

Relatório técnico de auditoria eleitoral

Endor Tecnologia

Identificador: audit-20261026T222836Z-eda682484006

Escopo: {"election":"6258","uf":"","municipality":"","section_id":"5625"}

Corte UTC: 2026-10-26T22:28:58+00:00

Geração UTC: 2026-10-26T22:28:58+00:00

Responsabilidade: geração automática pelo sistema; revisão e assinatura de perito pendentes.

1. Objeto e quesitos

Reproduzir a leitura dos arquivos oficiais preservados no escopo, conferir sua integridade, identidade, aritmética e projeção no índice e explicar a soma parcial.

1. Os bytes observados correspondem aos registros da captura e aos inventários VSC?
2. A identificação e as igualdades aritméticas dos BUs conferem?
3. O índice e a soma podem ser reproduzidos a partir desses originais?
4. Quais divergências foram demonstradas e quais verificações permanecem pendentes?

2. Cobertura e regras de inclusão

Estado no corte	Seções
succeeded	1

Casos relidos: 1. BUs incluídos: 1. Inventário completo do escopo: inventario.csv. Casos e decisões: casos.jsonl e observacoes.jsonl.

Apuração parcial. O relatório não declara concluída a auditoria da totalização oficial. Cobertura incompleta e universos ainda não reconciliados impedem concluir uma divergência nacional por simples subtração dos totais.

3. Métodos empregados

Conciliação cadastral separada: o CSV TSE de locais de votação gerado em 25/10/2026 contém 517.179 seções únicas em cada turno, coincidindo com o cadastro EA16 importado: 499.248 principais e 17.931 agregadas. A notícia preparatória de 04/09 informa 517.206; a origem histórica dos 27 de diferença permanece pendente de comprovação. Fontes e teste: <https://eleicoes.endortecnologia.com/conciliacao-secoes> . No pacote nacional, descompacte conferencia-cadastro.zip e execute python3 verificar_cadastro.py (Python 3.11 ou posterior). A conciliação do cadastro não equivale à validação dos votos.

3.1. Delimitação e corte

Eleição, cargo e território explícitos. A API de backup do SQLite produz uma cópia transacional do índice; o cadastro, os estados e os valores são exportados dessa cópia, sem manter uma leitura longa no banco de produção. As fontes oficiais têm suas próprias datas de captura e geração, preservadas separadamente.

3.2. Captura

Catálogos e auxiliar EA18 resolvem os endereços no domínio resultados.tse.jus.br. O coletor usa HTTPS com validação TLS, sem redirecionamentos, e preserva corpo da resposta, URL, horário UTC, cabeçalhos e status HTTP. A auditoria do relatório não faz novo download.

3.3. Preservação

Os corpos recebidos são armazenados por SHA-256 fora da raiz pública. Manifestos registram tamanho e proveniência. O relatório copia os bytes observados para um pacote fixo e recalcula os hashes dessa cópia antes da interpretação. Isso documenta a custódia local; não constitui carimbo de tempo independente.

3.4. Descompactação e decodificação

Os BUs .dat examinados não são ZIP. Não há descompactação do BU: o leitor decodifica ASN.1 de comprimento definido e extrai o OCTET STRING do envelope. No VSC, extrai os OCTET STRING dos inventários. A trilha registra tamanho e SHA-256 das entradas e saídas dessas extrações. Logs .jez, RDVs e arquivos comprimidos não integrados ao método não são declarados analisados.

3.5. Comparação de hashes

Primeiro, SHA-256 e tamanho observados são comparados ao manifesto da captura. Depois, SHA-512 e tamanho do BU inteiro são comparados ao arquivo de mesmo nome nos inventários de software e hardware do VSC. O tamanho e o SHA-512 de cada inventário também são conferidos. O hash do EA18 é identificador da pasta de publicação e não é usado como digest do BU.

3.6. Extração e identidade

O mapeamento ASN.1 preservado do aplicativo TSE define os campos. Seleciona-se unicamente a eleição solicitada e o cargo Presidente. Pleito, eleição, município, zona e seção devem corresponder ao cadastro e às URLs. Tipos desconhecidos ou ambíguos interrompem a liberação do caso.

3.7. Aritmética e somatório

Soma de votos nominais, brancos e nulos deve corresponder ao comparecimento do cargo e do BU; comparecimento não pode superar aptos; aptos da seção mais temporários devem corresponder ao total. Quando disponível, a soma das três habilitações deve corresponder ao comparecimento. A soma do relatório usa inteiros, uma única ocorrência por eleição/UF/município/zona/seção, estado sucedido no corte e releitura verificada. Agregadas, pendentes e revisões não são somadas. Percentual de candidatura = votos nominais da candidatura / votos nominais incluídos × 100.

3.8. Conferência do índice

Os valores extraídos novamente dos originais são comparados aos votos, aptos, comparecimento e habilitações que estavam no banco no corte. Divergência dessa projeção é achado sobre o nosso índice, sem atribuição automática ao TSE.

3.9. Achados e conclusão

Cada achado informa regra, esperado, observado, seção e evidências. Divergências reproduzidas, impedimentos e limitações são classificados separadamente. Cobertura parcial não é subtraída de total nacional completo para alegar erro. A conciliação conclusiva dos totais oficiais permanece pendente enquanto o universo e as regras eleitorais

aplicáveis não forem reconciliados.

3.10. Reprodução

O ZIP reúne originais observados, manifestos, cadastro do corte, índice, resultados, metodologia, código do verificador utilizado e SHA256SUMS. `php reproduzir.php` confere o pacote, repete as verificações sem rede e exige resultados idênticos aos publicados no relatório. `python3 conferir_votos.py` usa outra implementação para conferir independentemente o núcleo numérico ASN.1/BU/VSC, sem importar código PHP. O PDF é uma representação do mesmo conjunto fixo.

Função de cada tipo de arquivo

Catálogo de eleições e diretórios oficiais (catalog)

Formato: JSON · `ele-c.json`

Identifica ciclo, pleito, eleição e turno e fornece os modelos de endereços dos arquivos. É o ponto inicial para resolver as URLs oficiais. Não fornece votos para a soma.

Cadastro oficial de seções — EA16 (sections)

Formato: JSON · `*-cs.json`

Lista município, zona e seção; informa vínculos entre principais e agregadas e data/hora do auxiliar quando disponíveis. Delimita o universo e evita duplicar votos de agregadas. Não substitui o BU nem comprova, sozinho, que a seção foi instalada.

Auxiliar da seção — EA18 (auxiliary)

Formato: JSON · `*-aux.json`

Informa a situação da seção e as versões recebidas, seus nomes de arquivos e o identificador da pasta de publicação. Seleccionamos uma versão unicamente totalizada. Esse identificador chamado hash não é o SHA-256 ou SHA-512 do BU.

Boletim de Urna — BU (ballot)

Formato: Binário ASN.1 · `*-bu.dat`

É a fonte dos votos da nossa reconstrução. Contém identificação eleitoral, aptos, comparecimento, resultados por cargo/candidatura e habilitações quando presentes. O arquivo inteiro é conferido antes de extrair seu conteúdo. A soma não usa votos do EA20.

VSC — inventários e assinaturas da urna (signature)

Formato: Binário ASN.1 · `*-vota.vsc`

Contém os inventários de software e hardware com nomes de arquivos, tamanhos e resumos esperados, além de estruturas de assinatura. Confrontamos o BU com esses inventários e conferimos os resumos dos próprios inventários. A autenticação das assinaturas e da cadeia de confiança continua pendente.

Resultado oficial consolidado do município — EA20 (municipal_result)

Formato: JSON · município/cargo/eleição

Preserva a referência oficial municipal e seu momento de geração para futura conciliação de universos completos. Não gera nem corrige os votos extraídos dos BUs. Um consolidado completo e uma coleta parcial não são subtraídos para alegar divergência.

Resultado oficial consolidado nacional — EA20 (national_result)

Formato: JSON · Brasil/cargo/eleição

Fornece a referência nacional e os denominadores de cobertura apresentados separadamente no painel. A nossa soma continua baseada nos BUs únicos e conferidos.

4. Resultados reconstruídos dos BUs

Candidatura (número)	Votos	% dos nominais incluídos
13	172	61,209964%
22	109	38,790036%

Categoria	Quantidade
Nominais	281
Branco	7
Nulos	2
Comparecimento	290
Aptos nas seções incluídas	344
BUs com habilitações conhecidas	1
Habilitação biométrica	269
Habilitação biográfica	21
Habilitação sem biometria	0

Habilitações são contagens de eleitores; não permitem atribuir escolhas a candidatos. Contagens ausentes não foram convertidas em zero na cobertura conhecida.

Soma do índice igual à reconstrução dos originais: Sim, neste corte.

Soma independente do índice no mesmo corte

```
{
  "ballots": 1,
  "nominal": 281,
  "blank": 7,
  "null": 2,
  "turnout": 290,
  "eligible": 344,
  "candidates": {
    "13": 172,
    "22": 109
  }
}
```

```

},
"identification": {
  "covered_ballots": 1,
  "covered_turnout": 290,
  "biometric": 269,
  "biographic": 21,
  "without_biometrics": 0
}
}

```

5. Achados, comprovação e resposta aos quesitos

Classificação	Ocorrências
confirmed	0
pending	0
limitation	0

Divergências comprovadas: a regra e os valores esperado/observado constam de achados.jsonl e dos volumes PDF de achados. Impedimentos e limitações não são convertidos em divergências de hash.

Estados da releitura: {"verified":1}. Falhas de captura de evidências no pacote: 0.

Conferência da totalização oficial: pendente. Autoria, causa e intenção de eventuais achados: não determinadas por este procedimento.

6. Evidências e reprodução

O pacote ZIP contém os originais observados em objects/, manifestos em runs/, cadastro e índice do corte, histórico, trilhas de extração e o código utilizado em lib/.

Relação completa de BUS analisados: bus-analisados.csv, com 1 arquivos. Lista seção, URL original e consulta no TSE, URL do VSC, hashes, tamanho e inclusão na soma. Download direto:

<https://eleicoes.endortecnologia.com/auditorias/audit-20261026T222836Z-e-da682484006/baixar/bus-analisados.csv>

SHA-256 dessa lista:

```

0823fb2fa5557637b14a824266b1d996
922b6a61353e2b5ac9f765a9a2f2b029

```

1. Descompacte o pacote em uma pasta nova. 2. Use PHP CLI 8.2 ou posterior, com JSON e hash. 3. Execute php reproduzir.php. O verificador não usa rede nem Composer e exige igualdade dos resultados e dos hashes do pacote.

Conferência por outra implementação: execute python3 conferir_votos.py com Python 3.11 ou posterior. O programa lê ASN.1/BU/VSC e soma novamente os votos sem importar código PHP.

SHA-256 de observacoes.jsonl:

```

d4aa565302c53ec6f3c92095815ff015
230133825d4e0505fe4c94bc3b4ddfb6

```

Os resumos dos PDFs, dados, código e originais estão em SHA256SUMS. Conserve o hash do pacote baixado em meio independente. O PDF não é assinado digitalmente.

7. Versões e ambiente

```
{
  "application": "eleicoes-audit-0.4",
  "reader": "tse-bu-2026-president-v4",
  "method": "endor-audit-method-1",
  "php": "8.3.6",
  "os_family": "Linux",
  "openssl": "OpenSSL 3.0.13 30 Jan 2024",
  "curl": "8.5.0",
  "dompdf": "v3.1.6"
}
```

8. Limitações

- Documento técnico automático para instrução e revisão pericial; não contém assinatura de perito nem decisão sobre admissibilidade jurídica.
- Assinaturas criptográficas, cadeia de certificação e carimbo de tempo independente pendentes. Hash coincidente não autentica sozinho a origem.
- O conjunto analisado contém apenas os arquivos e versões selecionados no corte. Uma publicação posterior do TSE pode ser diferente.
- Tipos raros possuem cobertura estrutural por testes sintéticos; amostras reais e esquemas VSC adicionais continuam sujeitos à matriz de compatibilidade.
- Ausência de achados neste escopo não comprova ausência de irregularidades em toda a eleição. Achados técnicos não determinam autoria, intenção ou fraude.

9. Exemplos de rastreabilidade das fontes

Seção ID 5625 — JOÃO PESSOA / PB — zona 0077, seção 0416

Manifesto: recheck-20261026T195503Z-815ba91cdcd6.json

SHA-256: d474b3fb1976c103e7774ea6d1c96de0

ac7638a581290ddb9067668c6c941f19

Catálogo de eleições e diretórios oficiais (catalog)

Identifica ciclo, pleito, eleição e turno e fornece os modelos de endereços dos arquivos. É o ponto inicial para resolver as URLs oficiais. Não fornece votos para a soma.

HTTP 200 · 26574 bytes · Captura UTC: 2026-10-26T18:26:20+00:00

<https://resultados.tse.jus.br/oficial/comum/config/ele-c.json>

SHA-256 do arquivo original:

91d1c4fe50dbe92067b83677d77a4f18

56f5deca69a04b013a679ff690791721

Cadastro oficial de seções — EA16 (sections)

Lista município, zona e seção; informa vínculos entre principais e agregadas e data/hora do auxiliar quando disponíveis. Delimita o universo e evita duplicar votos de agregadas. Não substitui o BU nem comprova, sozinho, que a seção foi instalada.

HTTP 200 · 670012 bytes · Captura UTC: 2026-10-26T18:26:20+00:00

<https://resultados.tse.jus.br/oficial/ele2026/arquivo-urna/3221/config/pb/pb-p003221-cs.json>

SHA-256 do arquivo original:

3f22a0f5cfc1980eece5c2c4368c16bc
dcb63bddf1bf0a72cdeb37ab0cba6d4

Auxiliar da seção — EA18 (auxiliary)

Informa a situação da seção e as versões recebidas, seus nomes de arquivos e o identificador da pasta de publicação. Selecionamos uma versão unicamente totalizada. Esse identificador chamado hash não é o SHA-256 ou SHA-512 do BU.

HTTP 200 · 524 bytes · Captura UTC: 2026-10-26T19:36:07+00:00

<https://resultados.tse.jus.br/oficial/ele2026/arquivo-urna/3221/dados/pb/20516/0077/0416/p003221-pb-m20516-z0077-s0416-aux.json>

SHA-256 do arquivo original:

2367598589ae4cb991524861494e2196
ce8d0d7c00b57ffb5a1e30726ac48f31

Boletim de Urna — BU (ballot)

É a fonte dos votos da nossa reconstrução. Contém identificação eleitoral, aptos, comparecimento, resultados por cargo/candidatura e habilitações quando presentes. O arquivo inteiro é conferido antes de extrair seu conteúdo. A soma não usa votos do EA20.

HTTP 200 · 969 bytes · Captura UTC: 2026-10-26T19:36:07+00:00

<https://resultados.tse.jus.br/oficial/ele2026/arquivo-urna/3221/dados/pb/20516/0077/0416/485276446d30373773565656a477870415a506d6c707755772d4b4f6a514b505161314b4430477553314d3d/o03221pb2051600770416-bu.dat>

SHA-256 do arquivo original:

3efd06ab374ad04707c94fff031b6407
b362efbc3e3d41ea379d3613b431ad3c

VSC — inventários e assinaturas da urna (signature)

Contém os inventários de software e hardware com nomes de arquivos, tamanhos e resumos esperados, além de estruturas de assinatura. Confrontamos o BU com esses inventários e conferimos os resumos dos próprios inventários. A autenticação das assinaturas e da cadeia de confiança continua pendente.

HTTP 200 · 62611 bytes · Captura UTC: 2026-10-26T19:36:08+00:00

<https://resultados.tse.jus.br/oficial/ele2026/arquivo-urna/3221/dados/pb/20516/0077/0416/485276446d30373773565656a477870415a506d6c707755772d4b4f6a514b505161314b4430477553314d3d/o03221pb2051600770416-vota.vsc>

SHA-256 do arquivo original:

1d1bc39b4efbc3979e8c6c690193e696
9c14c3f28e8d028f41ad4a0f41ae4b53

Resultado oficial consolidado do município — EA20 (municipal_result)

Preserva a referência oficial municipal e seu momento de geração para futura conciliação de universos completos. Não gera nem corrige os votos extraídos dos BUs. Um consolidado completo e uma coleta parcial não são subtraídos para alegar divergência.

HTTP 200 · 3149 bytes · Captura UTC: 2026-10-26T19:26:25+00:00

<https://resultados.tse.jus.br/oficial/ele2026/6258/dados/pb/pb20516-c0001-e006258-u.json>

SHA-256 do arquivo original:

1a2e97689ac294813fa93b97664a82f0
4a2de3f3472481b9ed9402559bee879e

Extração: envelope.conteudo · 969 → 913 bytes.

Conteúdo ASN.1 do BU extraído do OCTET STRING do envelope. É esse conteúdo que fornece os campos de votos. Não é descompactação ZIP; a comparação oficial continua usando o BU inteiro, antes da extração.

SHA-256 da saída (rastreabilidade da extração):

bf599b321d0f2fdd9ecdb5aaea3b1fd4
6a9a61356b7204bbf9bfcfbf33ee4973b

Extração: software.inventario · 62611 → 53684 bytes.

Inventário de arquivos do componente de software no VSC, extraído de um OCTET STRING. O nome, tamanho e SHA-512 esperado do BU são consultados aqui.

SHA-256 da saída (rastreabilidade da extração):

02c6abc33d02aa430dc3b2f7541a68cd
6f2115e1ee205952cd1a69a7f491613f

Extração: hardware.inventario · 62611 → 2765 bytes.

Inventário de arquivos do componente de hardware no VSC, extraído separadamente. O BU é confrontado também com essa segunda relação.

SHA-256 da saída (rastreabilidade da extração):

cf1548a77c9fa822f3728ad13114e4db
ce388b0c0a9effa684d06e5e9b6a1b42

O pacote contém todas as fontes e decisões do escopo, não apenas estes exemplos.

10. Referências

Mapeamento do aplicativo TSE

<https://resultados.tse.jus.br/oficial/app/369.6fe9ea7d0c64a0e8.js>

Documentação técnica de arquivos de urna — TSE

<https://www.tse.jus.br/eleicoes/eleicoes-2026/eleicoes-2026>

CPC, art. 473 — objeto, análise, método e respostas aos quesitos

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm#art473

CPP, arts. 158-A e seguintes — referência para rastreabilidade da custódia

https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm#art158a