de urna que estiveram em pendência, sua motivação e respectiva decisão;
- relatório Resultado da Totalização, emitido pelo Sistema de Gerenciamento da Totalização (SISTOT), incluindo a relação das seções em que o boletim de urna tenha sido gerado em urna substituta;
- arquivos de dados de votação por seção; e
- relatório com dados sobre o comparecimento e a abstenção em cada seção eleitoral.

Como visto, garantir a transparência do sistema de votação é uma prioridade da Justiça Eleitoral. Seja por meio de eventos em momentos cruciais do processo, seja na entrega de dados às entidades fiscalizadoras, a cada eleição um grande trabalho é realizado a fim de que as informações cheguem a toda sociedade brasileira.

Saiba mais: Oportunidades de auditoria e fiscalização do processo eletrônico de votação.

7.5. Checagem pela sociedade

Tabela de correspondência

Assim como os computadores são identificados por um número de IP, cada urna é identificada por um número interno. A **correspondência** é a associação entre esse número de identificação da urna com:

- a seção para a qual foi preparada; ou
- sua atribuição como urna de contingência.

O número da **correspondência** é formado por 24 algarismos, gerado a partir das seguintes informações:

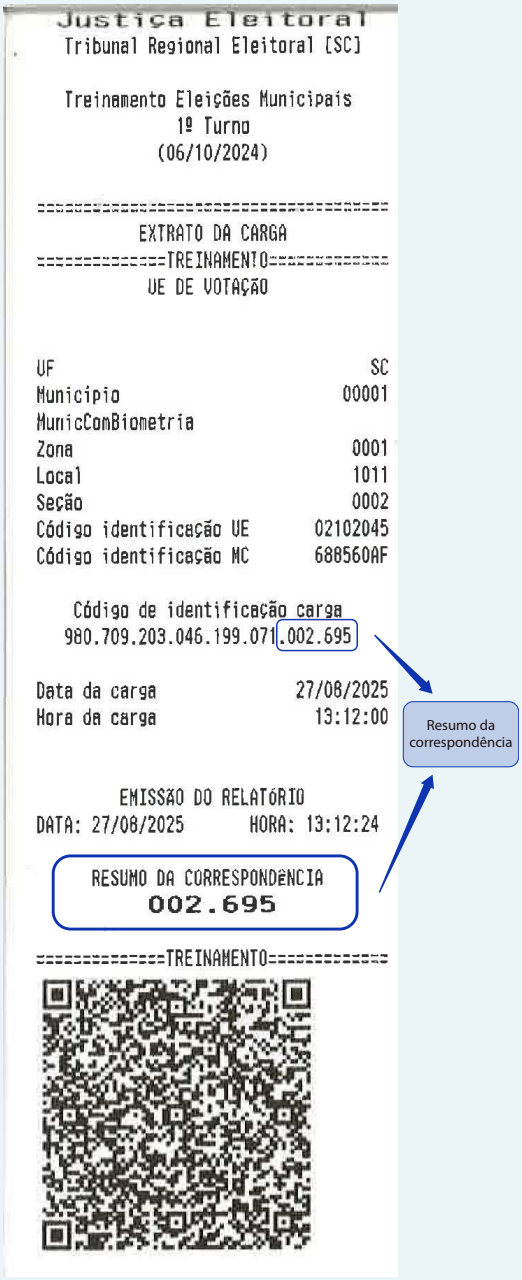
- Município;
- Zona eleitoral;
- Seção eleitoral;
- Código de identificação da urna;
- Código de identificação da mídia de carga;
- Data/hora da carga.

> Os seis últimos caracteres do código são chamados de **Resumo da Correspondência**.
>
> Esse resumo é utilizado para facilitar as conferências que devem ser realizadas.

Quando o código de correspondência é gerado? **No momento da preparação de cada urna**, ficando gravado na mídia de carga, bem como impresso no extrato e comprovante de carga.

A imagem a seguir exemplifica um extrato de carga, onde pode ser observado o código – nominado como "código de identificação da carga" – e o resumo da correspondência.

Figura 18 - Exemplo de um extrato de carga



Fonte: TRE-SC (2025).

Concluída a preparação das urnas, o cartório eleitoral efetua a leitura da mídia de carga no sistema GEDAI para recebimento e transmissão das correspondências de todas as urnas configuradas, permitindo que elas fiquem disponíveis para outros sistemas eleitorais, dentre eles, o SISTOT, responsável pela totalização dos resultados da eleição.

O conjunto de códigos de correspondência transmitidos forma a **tabela de correspondência**:

Figura 19 - Tabela de correspondência mostrada no SISTOT

Tipo correspondência	Cód. Município	Município	Zona Eleitoral	Local de Votação	Seção	Id Urna	Id Carga	Id MC	Data/Hora Carga	Data/Hora receb. GEDAI	Data/Hora receb. SISTOT	Situação
Esperada	82139	MODELO	0083	1015 - ESCOLA DE EDUCAÇÃO BÁSICA DOM HELDER CÂMARA	0073	2190993	426.931.245.558.895.489.436.549	6E1B3DDF	28/09/2024 08:39:00	28/09/2024 15:27:48	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1015 - ESCOLA DE EDUCAÇÃO BÁSICA DOM HELDER CÂMARA	0074	2005747	800.769.739.996.941.254.247.079	6E1B3DDF	28/09/2024 08:43:00	28/09/2024 15:27:48	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1015 - ESCOLA DE EDUCAÇÃO BÁSICA DOM HELDER CÂMARA	0075	2049959	426.931.468.458.848.068.934.465	6E1B3DDF	28/09/2024 08:47:00	28/09/2024 15:27:48	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1015 - ESCOLA DE EDUCAÇÃO BÁSICA DOM HELDER CÂMARA	0076	2047287	437.032.583.359.527.295.628.288	6E1B3DDF	28/09/2024 08:51:00	28/09/2024 15:27:49	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1015 - ESCOLA DE EDUCAÇÃO BÁSICA DOM HELDER CÂMARA	0077	2190972	467.335.722.862.767.525.125.723	6E1B3DDF	28/09/2024 08:54:00	28/09/2024 15:27:49	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1120 - ESCOLA MUNICIPAL PROFESSORA GRISELDI MARIA MULLER	0078	2019167	699.658.061.585.279.277.115.347	6E1B3DDF	28/09/2024 08:58:00	28/09/2024 15:27:49	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1040 - GINÁSIO DE ESPORTES DA LINHA JANGUTA	0079	2190917	588.547.061.974.407.654.758.350	6E1B3DDF	28/09/2024 09:02:00	28/09/2024 15:27:49	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1120 - ESCOLA MUNICIPAL PROFESSORA GRISELDI MARIA MULLER	0080	2196035	325.921.888.848.424.060.078.949	6E1B3DDF	28/09/2024 09:06:00	28/09/2024 15:27:49	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1120 - ESCOLA MUNICIPAL PROFESSORA GRISELDI MARIA MULLER	0082	2005447	901.779.688.806.747.517.936.113	6E1B3DDF	28/09/2024 09:11:00	28/09/2024 15:27:49	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1120 - ESCOLA MUNICIPAL PROFESSORA GRISELDI MARIA MULLER	0083	2020705	386.527.277.254.576.105.786.961	6E1B3DDF	28/09/2024 09:16:00	28/09/2024 15:27:50	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1120 - ESCOLA MUNICIPAL PROFESSORA GRISELDI MARIA MULLER	0084	2022947	962.385.962.412.363.597.756.863	6E1B3DDF	28/09/2024 09:19:00	28/09/2024 15:27:50	28/09/2024 15:29:46	Recebida
Esperada	82139	MODELO	0083	1120 - ESCOLA MUNICIPAL PROFESSORA GRISELDI MARIA MULLER	0086	2044687	932.082.158.409.003.754.564.564	6E1B3DDF	28/09/2024 09:23:00	28/09/2024 15:27:50	28/09/2024 15:29:46	Recebida

Fonte: TRE-SC (2025).

Nela, ficam armazenadas as **correspondências esperadas**. Elas apenas serão consideradas **correspondências efetivadas** após a validação dos arquivos de resultado da votação pelo SISTOT.

Veja a explicação resumida desse processo: no dia da eleição, o Boletim de Urna (BU) transmitido para totalização informa ao SISTOT o código de correspondência da urna em que foi gerado. O sistema, então, procede da seguinte forma:

- primeiramente, testa se a correspondência contida no BU é a mesma esperada para a seção e, caso afirmativo, o BU pode ser totalizado;
- caso contrário, verifica se a correspondência do BU é de urna de contingência registrada na tabela de correspondências e, se assim for, o BU também pode ser totalizado;
- não sendo atendida nenhuma das condições acima, o BU não poderá ser totalizado e cairá em pendência.

Caso ocorra pendência, ela precisa ser analisada pelo juízo eleitoral, para descartar a possibilidade de fraude ou de algum erro operacional (por exemplo, a urna ser reconfigurada

devido a problemas técnicos, sem se realizar a respectiva atualização da tabela de correspondência).

Percebeu por que a tabela de correspondência é um importante instrumento de segurança do processo eletrônico de votação? É preciso haver comprovação da origem legítima dos dados e cada passo respeita uma cadeia de segurança da informação.

Além disso, há também transparência nesse procedimento: as tabelas de correspondência são disponibilizadas pelo TSE na internet até a véspera da votação.

Também são publicados os *logs* do Sistema GEDAI-UE das máquinas utilizadas para geração das mídias para as eleições.

No Portal de Dados Abertos do TSE, no menu "Conjunto de dados", **qualquer pessoa** pode consultar as correspondências esperadas e efetivadas de cada eleição, em todo o país.

Zerésima

Zerésima é o relatório emitido pela urna eletrônica, antes do início da votação, que comprova que não existe no equipamento nenhum voto dado a candidata ou candidato.

Antes da abertura da seção eleitoral no dia da votação, o presidente da mesa receptora de votos liga a urna eletrônica, na presença dos mesários e fiscais de partidos políticos, para emitir o relatório da zerésima. O procedimento reforça a transparência e a segurança do processo eleitoral ao mostrar que a urna **não contém voto algum para candidata ou candidato antes do começo da votação**.

Após a impressão da zerésima, todos os presentes devem assinar o documento. Com essas etapas finalizadas, a seção eleitoral pode ser liberada para receber as eleitoras e os eleitores.

Fonte: TSE.

Quer saber mais?

Assista ao vídeo Você sabe o que é zerésima?.

Boletim de urna

Encerrada a votação, a urna eletrônica imediatamente faz a apuração (contagem) dos votos da seção e, em seguida, imprime várias vias de um extrato chamado **boletim de urna (BU)**.

Figura 20 - Exemplo de boletim de urna (BU)

Fonte: TRE-SC (2025).

O BU contém diversos dados que foram registrados na urna durante a votação:

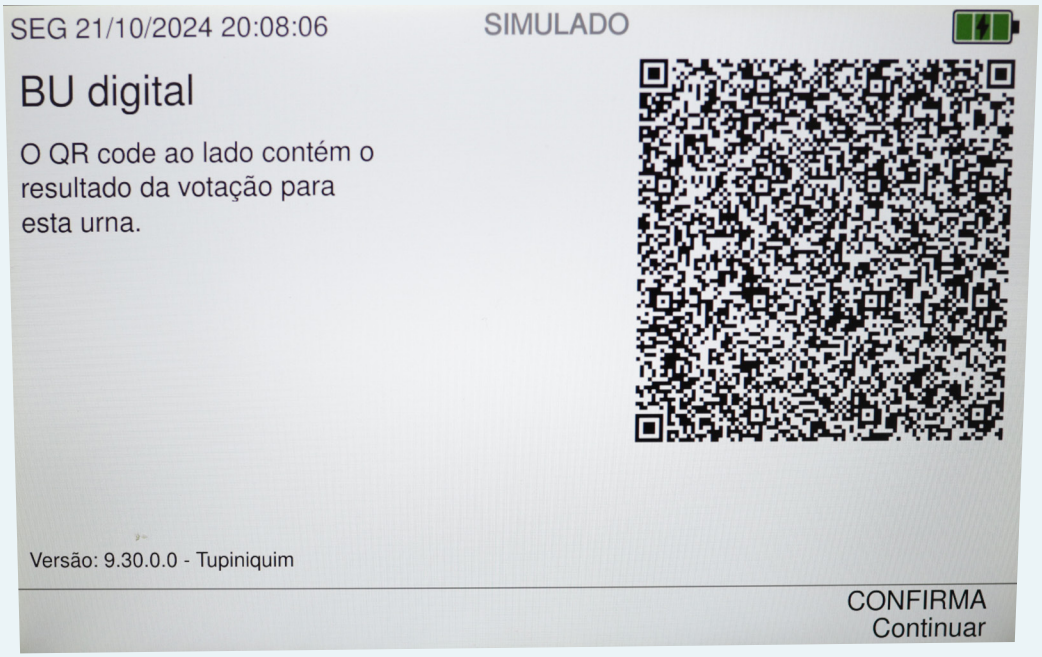
- total de votos por partido;
- total de votos por candidatura;
- total de votos nulos e em branco;
- total de comparecimento;
- identificação da seção e da zona eleitoral;
- hora do encerramento da eleição;
- código interno da urna eletrônica; e
- sequência de caracteres para a validação do boletim.

Uma das vias do BU é afixada na porta da seção eleitoral, tornando público o resultado daquela urna. Outra via será guardada pela própria pessoa que foi presidente da seção eleitoral para que possa conferir o resultado com o disponibilizado na internet. Vias adicionais ficam disponíveis para serem conferidas por fiscais dos partidos, das federações de partidos e das coligações.

Ao mesmo tempo, duas vias físicas do BU e a sua versão eletrônica (contida na memória de resultado) são enviadas à Junta Eleitoral. O resultado da seção é transmitido, em meio eletrônico, ao Tribunal Regional Eleitoral (TRE) do respectivo Estado.

Desde as eleições de 2016, os boletins de urna passaram a contar com um *QR Code*.

Figura 21 - *QR Code* na urna



Fonte: TRE-SC (2025).

Figura 22 - *QR Code* no boletim de urna

==========SIMULADO==========

----------PREFEITO----------

Nome do candidato Num cand Votos

MARIA EDUARDA LIMA 11 0005
MARIA IZABEL BOMFIM COSTA----------
----------> 12 0009
MARIA SENHORA DE FREITAS SOARE------
----------> 13 0006
ESTER GERALDA SILVA FERREIRA--------
----------> 15 0005

Eleitores aptos 0372
Originais da seção 0372
Temporários na seção 0000
Total de votos Nominais 0025
Brancos 0002
Nulos 0018
Total Apurado 0045

Código Verificador: 9.440.513.946

==========

---------- 1 de 2 ----------

---------- 2 de 2 ----------

ASSINATURA QR CODE:
844EFAE6CEAB2F4E2C9D0A36277520E3406SA6
4F3A798E0E23FCF37CB1751F0BB96705C8C268
701FC1339A8CF953407A4BE58EA902184B69FC
F46C6DFA1E3001

==========SIMULADO==========

Código de identificação da carga
738.137.064.676.943.852.710.328

Ver: 9.30.0.0

O conteúdo deste BU poderá ser conferido no endereço resultados.tse.jus.br

ASSINATURAS:

PRESIDENTE:

MESÁRIOS:

FISCAIS:

Fonte: TRE-SC (2025).

Por meio dele, **qualquer pessoa** pode ler os resultados do BU com a câmera de seu celular e auditar o resultado de uma ou mais seções, enquanto o TRE confere a autenticidade dos dados recebidos e inicia a contagem de votos no Estado.

Como os dados do boletim são codificados, é necessário um programa que faça a decodificação, permitindo o entendimento das informações. A Justiça Eleitoral (JE) disponibilizou o aplicativo **Boletim na Mão** para fazer a leitura desses BUs e armazenar os resultados no celular.

Há também a possibilidade de aplicativos desenvolvidos por terceiros fazerem a leitura desses BUs, uma vez que o algoritmo de leitura é público e disponibilizado pelo TSE na internet.

Figura 23 - *Leitura do QR Code* do boletim de urna

Fonte: TRE-SC (2025).

Sobre a divulgação na internet:

Desde as eleições de 2008, o TSE divulga na internet o boletim de urna, mas o prazo para disponibilização era de até 3 dias.

A partir das eleições de 2022, o TSE começou a disponibilizar os **boletins de urna e as tabelas de correspondência** em sua página na internet "**ao longo de todo o período de recebimento**, como alternativa de visualização, dando ampla divulgação nos meios de comunicação".

Publicação dos arquivos de RDV e *LOG* das urnas

Além dos boletins de urna, agora o TSE também publica na internet os arquivos de RDV e *LOG*. O objetivo é facilitar:

- a verificação da apuração dos votos em cada urna eletrônica, possibilitando análises a partir de estatísticas da votação; e
- a apuração do resultado da seção eleitoral a partir dos registros dos votos do RDV, comprovando-se o resultado do Boletim de Urna (BU).

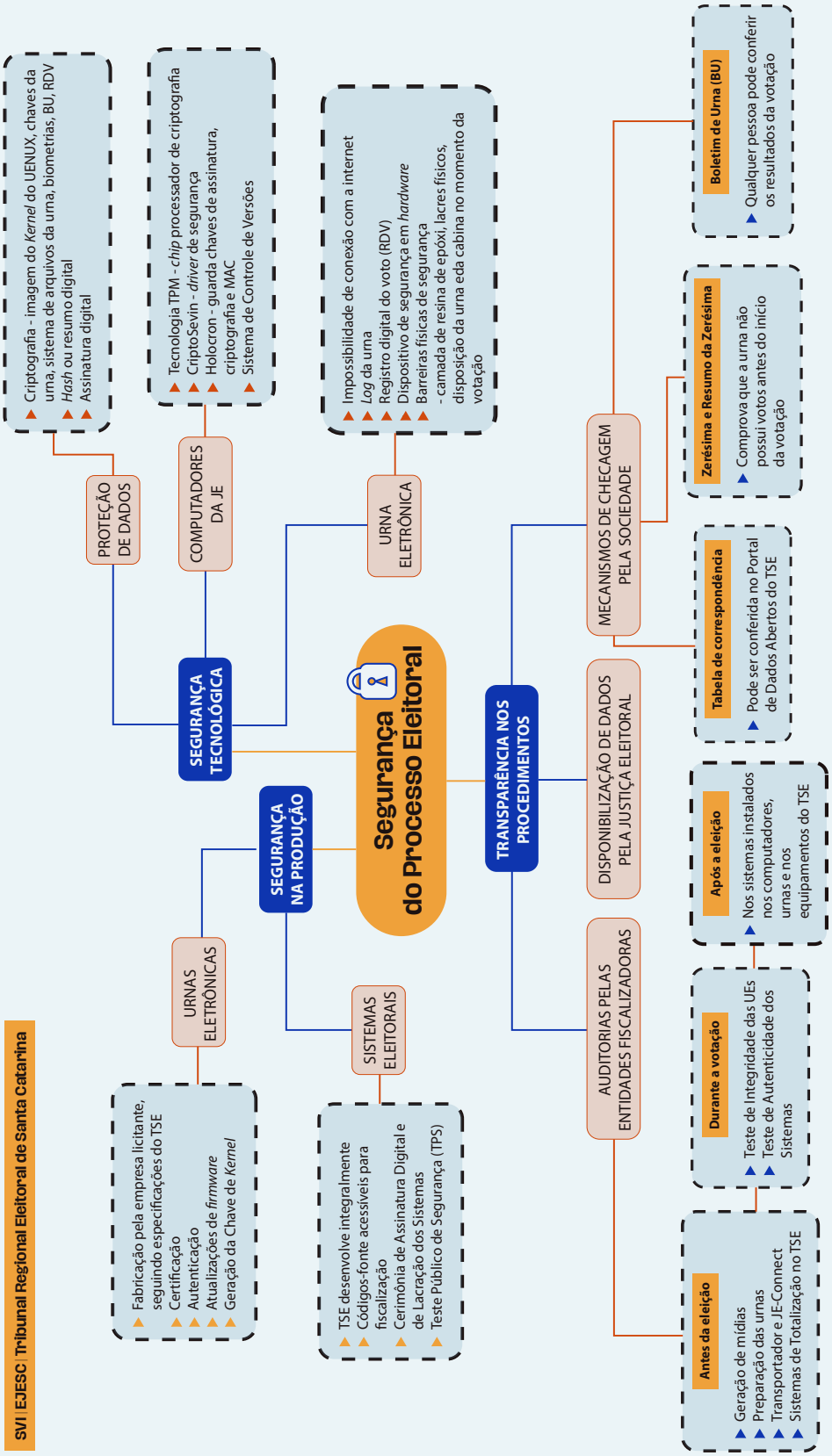
7.6. Infográfico e mapa mental sobre segurança do processo eleitoral

Para relembrar um pouco do que foi visto até aqui, veja o infográfico sobre os principais mecanismos de segurança do processo eletrônico de votação:

Figura 24 - Segurança da urna eletrônica, principais mecanismos

Fonte: Adaptado de Manual do Mesário (2024).

Figura 25 - Segurança da urna eletrônica, principais mecanismos



Fonte: Adaptado de Curso Segurança do Processo Eleitoral e Auditorias (2024).

MENSAGEM FINAL

8. MENSAGEM FINAL

A Justiça Eleitoral de Santa Catarina reuniu neste guia, para o leitor, em um instrumento único, não apenas conhecimento sobre o fenômeno da desinformação, mas mecanismos práticos e reais para efetivamente enfrentá-lo nas diversas áreas em que se manifesta, desde as mais simples atividades do cotidiano até a desinformação eleitoral, cujo potencial danoso ao processo democrático é muito real.

Como se sabe, no processo eleitoral vale a regra da intervenção judicial mínima no debate político, em respeito à livre manifestação do pensamento, protegida pela Constituição brasileira como direito fundamental (art. 5º, IV), com vedação constitucional à censura prévia (arts. 5º, IX, e 220, § 2º) e liberdade de expressão assegurada aos cidadãos sobretudo na condição de eleitores, para que participem e elejam a mais autêntica representação popular, no sagrado exercício do voto.

Por outro lado, se é crescente a preocupação com a desinformação, mais ainda se dá com a que tem como alvo o processo eleitoral e a Justiça Eleitoral, constantemente atingidos por narrativas enganosas e mesmo abertamente falsas, que visam a abalar a confiança nas instituições eleitorais e sobretudo no sistema eletrônico de votação – concebido, originado e desenvolvido em Santa Catarina. Em que pesem os avanços da Justiça Eleitoral para enfrentar o fenômeno da desinformação, os riscos de que esse fenômeno afete gravemente o processo eleitoral, com impactos quer à integridade do processo, quer à livre manifestação do voto, segue presente.

A propagação de desinformação, que pode ocorrer de forma orquestrada, é completamente distinta da crítica – que, mais do que aceitável, é necessária. Ela escala potenciais elevadíssimos de danos coletivos se adicionados os ingredientes, a cada dia mais acessíveis, da inteligência artificial e da proliferação de *deepfakes* pela produção de mídias sintéticas com capacidade para produzir conteúdo falso cada vez mais convincentes.

É importante munir de informações confiáveis o eleitor médio sem, contudo, deixar de trazer aos especialistas, inclusive da área tecnológica, múltiplas informações de que necessitem para avaliar e, espera-se, propagar informações verificáveis, íntegras, enfim, verdadeiras.

Os esforços despendidos no âmbito do Tribunal Regional Eleitoral de Santa Catarina, para compilar, estudar e aperfeiçoar medidas de enfrentamento de desinformação contra o processo eleitoral com informação útil e de qualidade, proporcional a um cenário tecnológico cada vez mais desafiador, mostram-se necessários e oportunos.

Institucionalmente, a Justiça Eleitoral catarinense propõe o enfrentamento dessa realidade tão complexa de forma simultânea e efetiva, estruturado em três eixos de sustentação: informação, capacitação e resposta.

O conteúdo desenvolvido e posto à disposição da sociedade neste guia materializa ação de educação e capacitação midiática importante, convicto que está o Tribunal Regional Eleitoral de Santa Catarina de que a capacidade de produzir e divulgar a contrainformação pode ser em muito ampliada se o eleitor souber, de antemão, como reconhecer a informação falsa. E essa habilidade exige letramento digital, identificação de confiabilidade da informação recebida e prevenção contra a disseminação de informações falsas, conteúdos que perpassam todo este guia.

REFERÊNCIAS

REFERÊNCIAS

ABRAJI. Disponível em: https://abraji.org.br. Acesso em: 24 jun. 2025.

AFP CHECAMOS. Disponível em: https://checamos.afp.com. Acesso em: 24 jun. 2025.

AGÊNCIA LUPA. Disponível em: https://lupa.uol.com.br. Acesso em: 24 jun. 2025.

ALFREDO, Maurício. **Economia da atenção: um desafio à democracia.** Observatório da Imprensa, 10 out. 2024. Disponível em https://www.observatoriodaimprensa.com.br/politica/economia-da-atencao-um-desafio-a-democracia. Acesso em: 16 jun. 2025.

AOS FATOS. Disponível em: https://www.aosfatos.org. Acesso em: 24 jun. 2025.

BBC NEWS BRASIL. **Pesquisadores criam Barack Obama digital capaz de falar como se fosse o original**. YouTube, 18 jul. 2017. 1 vídeo (1 min1s). Disponível em: https://www.youtube.com/watch?v=E6zBwqa3FTs. Acesso em: 24 jun. 2025.

BOATOS.ORG. Disponível em: https://www.boatos.org. Acesso em: 24 jun. 2025.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 2016. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 15 abr. 2025.

_____. Conselho Nacional de Justiça. **Painel de checagem de *Fake News***. Disponível em: https://www.cnj.jus.br/programas-e-acoes/painel-de-checagem-de-fake-news/guia-pratico. Acesso em: 24 jun. 2025.

_____. Justiça Eleitoral. Disponível em: https://www.justicaeleitoral.jus.br. Acesso em: 24 jun. 2025.

_____. Justiça Eleitoral. **Auditoria e Fiscalização**. Brasília, DF. Disponível em https://www.justicaeleitoral.jus.br/urna-eletronica/oportunidades-de-auditoria-e-fiscalizacao.html. Acesso em: 16 jun. 2025.

_____. Justiça Eleitoral. **Curso - Segurança e Auditoria nas Eleições Brasileiras**. Youtube, 5 ago. 2022. 1 vídeo. 2h01min22s. Disponível em: https://www.youtube.com/watch?v=U_GIMa99KBk. Acesso em: 16 jun. 2025.

_____. Justiça Eleitoral. **Histórico das fraudes nas eleições**. Brasília, DF, Disponível em https://www.justicaeleitoral.jus.br/urna-eletronica/historico-das-fraudes-nas-eleicoes.html. Acesso em: 26 jun. 2025.

_____. Justiça Eleitoral. **Manual do Mesário**. Brasília, DF, 2024. Disponível em https://www.justicaeleitoral.jus.br/eleicoes/mesario/assets/arquivos/Manual_do_mesario_2024_WEB_Seprev_OK_FINAL.pdf. Acesso em: 16 jun. 2025.

_____. Justiça Eleitoral. **Programa de Enfrentamento à Desinformação**. Brasília, DF, Disponível em https://www.justicaeleitoral.jus.br/desinformacao. Acesso em: 24 jun. 2025.

_____. Justiça Eleitoral. **Teste Público de Segurança da Urna**. Brasília, DF, [s.d.]. Disponível em https://www.justicaeleitoral.jus.br/tps/#. Acesso em: 16 jun. 2025.

_____. Justiça Eleitoral de SC. **Plebiscito para a emancipação do Distrito de Cocal - 1991**. Youtube. 8 set. 2022. 1 vídeo (5min53s). Disponível em: https://www.youtube.com/watch?v=u6daeHT5q-g. Acesso em: 26 jun. 2025.

_____. Justiça Eleitoral de SC. **Você sabe o que é zerésima?**. Youtube. 23 ago. 2021. 1 vídeo (48s). Disponível em: https://www.youtube.com/watch?v=ovenIQ5WVro. Acesso em: 16 jun. 2025.

_____. **Lei n° 9.504, de 30 de setembro de 1997**. Estabelece normas para as eleições. Brasília, DF, 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9504.htm. Acesso em: 26 jun. 2025.

_____. **Lei n° 10.740, de 1º de outubro de 2003**. Altera a Lei nº 9.504, de 30 de setembro de 1997, e a Lei nº 10.408, de 10 de janeiro de 2002, para implantar o registro digital do voto. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/L10.740.htm. Acesso em: 27 jun. 2025.

_____. Tribunal Superior Eleitoral. **Cédulas eleitorais**. Disponível em: https://www.tse.jus.br/institucional/museu-do-voto/temas/cedulas-eleitorais. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. **Criptografia**. Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/criptografia. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. Dispõe sobre a propaganda eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. Dispõe sobre a realização periódica do Teste Público de Segurança - TPS nos sistemas eleitorais que especifica. **Resolução nº 23.444, de 30 de abril de 2015**. Disponível em: https://www.tse.jus.br/legislacao/codigo-eleitoral/normas-editadas-pelo-tse/resolucao-no-23-444-de-30-de-abril-de-2015-2013-brasilia-2013-df. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. Dispõe sobre os procedimentos de fiscalização e auditoria do sistema eletrônico de votação. **Resolução n.º 23.673, de 14 de dezembro de 2021**. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-673-14-de-dezembro-de-2021. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. Dispõe sobre o enfrentamento à desinformação que atinja a integridade do processo eleitoral. **Resolução nº 23.714, de 22 de outubro de 2022**. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2022/resolucao-no-23-714-de-20-de-outubro-de-2022. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. Dispõe sobre o uso do aplicativo Pardal Móvel para denúncias de propaganda irregular nas eleições 2024. **Portaria nº 662, de 15 de agosto de 2024**. Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2024/portaria-no-662-de-15-de-agosto-de-2024. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. **Teste público de segurança da urna: guia para jornalistas**. Disponível em: https://www.tse.jus.br/institucional/catalogo-de-publicacoes/lista-do-catalogo-de-publicacoes/publicacoes/t/teste-da-urna-2023-guia-para-jornalistas. Acesso em 24 jun. 2025.

_____. Tribunal Superior Eleitoral. Institui o Programa Permanente de Enfrentamento à Desinformação no âmbito da Justiça Eleitoral e disciplina a sua execução. **Portaria nº 510, de 4 de agosto de 2021**. Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-510-de-04-de-agosto-de-2021. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. Institui o Programa de Fortalecimento Institucional a Partir da Gestão da Imagem da Justiça Eleitoral - PROFI no âmbito da Justiça Eleitoral e disciplina a sua execução. **Portaria nº 282, de 22 de março de 2022**. Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2022/portaria-no-282-de-22-de-marco-de-2022. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. Institui o Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia e disciplina a sua atuação. **Portaria nº 180, de 12 de março de 2024**. Disponível em: https://www.tse.jus.br/legislacao/compilada/prt/2024/portaria-no-180-de-12-de-marco-de-2024. Acesso em: 26 jun. 2025.

_____. Tribunal Superior Eleitoral. **Portal de Dados Abertos do TSE**. Brasília, DF. Disponível em: https://dadosabertos.tse.jus.br. Acesso em: 16 jun. 2025.

_____. Tribunal Superior Eleitoral. **Plano de Ação elaborado pela Comissão de Transparência deixará as eleições ainda mais seguras**. 25 abr. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Abril/plano-de-acao-elaborado-pela-comissao-de-transparencia-deixara-as-eleicoes-ainda-mais-seguras. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. **Registro Digital do Voto permite recontagem e amplia transparência do processo eleitoral**. Brasília, DF, Disponível em: https://www.tse.jus.br/comunicacao/noticias/2021/Julho/registro-digital-do-voto-permite-recontagem-e-amplia-transparencia-do-processo-eleitoral. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. **Resumos digitais (*hashes*) dos sistemas eleitorais**. Brasília, DF, Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/*hash*/resumos-digitais-*hash*-dos-sistemas-eleitorais. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. **Resumos digitais (*hashes*) das Eleições 2024 – 1º e 2º turnos**. Brasília, DF, Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/*hash*/resumos-digitais-*hashes*-das-eleicoes-2024-1o-e-2o-turnos. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. **Sistema de Alertas de Desinformação Eleitoral - SIADE**. Brasília, DF. Disponível em: https://www.tse.jus.br/eleicoes/sistema-de-alertas. Acesso em: 27 jun. 2025.

_____. Tribunal Superior Eleitoral. **Visão Gráfica Aplicativo Pardal**. Brasília, DF. Disponível em: https://www.tse.jus.br/++theme++justica_eleitoral/pdfjs/web/viewer.html?file=https://www.tse.jus.br/comunicacao/arquivos/infografico-do-aplicativo-pardal/@@download/file/vg_app_pardal-3_5_24.pdf. Acesso em: 24 jun. 2025.

_____. Tribunal Superior Eleitoral. **Você sabe o que é zerésima? O Glossário explica**. Brasília, DF, 26 jul. 2023. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2023/Julho/voce-sabe-o-que-e-zeresima-o-glossario-explica. Acesso em: 16 jun. 2025.

_____. Escola Judiciária Eleitoral de Santa Catarina. **Segurança do Processo Eleitoral e Auditorias - 2024**. Curso EaD. Florianópolis, SC, 20 maio 2024 a 30 ago. 2024. Disponível em: https://apps.tre-sc.jus.br/moodle/enrol/index.php?id=218.

_____. Tribunal Regional Eleitoral de Santa Catarina. Institui o Programa Permanente de Enfrentamento à Desinformação no âmbito do Tribunal Regional Eleitoral de Santa Catarina (TRE-SC). **Portaria P nº 66, de 2 de junho de 2021**. Disponível em: https://www.tre-sc.jus.br/legislacao/compilada/portaria-p/2021/portaria-p-n-66-de-2-de-junho-de-2021. Acesso em: 26 jun. 2025.

_____. Institui o Programa Permanente de Enfrentamento à Desinformação no âmbito do Tribunal Regional Eleitoral de Santa Catarina (TRE-SC). **Portaria P nº 135, de 22 de agosto de 2024**. Disponível em: https://www.tre-sc.jus.br/legislacao/compilada/portaria-p/2024/portaria-p-n-135-de-22-de-agosto-de-2024. Acesso em: 7 abr. 2025.

BRITO, Edivaldo. **Endereço MAC: o que é, como ver e o que fazer com o identificador**. TechTudo, 3 nov. 2014. Disponível em https://www.techtudo.com.br/noticias/2014/11/o-que-e-endereco-mac-saiba-como-encontrar.ghtml. Acesso em: 16 jun. 2025.

CATAI PORTAL. **O VEO3 mudou tudo: você precisa mandar esse vídeo no grupo do zap da sua família**. Instagram. 31 maio 2025. Disponível em: https://www.instagram.com/reel/DKUOtfyNrOX/?igsh=MTU4OXJhZmZxN3E3Yg%3D%3D. Acesso em: 24 jun. 2025.

CERT.BR. **Cartilha sobre Segurança para Internet Fascículos**. Disponível em https://cartilha.cert.br/fasciculos. Acesso em: 24 jun. 2025.

CERT.BR. **Cartilha sobre Segurança para Internet Dicas Rápidas**. Disponível em https://cartilha.cert.br/dicas-rapidas. Acesso em: 24 jun. 2025.

COMISSÃO EUROPEIA: Diretório-Geral para Redes de Comunicação, Conteúdo e Tecnologia. ***A multi-dimensional approach to disinformation*** – Report of the independent High level Group on fake news and *online* disinformation, Publications Office, 2018. Disponível em: https://data.europa.eu/doi/10.2759/739290. Acesso em 1 jul. 2025.

DESINFORMANTE. **O que é *deepfake*?** YouTube. 15 mar. 2023. 1 vídeo (6min35s). Disponível em: https://www.youtube.com/watch?v=1tFqyHqn2uQ . Acesso em: 24 jun. 2025.

EDUCAMÍDIA. **Educação midiática e IA**. Disponível em: https://educamidia.org.br/educacao-midiatica-e-inteligencia-artificial. Acesso em: 24 jun. 2025.

E-FARSAS. Disponível em: https://www.e-farsas.com. Acesso em: 24 jun. 2025.

ESTADÃO VERIFICA. Disponível em: https://www.estadao.com.br/estadao-verifica. Acesso em: 24 jun. 2025.

FATO OU BOATO. Disponível em: https://www.justicaeleitoral.jus.br/fato-ou-boato. Acesso em 24 jun. 2025.

FATO OU FAKE. Disponível em: https://g1.globo.com/fato-ou-fake. Acesso em: 24 jun. 2025.

FELDSTEIN, Steven (editor). ***Digital Democracy in a Divided Global Landscape***. New York: Carnegie Endowment for International Peace, 2025. Disponível em: https://carnegieendowment.org/research/2025/05/digital-democracy-in-a-divided-global-landscape?lang=en. Acesso em: 1 jul. 2025.

FERREIRA, Bruno. **E-books Educom**. Disponível em https://brunoeducom.com.br/e-books. Acesso em: 24 jun. 2025.

FOLHA. **A história da urna eletrônica no Brasil**. Disponível em: https://www1.folha.uol.com.br/webstories/cultura/2020/08/a-historia-da-urna-eletronica. Acesso em: 24 jun. 2025.

GOV.BR. Disponível em: https://www.gov.br/pt-br. Acesso em: 24 jun. 2025.

GOV.UK. ***Online disinformation and IA threat guidance for electoral candidates and officials***. Reino Unido, 30 abr. 2025. Disponível em:https://www.gov.uk/government/publications/security-guidance-for-may-2021-elections/*online*-disinformation-and-ai-threat-guidance-for-electoral-candidates-and-officials. Acesso em: 1 jul. 2025.

KOSMYNA, Nataliya; HAUPTMANN, Eugene; YUAN, YeTong; SITU, Jessica; LIAO, Xian-Hao; BERESNITZKY, Ashly Vivian; BRAUNSTEIN, Iris; MAES, Pattie. **Your Brain on *ChatGPT:*** *Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task*. Cornell University, New York, 10 jun. 2025.Disponível em: https://arxiv.org/abs/2506.08872. Acesso: 1 jul. 2025.

MANUAL DO MUNDO. **MENSAGEM SECRETA: Entenda a CRIPTOGRAFIA**. Youtube. 17 set. 2021. 1 vídeo (9min36s) . Disponível em: https://www.youtube.com/watch?v=aTI99jztZds&list=PLIrCHkvlD-1SGEHyIF0IrQEHlads_hWVl&index=4&t=218s. Acesso em: 24 jun. 2025.

MICROSOFT. **Visão geral da tecnologia *Trusted Platform Module***. 24 fev. 2025. Disponível em: https://learn.microsoft.com/pt-br/windows/security/hardware-security/tpm/trusted-platform-module-overview. Acesso em: 16 jun. 2025.

MINISTÉRIO PÚBLICO FEDERAL. **MPF Serviços**. Disponível em: https://www.mpf.mp.br/mpfservicos. Acesso em: 24 jun. 2025.

NAÇÕES UNIDAS. **Princípios Globais das Nações Unidas para a Integridade da Informação** - Recomendações para Ação de Múltiplas Partes Interessadas. Disponível em https://brasil.un.org/*sites*/default/files/2024-07/ONU_PrincipiosGlobais_IntegridadeDaInformacao_20240624.pdf. Acesso em: 16 jun. 2025.

NATIONAL CYBER SECURITY CENTRE. ***Defending democracy***. Reino Unido, 15 mai. 2024. 6 pag. Disponível em: https://www.ncsc.gov.uk/collection/defending-democracy/resources. Acesso em: 1 jul. 2025.

NICOLAU, Jairo. **A história do voto no Brasil**. Rio de Janeiro: Jorge Zahar, 2002.

O GLOBO. **Fraudes na eleição de 1994 mostram caos na apuração antes da urna eletrônica**. Blog do Acervo, Rio de Janeiro, 19 jul. 2022. Disponível em: https://oglobo.globo.com/blogs/blog-do-acervo/post/2022/07/fraudes-na-eleicao-de-1994-mostram-como-era-apuracao-antes-da-urna-eletronica.ghtml. Acesso em: 2 set. 2025.

PORTAL G1. **Show de Lady Gaga será de graça no Rio? Sem ingresso mesmo?** 30 abr. 2025. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/show-da-lady-gaga/noticia/2025/04/30/show-de-lady-gaga-sera-de-graca-no-rio-sem-ingresso-mesmo.ghtml. Acesso em: 24 jun. 2025

POSETTI, Julie; MATTHEWS, Alice. **A Short Guide to the History of 'Fake News' and Disinformation**. International Center for Journalists – ICFJ, 2018. Disponível em: https://www.icfj.org/*sites*/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf. Acesso em: 1 jul. 2025.

PROJETO COMPROVA. Disponível em: https://projetocomprova.com.br. Acesso em 24 jun. 2025.

PROJETO COMPROVA. **Aprenda a identificar boatos nas redes**. Disponível em: https://projetocomprova.com.br/aprenda-a-identificar-boatos-nas-redes. Acesso em 24 jun. 2025.

PROJETO COMPROVA. **Dicas para verificar conteúdos de diferentes formatos e não espalhar desinformação**. Disponível em: https://projetocomprova.com.br/dicas. Acesso em 24 jun. 2025.

PROJETO COMPROVA. **Entenda como funcionam os algoritmos e veja dicas para tentar escapar das bolhas**. 9.5.2025. Disponível em: https://projetocomprova.com.br/publica%C3%A7%C3%B5es/entenda-como-funcionam-os-algoritmos-e-veja-dicas-para-tentar-escapar-das-bolhas. Acesso em: 16 jun. 2025.

PROJETO COMPROVA. **Inteligência Artificial: o básico para entendê-la**. Disponível em: https://projetocomprova.com.br/inteligencia-artificial-o-basico-para-jornalistas. Acesso em 24 jun. 2025.

RAIS, Diogo. **Direito eleitoral digital**. São Paulo: Thomson Reuters, 2018.

SEGINFO. **PF e FBI não conseguem ter acesso aos dados criptografados de Daniel Dantas**. 28 jun. 2010. Disponível em: https://seginfo.com.br/2010/06/28/pf-e-fbi-nao-conseguem-ter-acesso-aos-dados-criptografados-de-daniel-dantas. Acesso em: 26 jun. 2025.

UOL CONFERE. Disponível em: https://noticias.uol.com.br/confere. Acesso em 24 jun. 2025.

WHICH FACE IS REAL. Disponível em: https://www.whichfaceisreal.com. Acesso em 24 jun. 2025.

ANEXO

ANEXO I

Imagem

Ferramenta/Idioma	FotoForensics/Inglês
Funcionalidades	Análise de Nível de Erro (ELA), análise de metadados (EXIF), visualização de estrutura JPEG, detecção de potencial clonagem.
Benefícios	Gratuito (maioria das funções), revela inconsistências e potenciais manipulações na estrutura da imagem que não são visíveis a olho nu, baseado na web (fácil acesso).
Restrições	Requer conhecimento técnico para interpretar corretamente os resultados (especialmente ELA). Não prova autenticidade, apenas indica possíveis edições. Metadados podem ser removidos ou falsificados.
Aplicabilidade em órgão público	Investigar a autenticidade de imagens recebidas ou encontradas *online* que pareçam suspeitas. Útil para equipes de perícia digital ou comunicação com treinamento específico.

Ferramenta/Idioma	InVID Verification Plugin (Extensão p/ Navegador)/Inglês
Funcionalidades	Análise forense de imagens (filtros, metadados), busca reversa de imagens em múltiplos motores (*Google*, *Bing*, *Yandex*, *TinEye*), análise de miniaturas de vídeo (*keyframes*).
Benefícios	Ferramenta "tudo-em-um" para verificação rápida. Agrega várias técnicas em uma interface. Facilita a busca por origem e contexto. Amplamente usada por jornalistas. Gratuito.
Restrições	Depende da disponibilidade e indexação dos motores de busca externos. Algumas análises forenses exigem conhecimento técnico. Funciona como extensão de navegador (*Chrome*/*Firefox*).
Aplicabilidade em órgão público	Essencial para equipes de comunicação e imprensa para verificar rapidamente imagens e vídeos que circulam *online*, identificar uso fora de contexto ou reutilização de material antigo.

Ferramenta/Idioma	TinEye/Inglês
Funcionalidades	Busca reversa de imagens. Encontra onde uma imagem específica (ou versões modificadas dela) apareceu *online* anteriormente.
Benefícios	Gratuito para uso não comercial.Excelente para rastrear a origem e o primeiro uso de uma imagem. Identifica reutilização e uso fora de contexto. Interface simples. Possui API (paga) para automação.
Restrições	Focado em encontrar cópias *online*, não analisa a imagem em si para edições. Pode não encontrar imagens muito recentes ou não indexadas publicamente.
Aplicabilidade em órgão público	Verificar se uma imagem atribuída a um evento recente é, na verdade, antiga. Descobrir a fonte original de uma fotografia. Monitorar o uso de imagens oficiais do órgão.

Ferramenta/Idioma	Truepic/Inglês
Funcionalidades	Captura de fotos/vídeos com metadados seguros e verificáveis (hora, data, local, dispositivo) via app ou SDK. Cria um registro digital inviolável no momento da captura.
Benefícios	Garante a autenticidade da imagem/vídeo no momento da captura. Dificulta a falsificação de evidências visuais. Gera um "selo" de autenticidade verificável.
Restrições	Não verifica imagens/vídeos existentes que não foram capturados com a tecnologia Truepic. É uma solução comercial (requer implementação e pode ter custos).
Aplicabilidade em órgão público	Coleta de evidências em vistorias, fiscalizações ou auditorias. Registro de condições de infraestrutura. Documentação oficial onde a autenticidade da captura é crítica (requer adoção da tecnologia).

Ferramenta/Idioma	SunCalc/Inglês
Funcionalidades	Calcula a posição do sol (azimute, altitude, trajetória) e a direção das sombras para qualquer local, data e hora.
Benefícios	Ajuda a verificar a consistência temporal e geográfica de uma imagem com base nas sombras presentes. Gratuito e fácil de usar.
Restrições	Requer que a imagem tenha sombras claras e pontos de referência identificáveis. A precisão depende da identificação correta do local e hora (ou da alegação a ser verificada).
Aplicabilidade em órgão público	Validar a plausibilidade de data/hora alegada para uma foto (ou vídeo) com base na iluminação solar e sombras. Útil em investigações ou análise de denúncias que envolvam locais externos.

Vídeo

Ferramenta/Idioma	InVID Verification Plugin (Extensão p/ Navegador)/Inglês
Funcionalidades	Extração de *Keyframes* (quadros-chave), busca reversa desses *keyframes*, análise de metadados, análise forense de vídeo, verificação de direitos autorais (*YouTube*).
Benefícios	Ferramenta multifuncional para análise rápida de vídeos. Permite decompor o vídeo em imagens para análise individual e busca reversa. Integra várias funcionalidades úteis. Gratuito.
Restrições	A análise forense detalhada pode ser complexa. A busca reversa depende dos motores externos.
Aplicabilidade em órgão público	Ferramenta de linha de frente para verificar vídeos virais, checar se são montagens, se foram filmados onde/quando alegado, ou se são antigos e reutilizados.

Ferramenta/Idioma	Deepware Scanner/Inglês
Funcionalidades	Detecção de *Deepfakes* em Vídeos: A ferramenta analisa arquivos de vídeo enviados ou URLs de plataformas como *YouTube*, *Facebook* e *X* para identificar manipulações faciais geradas por Inteligência Artificial (IA). Análise Baseada em IA: Utiliza um modelo de IA que foca em identificar sinais de manipulação na área do rosto de pessoas presentes no vídeo. Processamento Assíncrono: As solicitações de varredura são adicionadas a uma fila e processadas em segundo plano. Relatórios de Análise: Pode fornecer relatórios que indicam as áreas da mídia que foram potencialmente alteradas.
Benefícios	Combate à Desinformação: Ajuda a identificar conteúdo de vídeo fabricado, prevenindo a disseminação de notícias falsas e narrativas enganosas. Proteção contra Falsificação de Identidade: Auxilia na detecção de vídeos que utilizam rostos de pessoas de forma fraudulenta. Verificação de Autenticidade: Permite uma camada de verificação da autenticidade de vídeos antes de serem compartilhados ou utilizados como fonte de informação. Acesso Gratuito (Beta): Atualmente, a ferramenta pode ser utilizada gratuitamente, o que facilita o acesso à tecnologia de detecção.
Restrições	Fase Beta: A ferramenta ainda está em fase *Beta*, o que significa que sua precisão e funcionalidades podem estar em contínuo desenvolvimento e aprimoramento. Podem ocorrer falsos positivos ou falsos negativos. Foco em Manipulações Faciais: O *Deepware Scanner* é especializado na detecção de manipulações em rostos humanos em vídeos. Ele não detecta manipulações de voz ou outros tipos de mídia sintética. Necessidade de Rostos Humanos: Para que a análise seja efetiva, o vídeo submetido deve conter rostos humanos. Limite de Duração do Vídeo: Existe um limite para a duração dos vídeos que podem ser escaneados (atualmente, 10 minutos por vídeo). Resolução Recomendada: Para melhores resultados, recomenda-se que os vídeos tenham uma resolução de pelo menos 1920x1080. Termos de Serviço: O uso da ferramenta está sujeito a termos de serviço que incluem restrições quanto ao uso indevido ou ilegal.

Aplicabilidade em órgão público	Verificação de Conteúdo Midiático: Órgãos governamentais podem utilizar a ferramenta para analisar vídeos suspeitos que circulam em redes sociais ou são enviados como denúncias, ajudando a discernir entre conteúdo autêntico e manipulado. Análise de Evidências Digitais: Em contextos investigativos ou de inteligência, a ferramenta pode oferecer um suporte preliminar na análise de vídeos, identificando possíveis adulterações. Comunicação Pública e Alerta: Departamentos de comunicação podem usar a ferramenta para verificar a autenticidade de vídeos antes de divulgá-los ou para alertar o público sobre a circulação de *deepfakes* específicos. Fortalecimento da Integridade Informacional: Contribui para os esforços de órgãos públicos em manter a integridade das informações e combater campanhas de desinformação que possam afetar a opinião pública, a segurança ou a estabilidade.

Ferramenta/Idioma	YouTube Data Viewer/Inglês
Funcionalidades	Extrai a data e hora exatas de upload de um vídeo no YouTube. Permite extrair miniaturas (*thumbnails*) para busca reversa.
Benefícios	Simples e direto para descobrir quando um vídeo foi carregado no *YouTube* (não quando foi gravado). Facilita a busca reversa das miniaturas para encontrar cópias ou origem. Gratuito.
Restrições	Funciona apenas para vídeos hospedados no *YouTube*. A data de upload pode não corresponder à data do evento. Ferramenta pode ficar indisponível temporariamente.
Aplicabilidade em órgão público	Verificar rapidamente se um vídeo que alega ser de um evento atual foi, na verdade, postado muito antes. Identificar a data de publicação original de vídeos relevantes.

Ferramenta/Idioma	FotoForensics/Inglês
Funcionalidades	Análise de frames individuais de um vídeo (exportados como imagem) usando as mesmas técnicas de análise de imagem (ELA, metadados).
Benefícios	Permite aplicar análise forense a quadros específicos de um vídeo para detectar inconsistências ou edições.
Restrições	Requer a exportação prévia dos frames do vídeo. Análise demorada se muitos frames precisarem ser verificados. Mesmas limitações de interpretação do *FotoForensics* para imagens.
Aplicabilidade em órgão público	Análise aprofundada de quadros específicos em vídeos suspeitos de manipulação (requer exportação dos frames e conhecimento técnico). Menos prático para verificação rápida.

Ferramenta/Idioma	Amnesty International's YouTube Dataviewer/Inglês
Funcionalidades	Mesmas funcionalidades do *YouTube DataViewer* listado acima. Ferramenta desenvolvida pela Anistia Internacional.
Benefícios	Mesmos benefícios do *YouTube DataViewer*.
Restrições	Mesmas restrições do *YouTube DataViewer*.
Aplicabilidade em órgão público	Mesma aplicabilidade do *YouTube DataViewer*.

Ferramenta/Idioma	SunCalc/Inglês
Funcionalidades	Calcula a posição do sol e sombras para qualquer local, data e hora, aplicável à análise de cenas em vídeo.
Benefícios	Ajuda a verificar a consistência temporal e geográfica de um vídeo com base nas sombras visíveis nas cenas. Gratuito.
Restrições	Requer cenas com sombras claras e referências geográficas. A análise pode ser complexa se a câmera ou os objetos se movem muito.
Aplicabilidade em órgão público	Validar a plausibilidade de data/hora alegada para um vídeo baseado na iluminação e sombras. Útil em investigações de vídeos gravados em ambientes externos.

Texto

Ferramenta/Idioma	Snopes/Inglês
Funcionalidades	Base de dados extensa e pesquisável de checagens de fatos sobre rumores, lendas urbanas, desinformação, notícias falsas e alegações políticas/sociais.
Benefícios	Um dos *sites* de *fact-checking* mais antigos e conhecidos. Boa cobertura de desinformação viral e cultura da internet. Metodologia geralmente transparente. Gratuito.
Restrições	Foco principal em tópicos de interesse global ou dos EUA. Pode não ter cobertura extensiva de assuntos estritamente locais ou regionais do Brasil. É um repositório, não uma ferramenta de análise de texto.
Aplicabilidade em órgão público	Consultar se um boato específico que está circulando (inclusive internamente no órgão) já foi verificado. Fonte de referência para desmentir desinformação comum.

Ferramenta/Idioma	FactCheck.org/Inglês
Funcionalidades	Checagem de fatos focada em política dos EUA, mas também cobre saúde, ciência e outras alegações factuais. Projeto do A*nnenberg Public Policy Center*.
Benefícios	Checagens aprofundadas, bem pesquisadas e referenciadas. Considerado não-partidário e confiável. Gratuito.
Restrições	Foco geográfico muito específico (EUA). Pouca ou nenhuma cobertura de política ou boatos locais do Brasil.
Aplicabilidade em órgão público	Modelo de metodologia de checagem. Consulta sobre temas de ciência ou saúde com repercussão internacional que possam afetar políticas ou comunicações do órgão.

Ferramenta/Idioma	FakeCheck - Detector de *Fake News*/Português
Funcionalidades	Análise de *URL* para identificar notícias falsas.
Benefícios	Gratuito, interface em português e fácil de usar, oferece um resultado rápido sobre a probabilidade de uma notícia ser falsa ou verdadeira.
Restrições	Não é 100% preciso, dependendo da base de dados e dos algoritmos utilizados. Pode apresentar falsos positivos ou falsos negativos. Não substitui a checagem manual de fatos.

Aplicabilidade em órgão público	Pode ser usada para triagem inicial de notícias suspeitas divulgadas em redes sociais ou outros meios *online*, auxiliando equipes de comunicação ou análise de informações.

Ferramenta/Idioma	Google Fact Check Tools/Inglês
Funcionalidades	Inclui o *Fact Check Explorer* (busca checagens de fatos de várias agências parceiras globalmente) e o *Fact Check Markup Tool* (para publicadores marcarem suas checagens).
Benefícios	Agrega checagens de diversas fontes confiáveis (incluindo agências brasileiras). Facilita encontrar rapidamente se uma alegação já foi verificada por múltiplos checadores. Gratuito.
Restrições	É um agregador/buscador, não realiza a checagem em si. A qualidade e cobertura dependem das agências parceiras. A interface do Explorer pode ser simples demais para análises complexas.
Aplicabilidade em órgão público	Ferramenta essencial para buscar rapidamente checagens existentes sobre um determinado boato ou alegação antes de iniciar uma investigação própria. Monitorar temas que estão sendo checados.

Ferramenta/Idioma	Hoaxy/Inglês
Funcionalidades	Visualiza a disseminação *online* (principalmente *X*) de *links* para artigos de fontes de baixa e alta credibilidade, mostrando como a informação (e desinformação) se espalha.
Benefícios	Permite entender a dinâmica viral de uma notícia ou boato específico (que tenha um *link* associado). Identifica contas influentes na disseminação. Gratuito.
Restrições	Focado na disseminação de *links*, não analisa o conteúdo em si. Dependente de dados históricos (principalmente *Twitter API*). A visualização em grafo pode requerer interpretação.
Aplicabilidade em órgão público	Analisar a origem e o padrão de viralização de campanhas de desinformação específicas que se baseiam em *links*. Útil para análise estratégica de comunicação e resposta a crises.

Ferramenta/Idioma	LongShot AI/Inglês
Funcionalidades	Plataforma de escrita e geração de conteúdo por IA que inclui uma funcionalidade de verificação de fatos ("*Fact Check*") para as alegações presentes no texto gerado ou analisado.
Benefícios	Pode ajudar a identificar rapidamente alegações potencialmente questionáveis em textos longos durante o processo de criação ou revisão.
Restrições	Ferramenta primariamente de geração de conteúdo, não de checagem. A função de fact-checking é secundária, baseada em IA, e sua precisão/abrangência pode ser limitada. Geralmente é pago.
Aplicabilidade em órgão público	Usar com muita cautela para uma triagem inicial de alegações em documentos internos ou rascunhos. Não deve ser considerada uma ferramenta de checagem final ou definitiva.

Site

Ferramenta/Idioma	Agência Lupa/Português
Funcionalidades	Uma das principais organizações de verificação de fatos do Brasil, especializada em checar informações, combater desinformação e promover educação midiática.
Benefícios	Aumenta a transparência do discurso público. Combate a disseminação de mentiras. Promove o pensamento crítico. Oferece conteúdo verificado para o público e imprensa.
Restrições	Capacidade de checagem limitada pela equipe. Alcance pode ser menor que o da desinformação. Resistência de quem acredita na desinformação. Financiamento.
Aplicabilidade em órgão público	Reforçar a transparência institucional, a comunicação responsável e o enfrentamento à desinformação, além de apoiar a formulação de políticas e o relacionamento com a sociedade.

Ferramenta/Idioma	Aos Fatos/Português
Funcionalidades	Verificar declarações de autoridades e conteúdos virais, monitorar narrativas falsas em redes sociais, produzir reportagens investigativas sobre o ecossistema da desinformação e disponibilizar um banco de checagens acessível ao público. Além disso, oferece ferramentas automatizadas, como o robô Fátima, desenvolve ações de educação midiática e mantém parcerias com plataformas digitais para reduzir a circulação de notícias falsas.
Benefícios	Alta credibilidade. Uso de tecnologia para identificar e combater desinformação em larga escala. Investigação aprofundada de redes de desinformação.
Restrições	Similar à Lupa. Desafios de escala frente ao volume de desinformação. Ataques e tentativas de desacreditar o trabalho.
Aplicabilidade em órgão público	Similar à Lupa. Insights sobre táticas de desinformação. Possível parceria para monitoramento ou treinamento.

Ferramenta/Idioma	Fato ou Boato - Esclarecimento sobre informações falsas/Português
Funcionalidades	Foco em desinformação relacionada a eleições, urnas eletrônicas, Justiça Eleitoral e políticas públicas do Governo Federal. Esclarecimento de boatos.
Benefícios	Fonte oficial de esclarecimento sobre temas sensíveis (eleições, ações governamentais). Combate direto a boatos que afetam a administração pública e a democracia.
Restrições	Foco temático específico (eleitoral/governamental), não abrangendo todos os tipos de boatos. Pode ser percebido por alguns como tendo um viés governamental.
Aplicabilidade em órgão público	Principal referência para desmentir boatos sobre eleições e ações do governo. Usado para comunicação oficial e esclarecimento público.

Ferramenta/Idioma	Fato ou Fake (G1)/Português
Funcionalidades	Checagem de conteúdo viral (texto, imagem, vídeo) que circula em redes sociais e aplicativos de mensagens. Foco em temas de grande repercussão.
Benefícios	Grande alcance devido à plataforma G1. Linguagem acessível ao grande público. Rapidez na resposta a virais recentes.
Restrições	Pode priorizar temas de maior apelo popular em detrimento de desinformação de nicho. Dependência da estrutura do G1.
Aplicabilidade em órgão público	Referência rápida para verificar virais que impactam o público. Pode ser usado para informar comunicados internos ou públicos sobre boatos de grande alcance.

Ferramenta/Idioma	E-farsas/Português
Funcionalidades	Checagem de boatos, lendas urbanas e notícias falsas que circulam há muito tempo na internet ("arqueologia de boatos"). Foco em desmistificar farsas.
Benefícios	Foco em desbancar farsas persistentes e educar o público sobre como boatos são criados e disseminados. Tom mais informal e acessível.
Restrições	Foco em boatos mais "clássicos" ou curiosos, podendo não cobrir toda a desinformação política ou de última hora. Estrutura geralmente menor.
Aplicabilidade em órgão público	Útil para entender a longevidade de certos boatos e como eles são construídos. Material para educação midiática interna sobre identificação de farsas.

Ferramenta/Idioma	Comprova/Português
Funcionalidades	Coalizão de múltiplos veículos de imprensa para investigar e verificar informações suspeitas de grande alcance, especialmente em períodos eleitorais. Checagem colaborativa.
Benefícios	Ampla capacidade de apuração e alcance devido à união de diversos veículos. Foco em desinformação complexa e de alto impacto. Aumenta a confiança do público.
Restrições	Complexidade da coordenação entre múltiplos veículos. Foco geralmente em períodos específicos (eleições).
Aplicabilidade em órgão público	Fonte confiável para entender e combater desinformação de alto impacto, especialmente durante eleições. Pode subsidiar ações de comunicação e inteligência.

Ferramenta/Idioma	AFP Fact Check/Inglês
Funcionalidades	Checagem de informações virais (imagens, vídeos, textos) em diversos idiomas, incluindo português. Foco em desinformação com alcance internacional e nacional.
Benefícios	Perspectiva global sobre desinformação. Verificações detalhadas e bem fundamentadas. Credibilidade de uma agência de notícias internacional.
Restrições	Pode ter um foco maior em desinformação com repercussão internacional, embora atue localmente. Barreiras linguísticas podem ser um desafio em alguns contextos.
Aplicabilidade em órgão público	Fonte para verificar desinformação com origem ou paralelos internacionais. Análises podem ajudar a entender campanhas coordenadas globais. Exportar para as Planilhas

Ferramenta/Idioma	Boatos.org/Português
Funcionalidades	Verificação de boatos que circulam em redes sociais, *WhatsApp* e correntes virais; linguagem acessível e explicativa.
Benefícios	Ajuda a desmistificar rumores de grande alcance popular; linguagem simples que facilita o entendimento geral.
Restrições	Não possui caráter institucional; nem sempre apresenta fontes oficiais em profundidade.
Aplicabilidade em órgão público	Pode apoiar campanhas de esclarecimento à população sobre *fake news* comuns e recorrentes em períodos eleitorais ou de crise.

Ferramenta/Idioma	Estadão Verifica/Português
Funcionalidades	Checagem de fatos ligados a declarações de autoridades, políticos e temas de interesse público; parte do jornal Estadão.
Benefícios	Vinculado a um veículo tradicional de informação. Metodologia de checagem reconhecida.
Restrições	Pode ter limitação de acesso gratuito (*paywall* do Estadão); foco maior em política nacional.
Aplicabilidade em órgão público	Útil para conferência de declarações de autoridades e para dar suporte técnico à comunicação institucional.

Ferramenta/Idioma	UOL Confere/Português
Funcionalidades	Checagem de informações falsas em circulação, especialmente ligadas a temas de saúde, política e cotidiano; integra o portal UOL.
Benefícios	Grande alcance devido ao tráfego do UOL; boa cobertura de temas variados com impacto social direto.
Restrições	Algumas checagens podem ser resumidas; nem sempre aprofunda aspectos técnicos ou jurídicos.
Aplicabilidade em órgão público	Relevante para monitorar narrativas falsas que impactam serviços públicos e reforçar a credibilidade em comunicados oficiais.

Ferramenta/Idioma	VirusTotal/Inglês
Funcionalidades	Análise *Multi-scanner*: O *VirusTotal* utiliza dezenas de motores de antivírus e ferramentas de análise de *sites* para verificar arquivos e *URLs*. Isso fornece uma visão agregada de como diferentes soluções de segurança classificam um item. Análise de *URLs* e Domínios: Verifica se um *site* ou domínio está sinalizado como malicioso por diversas ferramentas, o que pode ajudar a identificar *sites* criados para disseminar desinformação ou aplicar golpes. Análise de Arquivos: Permite o upload de arquivos para verificar se contêm *malware*. Isso é útil caso a desinformação esteja embutida em documentos ou executáveis. Relatórios Detalhados: Fornece relatórios com os resultados de cada motor de varredura, informações sobre o arquivo ou *URL* (como *hashes*, data de criação, informações de contato do domínio, etc.) e, em alguns casos, detalhes comportamentais. Comunidade e API: Os dados submetidos ao *VirusTotal* são compartilhados com a comunidade de segurança, auxiliando na melhoria da detecção de ameaças. Sua API permite a integração com outras ferramentas e fluxos de trabalho de segurança.

Benefícios	Detecção Ampla: Ao agregar múltiplas opiniões de segurança, aumenta a chance de identificar ameaças que um único antivírus poderia não detectar. Identificação de Infraestrutura Maliciosa: Pode ajudar a identificar *sites*, domínios e arquivos usados em campanhas de desinformação que também têm componentes maliciosos (*phishing*, *malware*). Auxílio na Investigação: Fornece informações contextuais sobre URLs e arquivos que podem ser úteis para analistas investigarem a origem e a natureza de campanhas de desinformação. Gratuito e Acessível: É uma ferramenta de fácil acesso e sem custo para o usuário final. Conscientização e Prevenção: Ao verificar um *link* ou arquivo suspeito, o usuário pode evitar ser vítima de golpes ou da propagação de *malware* associado à desinformação.
Restrições	Não Analisa o Conteúdo da Desinformação: O VirusTotal não verifica a veracidade da informação em si. Seu foco é em ameaças de segurança (*malware*, *phishing*), não na análise semântica ou factual do conteúdo. Uma notícia falsa hospedada em um *site* "limpo" não será sinalizada como desinformação pelo VirusTotal. É crucial entender que o VirusTotal é uma ferramenta complementar e não uma solução definitiva para o combate à desinformação. A análise da veracidade do conteúdo em si requer outras abordagens, como checagem de fatos (*fact-checking*), análise de discurso e investigação jornalística. No entanto, ao ajudar a identificar e neutralizar os aspectos técnicos e de cibersegurança que muitas vezes acompanham as campanhas de desinformação, o VirusTotal pode ser um aliado valioso para os órgãos públicos.
Aplicabilidade em órgão público	Verificação de Fontes Suspeitas: Antes de interagir com *links* ou arquivos recebidos por e-mail, mensagens ou encontrados em redes sociais, especialmente aqueles com alegações alarmantes ou duvidosas, os funcionários públicos podem usar o *VirusTotal* para verificar se são vetores de *malware* ou *phishing*. Isso ajuda a proteger a infraestrutura do órgão e os dados dos funcionários. Análise de Campanhas de Desinformação com Componentes Maliciosos: Em investigações sobre campanhas de desinformação, o VirusTotal pode ajudar a identificar se os *sites* ou arquivos utilizados para disseminar o conteúdo falso também hospedam *malware* ou estão envolvidos em atividades de *phishing*. Isso pode fornecer informações sobre os atores por trás da campanha e seus métodos. Treinamento e Conscientização: Órgãos públicos podem incluir o uso do VirusTotal em treinamentos de segurança da informação e conscientização sobre desinformação, ensinando os servidores a verificar links e arquivos suspeitos como uma prática de higiene digital. Apoio a Equipes de Resposta a Incidentes: Em caso de um incidente de segurança que possa estar relacionado à desinformação (por exemplo, um e-mail de *phishing* contendo um *link* para uma notícia falsa que instala *malware*), o *VirusTotal* pode fornecer informações rápidas para a equipe de resposta. Monitoramento de Domínios e *IPs* Relevantes: Embora não seja sua função primária, é possível monitorar a reputação de domínios e IPs associados a campanhas de desinformação conhecidas, caso haja suspeita de que possam ser usados para atividades maliciosas.

Ferramenta/Idioma	Wayback Machine/Inglês
Funcionalidades	Arquivamento de Páginas da *Web*: A Wayback Machine rastreia e armazena "*snapshots*" (cópias instantâneas) de *websites* em diferentes momentos. Navegação por Histórico: Permite aos usuários inserir um *URL* e visualizar um calendário com as datas em que aquele *site* foi arquivado. Ao selecionar uma data, o usuário pode ver como a página se apresentava naquele momento. Preservação de Conteúdo: Disponibiliza acesso a *websites* ou páginas que foram removidos da *web* ou cujo conteúdo foi significativamente alterado. Funcionalidade "*Save Page Now*": Permite que qualquer usuário solicite o arquivamento de uma página específica, criando um registro daquele conteúdo em um determinado momento.
Benefícios	Verificação de Alterações de Conteúdo: É possível comparar a versão atual de uma página com versões anteriores para identificar se informações foram adicionadas, removidas ou alteradas. Isso é crucial para detectar manipulações ou negações posteriores de declarações. Recuperação de Informações Removidas: Se uma notícia, postagem ou documento contendo desinformação for apagado, a *Wayback Machine* pode ter uma cópia arquivada, permitindo que o conteúdo original seja recuperado e analisado. Contextualização Histórica: Ajuda a entender a evolução de narrativas e como determinadas informações (ou desinformações) foram apresentadas ao longo do tempo por um *site* específico. Identificação da Origem de Desinformação: Ao rastrear o histórico de um *site*, pode-se, em alguns casos, identificar quando uma peça de desinformação apareceu pela primeira vez ou como ela foi modificada. Acesso a Fontes Indisponíveis: Permite o acesso a informações de *sites* que foram desativados, o que pode ser útil em investigações. Transparência e Responsabilização: A existência de um arquivo público pode incentivar maior responsabilidade por parte dos publicadores de conteúdo, sabendo que suas publicações podem ser preservadas.
Restrições	Não Garante Autenticidade Absoluta para Fins Legais (sem medidas adicionais): Embora útil, um simples "*print screen*" de uma página arquivada pode não ser suficiente como prova irrefutável em um contexto legal sem o uso de ferramentas adicionais de certificação digital para garantir a integridade da captura.Possibilidade de Exclusão: Proprietários de *sites* podem solicitar a exclusão de seus arquivos da *Wayback Machine*, embora o processo possa ser complexo. Cobertura Incompleta: Nem todos os *sites* da internet são arquivados, e nem todas as páginas de um *site* são capturadas. *Sites* com restrições de rastreamento (*robots.txt*) ou conteúdo dinâmico complexo podem não ser bem arquivados.

Aplicabilidade em órgão público	Monitoramento e Análise de Narrativas: Verificar como informações em *sites* de interesse (incluindo os de fontes potencialmente hostis ou de disseminação de desinformação) evoluem, são alteradas ou removidas. Isso ajuda a entender táticas de manipulação informativa. Investigação de Campanhas de Desinformação: Rastrear a origem e as modificações de conteúdo falso. Se um *site* publica uma informação e depois a altera ou apaga para encobrir rastros, a *Wayback Machine* pode revelar o conteúdo original. Coleta de Evidências: Embora com as ressalvas legais mencionadas, páginas arquivadas podem servir como ponto de partida ou evidência contextual em investigações sobre a disseminação de notícias falsas, discursos de ódio ou outras formas de desinformação. Verificação de Declarações Públicas: Confrontar declarações atuais de figuras públicas ou organizações com o que foi publicado anteriormente em seus próprios *sites*, caso haja suspeita de contradição ou negação. Preservação de Conteúdo Relevante: Órgãos públicos podem usar a função "*Save Page Now*" para garantir que páginas de interesse (por exemplo, uma página contendo uma ameaça ou desinformação flagrante) sejam arquivadas antes que possam ser removidas. Apoio a Ações de Transparência: Utilizar o arquivo para demonstrar como informações oficiais foram comunicadas em diferentes momentos, caso haja questionamentos sobre a consistência da comunicação do próprio órgão. Produção de Relatórios e Análises: Incluir links para versões arquivadas em relatórios de inteligência ou análises sobre desinformação para fundamentar as conclusões sobre a evolução de certas narrativas.

Ferramenta/Idioma	Who.is/Inglês
Funcionalidades	Consulta de informações de registro de domínio (WHOIS), incluindo dados da pessoa que registrou (nome, organização, contato), datas de criação e expiração do domínio e servidores DNS.
Benefícios	Gratuito, fornece informações essenciais para identificar a propriedade de um *site*, auxiliar em investigações de fraude ou *phishing*, e verificar a legitimidade de entidades *online*.
Restrições	Os dados WHOIS podem ser ocultados por serviços de privacidade, tornando a identificação mais difícil. As informações podem estar desatualizadas.
Aplicabilidade em órgão público	Auxilia equipes de investigação cibernética, segurança da informação e jurídica. Pode ser usado para identificar responsáveis por *sites* maliciosos, coletar evidências em casos de crimes cibernéticos ou verificar a autenticidade de organizações *online*.

Ferramenta/Idioma	Sistema de Alertas de Desinformação Eleitoral - SIADE/Português
Funcionalidades	Permite a qualquer pessoa o apontamento de fatos notoriamente inverídicos ou descontextualizados com potencial para causar danos ao equilíbrio do pleito ou à integridade do processo eleitoral. Emissão de alertas a plataformas digitais e agências de checagem para pronta atuação na remoção ou rotulagem de conteúdo; centralização de denúncias de desinformação eleitoral recebidas da sociedade.

Benefícios	Combate proativo à disseminação de notícias falsas e desinformação durante o período eleitoral; agilidade na identificação e notificação de conteúdos problemáticos; fortalecimento da integridade do processo eleitoral; promoção de um ambiente informacional mais saudável para o eleitor; acessível publicamente via portal do Tribunal Superior Eleitoral (TSE).
Restrições	Dependência da colaboração das plataformas digitais para a efetiva remoção ou sinalização do conteúdo; volume massivo de informações a serem processadas pode dificultar a identificação de todos os focos de desinformação; eficácia limitada em ambientes fechados (grupos de mensagens privados, por exemplo); não impede a criação ou circulação inicial de desinformação.
Aplicabilidade em órgão público	Essencial para órgãos da Justiça Eleitoral no monitoramento e combate à desinformação que possa comprometer a lisura do processo eleitoral. Pode ser utilizado por equipes de comunicação, assessoria de imprensa e áreas de segurança institucional para acompanhar e responder a narrativas desinformativas.

Ferramenta/Idioma	Registro.BR/Português
Funcionalidades	**#1)** Who.is: consulta de titularidade (nome e CPF/CNPJ). Verificação dos contatos (técnico, administrativo). Informações sobre os servidores DNS associados ao domínio. Datas de criação e expiração do registro. **#2)** Verificação de DNS e DNSSEC: analisa a configuração dos servidores DNS de um domínio, apontando erros e inconsistências que possam afetar a disponibilidade do *site*. O DNSSEC (*DNS Security Extensions*) é uma tecnologia que garante a autenticidade e a integridade dos dados do DNS, prevenindo ataques de envenenamento de cache e redirecionamento de tráfego. A ferramenta do REGISTRO.br auxilia na sua implementação. **#3)** Traceroute: permite rastrear a rota que os pacotes de dados percorrem desde o servidor do REGISTRO.br até o servidor que hospeda o *site* do órgão público. Se um serviço *online* do governo está lento ou inacessível, o Traceroute ajuda a identificar em que ponto da rede (se no provedor do órgão, em um *link* de comunicação, etc.) está o gargalo ou a falha.
Benefícios	Credibilidade e Confiança: Um domínio .gov.br ou de outra categoria governamental assegura ao cidadão que ele está acessando um canal oficial, combatendo a desinformação e o *phishing*. Identidade Nacional: Reforça a soberania digital e a localização da entidade governamental no Brasil. Segurança Jurídica: O registro no REGISTRO.br, seguindo suas políticas, oferece respaldo e clareza sobre a titularidade do domínio.
Restrições	O âmbito da pesquisa limita-se aos nomes de domínio ".br". Algumas das ferramentas exigem conhecimento técnico especializado para a interpretação dos resultados.
Aplicabilidade em órgão público	Verificação de Autenticidade: Permite a outros entes públicos e à sociedade em geral verificar a legitimidade de um *site* que se apresenta como governamental. Inteligência e Segurança: Órgãos de segurança e fiscalização podem utilizar o *Whois* para identificar os responsáveis por *sites* que cometem irregularidades ou crimes cibernéticos. Gestão Interna: Facilita a gestão de múltiplos domínios de um mesmo órgão ou de uma esfera de governo, centralizando a informação de contato e titularidade.

Áudio

Ferramenta/Idioma	Hiya - Detector de Voz *Deepfake*/Inglês
Funcionalidades	Analisa gravações de áudio para identificar a presença de vozes sintéticas ou geradas por inteligência artificial (*deepfakes*). A ferramenta é capaz de distinguir entre vozes humanas reais e áudio manipulado, buscando por anomalias e padrões característicos de criações artificiais.
Benefícios	Ajuda a verificar a autenticidade de chamadas telefônicas e outras interações de voz, alertando os usuários sobre possíveis tentativas de golpes ou manipulação. Sua integração com plataformas de comunicação o torna uma ferramenta proativa na defesa contra o uso malicioso de *deepfakes* de voz.
Restrições	Pode ocasionalmente gerar falsos positivos (identificar uma voz real como *deepfake*) ou falsos negativos (não detectar um *deepfake* real), especialmente com a evolução constante das tecnologias de síntese de voz. A precisão pode ser influenciada pela qualidade do áudio analisado. Além disso, a ferramenta foca exclusivamente na detecção de *deepfakes* de voz, não abordando outras formas de manipulação de mídia.
Aplicabilidade em órgão público	Pode ser utilizado para verificar a autenticidade de gravações de áudio em investigações, para validar a identidade de quem telefona em situações sensíveis, ou para analisar comunicações suspeitas e identificar a disseminação de desinformação por áudio.

ANEXO II

ANEXO II

Tecnologia TPM nos computadores da Justiça Eleitoral

O TPM (*Trusted Platform Module*) é um *chip* processador de criptografia que fica integrado à placa-mãe de computadores, *tablets* e celulares. É, portanto, um mecanismo de segurança baseado em *hardware*.

O *chip* TPM executa operações criptográficas e inclui vários mecanismos de segurança física para torná-lo resistente a violações, de modo que um *software* mal-intencionado não possa rompê-lo. Algumas das principais vantagens do uso da tecnologia TPM são a possibilidade de:

- Gerar, armazenar e limitar o uso de chaves de criptografia.
- Autentificar um dispositivo de plataforma usando a chave RSA exclusiva do TPM, que está nele gravada (RSA é um sistema criptográfico em que a chave de encriptação é pública e é diferente da chave de descriptação, que é secreta/privada).
- Ajudar a garantir a integridade da plataforma, executando e armazenando medidas de segurança.

A Justiça Eleitoral usa o TPM em seus computadores para a segurança do GEDAI e de demais aplicativos *desktop* desenvolvidos pelo TSE, guardando nele suas chaves privadas.

Quando a JE começou a usar o TPM?

"As principais evoluções feitas após o TPS 2019 foram o fortalecimento da proteção da chave do SIS e o uso do processador de segurança TPM, presente nas estações de trabalho da Justiça Eleitoral, para fazer a proteção do Gedai-UE e das chaves por ele utilizadas.

Essas evoluções impedem qualquer tentativa de controle indevido do Gedai-UE e geração de configurações manipuladas para a urna."

Fonte: TSE.

CriptoSevin

Trata-se de um *driver* de segurança que verifica os parâmetros dos sistemas produzidos pela Seção de Voto Informatizado do TSE (SEVIN), a fim de verificar se houve alguma alteração que os afete.

O CriptoSevin utiliza informações do sistema operacional para a composição de elementos que serão criptografados pelo *chip* TPM.

Holocron

É o serviço responsável pela guarda das chaves de assinatura, criptografia e MAC utilizadas pelos aplicativos. Ele protege as chaves, criando, com o auxílio do CriptoSevin, chaveiros durante o seu processo de instalação.

Todas as operações de assinatura, criptografia e MAC que as aplicações necessitam são feitas pelo Holocron. Após instalado, o serviço é iniciado automaticamente durante a inicialização do *Windows*.

O Holocron e o CriptoSevin são instalados pelos cartórios eleitorais juntamente com o GEDAI.

O que é MAC?

O endereço MAC (*Media Access Control* ou Controle de Acesso de Mídia) é um endereço físico e único, que é associado às interfaces de comunicação utilizadas em dispositivos de rede.

A identificação é gravada em *hardware* por fabricantes de placa de rede, tornando-se, posteriormente, parte de computadores, roteadores, *smartphones*, *tablets*, impressoras e diversos outros equipamentos que usam comunicação em rede.

Fonte: Techtudo.


Justiça
Eleitoral