CONSELHO FEDERAL DE ENFERMAGEM – COFEN

RELATÓRIO DE CONFORMIDADE DO SISTEMA ELEITORAL

RELATÓRIO DE CONFORMIDADE DO SISTEMA DE ELEIÇÃO

Cachoeirinha, 16 de agosto de 2023.

RESP 0055/2023

Ao
CONSELHO FEDERAL DE ENFERMAGEM – COFEN

Em agosto de 2023, acompanhamos a realização da prova de conceito do sistema informatizado a ser utilizado no processo de eleição dos membros do Conselho Federal de Enfermagem – COFEN.

Para a referida prova, utilizamos de técnicas de auditoria de sistemas, cujos aspectos relevantes estão expostos neste relatório, que é estritamente confidencial, e tem por finalidade o atendimento ao contrato referente ao Pregão Eletrônico nº **PREGÃO ELETRÔNICO Nº 14/2023,** datado de 13 de abril de 2023

Apresentamos a seguir, os resultados de nossos trabalhos e as recomendações aplicáveis para apreciação de V.S.as.

Permanecemos à disposição de V.S.as para quaisquer esclarecimentos adicionais julgados necessários.

MACIEL ASSESSORES S/S LTDA
CRC RS-007503/O-8

ANDRE HENRIQUE DE OLIVEIRA GASPAR:01015724922

Assinado de forma digital por ANDRE HENRIQUE DE OLIVEIRA GASPAR:01015724922
Dados: 2023.08.28 16:48:24 -03'00'

André Henrique de Oliveira Gaspar
Contador CRC RS 103562/O-6
Sócio Responsável Técnico

SUMÁRIO

1. OBJETIVO

O objetivo do presente documento é apresentar os resultados e conclusões da verificação de conformidade realizada no sistema de eleições desenvolvido pela empresa Webvoto Tecnologia Em Eleições LTDA, sediada em Asa Norte CLN 110 BL A Sala 203 - A - Asa Norte, Brasília - DF, 70753-510, 2ª colocada no **PREGÃO ELETRÔNICO Nº 14/2023.**

2. ESCOPO

Abranger o disposto no item "**2.1. Demonstração prática das funcionalidades previstas por meio de procedimento automatizado."** do TERMO DE REFERÊNCIA, ANEXO B, do **PREGÃO ELETRÔNICO Nº 14/2023,** datado de 13 de abril de 2023, validando assim a prova de conceito com a sistemática proposta para a eleição da Diretoria e o Delegado Regional e seu suplente do Conselho Federal de Enfermagem – COFEN.

3. METODOLOGIA

Os procedimentos de auditoria contemplaram a verificação dos aspectos relativos à aderência do sistema informatizado ao disposto na RESOLUÇÃO COFEN N 695/2022, bem como no item 2.1 do **PREGÃO ELETRÔNICO Nº 14/2023,** cujo objeto é a "Contratação de empresas especializadas na prestação de serviços de auditoria de eleição a ser realizada via internet".

4. CONCEITUAÇÃO

4.1. OBJETO

O objeto das eleições do COFEN tem fé de eleger seus representantes para os mandatos de Conselheiros Regionais e seus respectivos Suplentes;

4.2. PROCESSO ELEITORAL

As eleições serão realizadas por meio eletrônico, via internet, nos termos do art. 45º do Código Eleitoral dos Conselhos Federal e Regionais de Enfermagem – Resolução Cofen nº 695/2022, bem como com suas possíveis alterações e edições até as datas dos pleitos.

Conforme Código Eleitoral dos Conselhos Federal e Regionais de Enfermagem – Resolução Cofen nº 695/2022, Decisão Cofen nº 184/2022, e possíveis alterações e edições até a data do pleito, as eleições para os Conselhos Regionais de Enfermagem ocorrerão das 08h00min do dia 1º de outubro de 2023 e se encerrarão às 08h00min do dia 2 de outubro de 2023, referente ao mandato do triênio 2024/2026;

5. ANÁLISE DE CONFORMIDADE

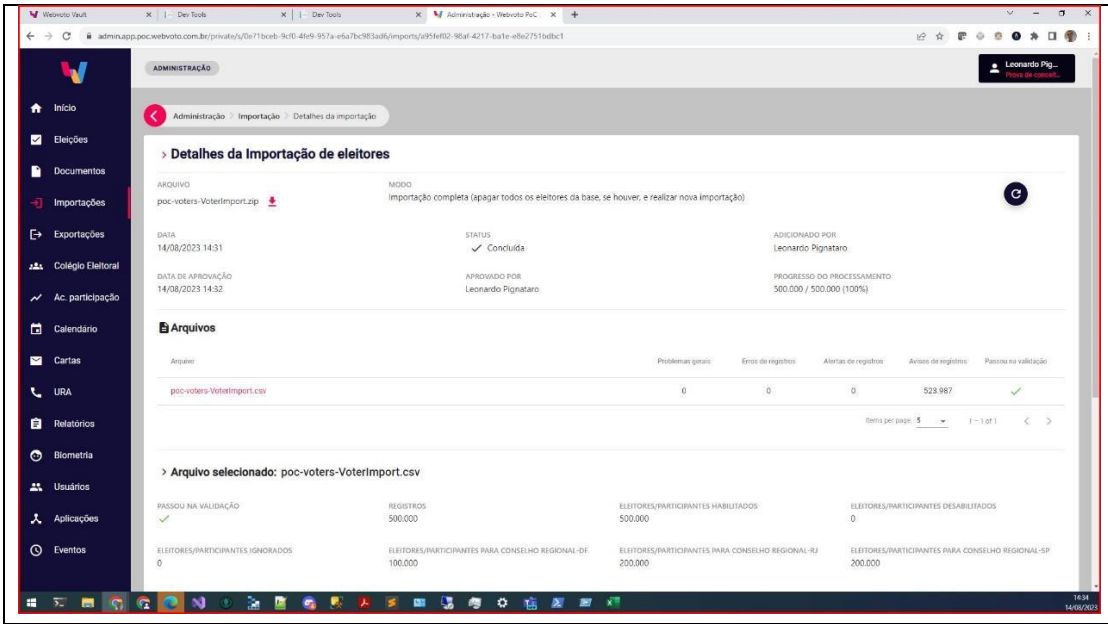
5.1. EVIDÊNCIAS

A Webvoto Tecnologia Em Eleições LTDA disponibilizou, para esta auditoria, a URL https://privapp.poc.webvoto.com.br para simulação de votação seguindo as solicitações dispostas no item bem como no item 2.1 do Anexo B, do **PREGÃO ELETRÔNICO Nº 14/2023.**

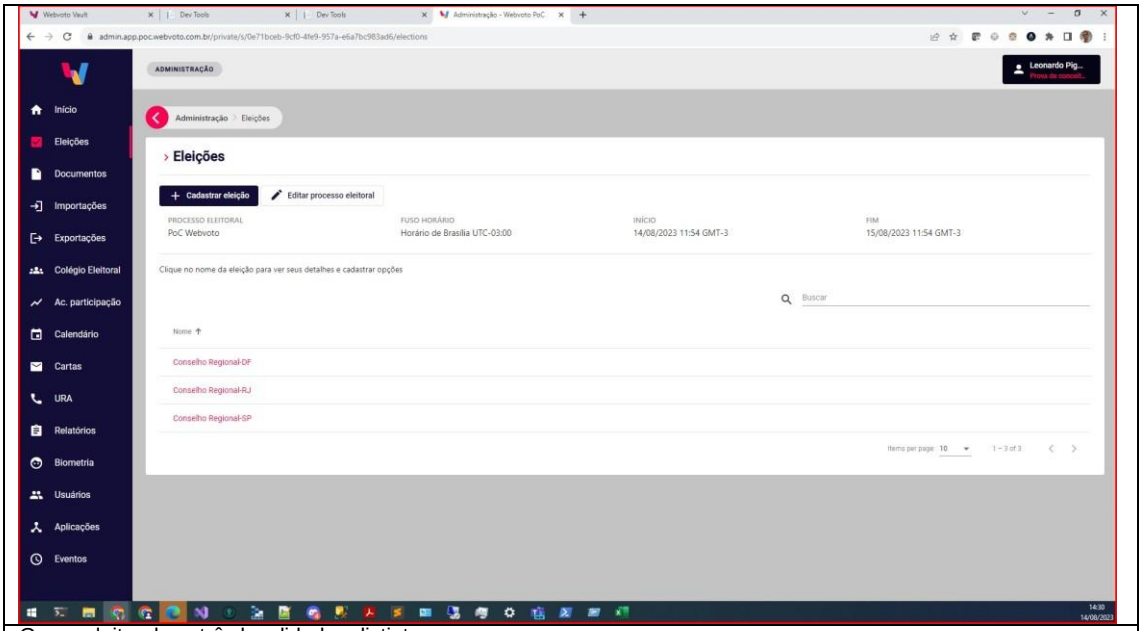
Abaixo iremos evidenciar os pontos solicitados pela prova conceito:

5.1.1. Desempenho

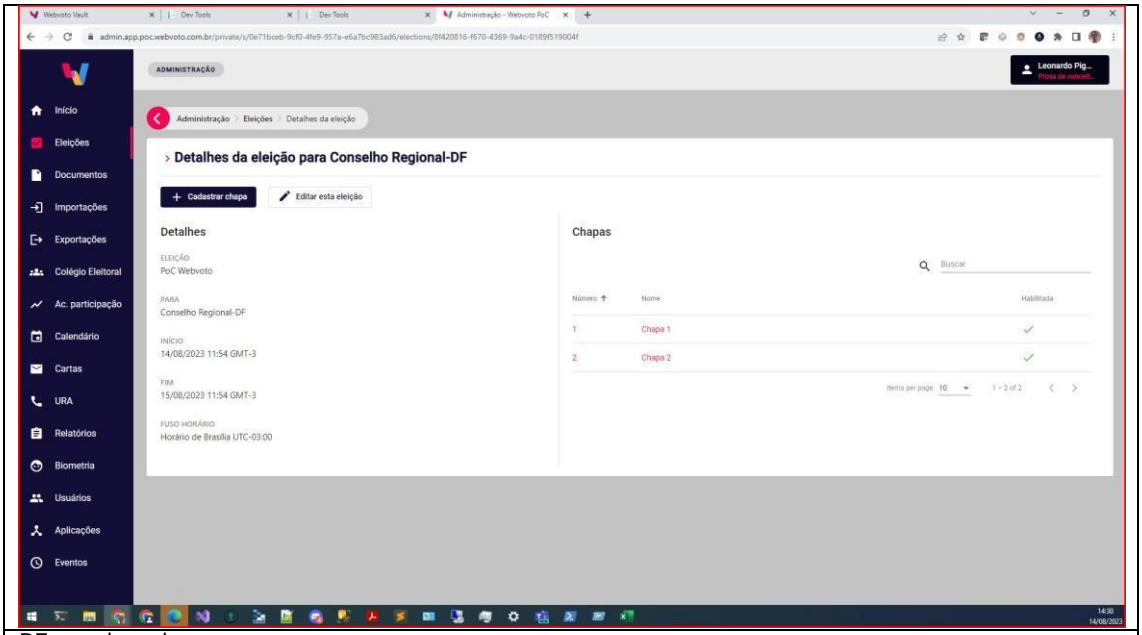
5.1.1.1. Gerar um colégio eleitoral com dados fictícios de no mínimo 500 mil eleitores distribuídos em pelo menos três localidades distintas a serem quantificados no processo do Sistema Eleitoral. Deverão existir, no mínimo, duas chapas concorrentes para cada localidade;



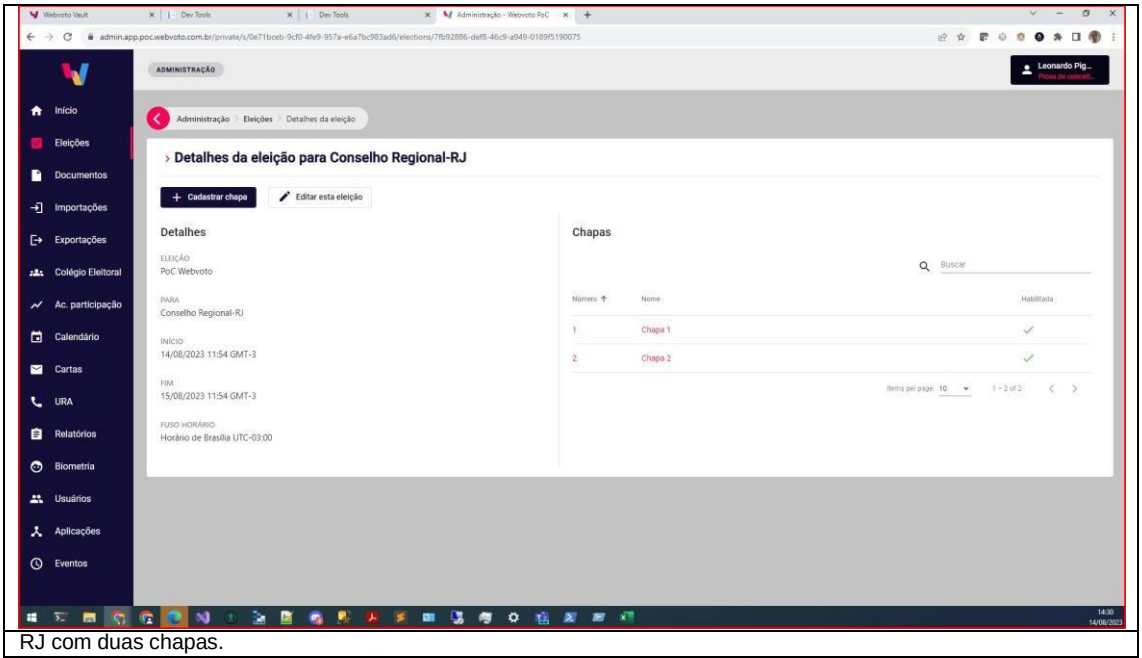
Importação de 500.000,00 eleitores.



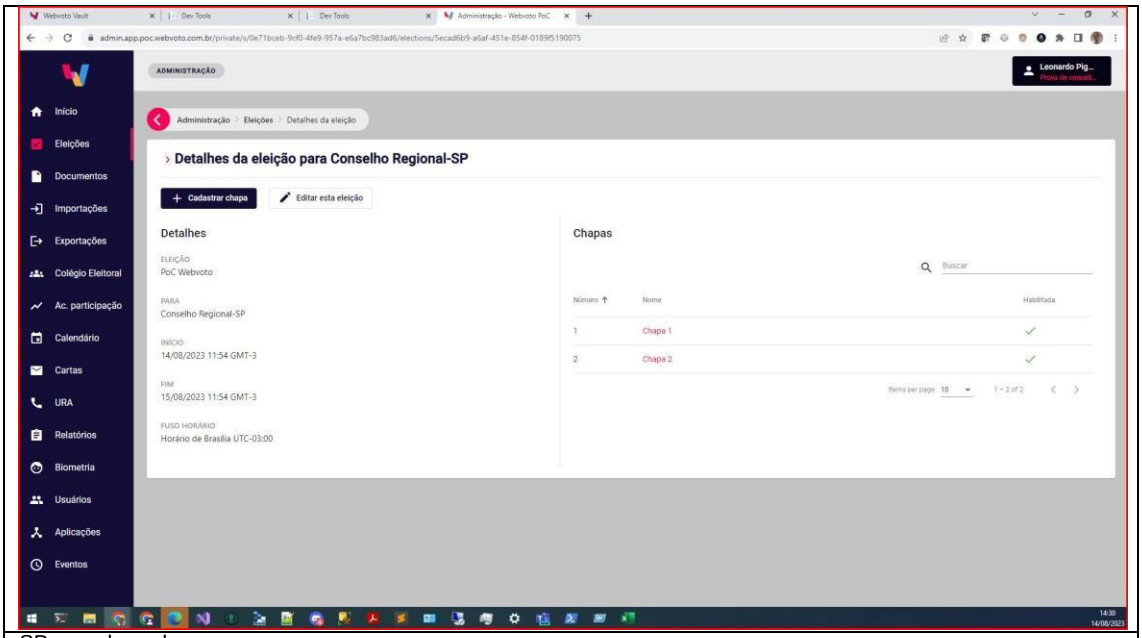
Grupo eleitoral em três localidades distintas.



DF com duas chapas.

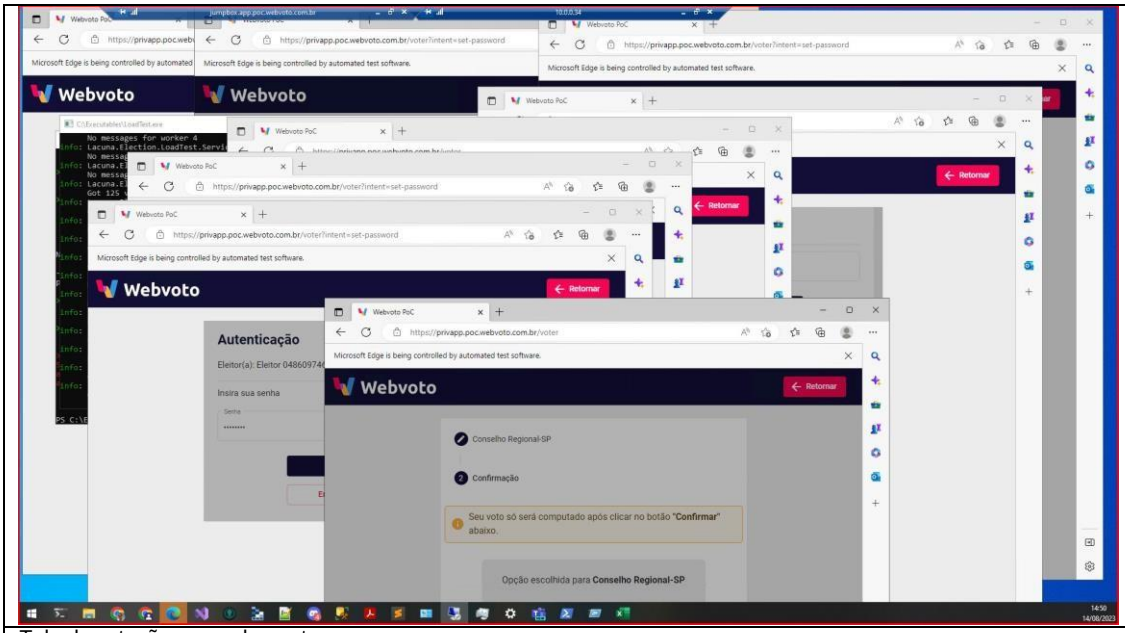


RJ com duas chapas.



SP com duas chapas.

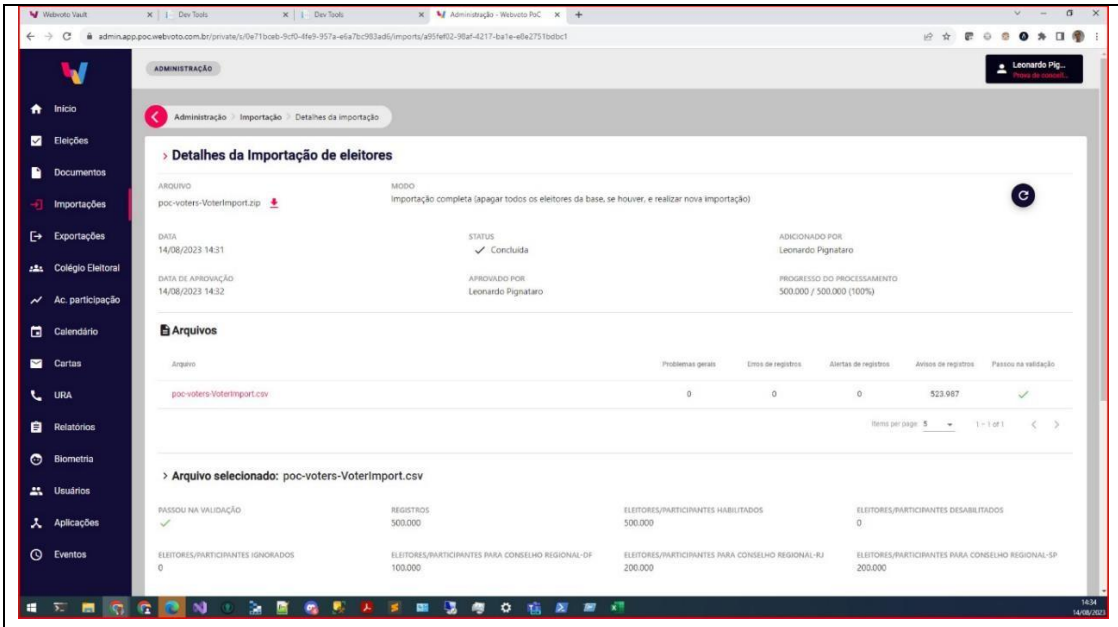
5.1.1.2. Simular uma eleição completa com o colégio eleitoral acima descrito em até duas horas ininterruptas com todos os procedimentos envolvidos, com concorrência mínima de 400 eleitores simultâneos durante o processo;



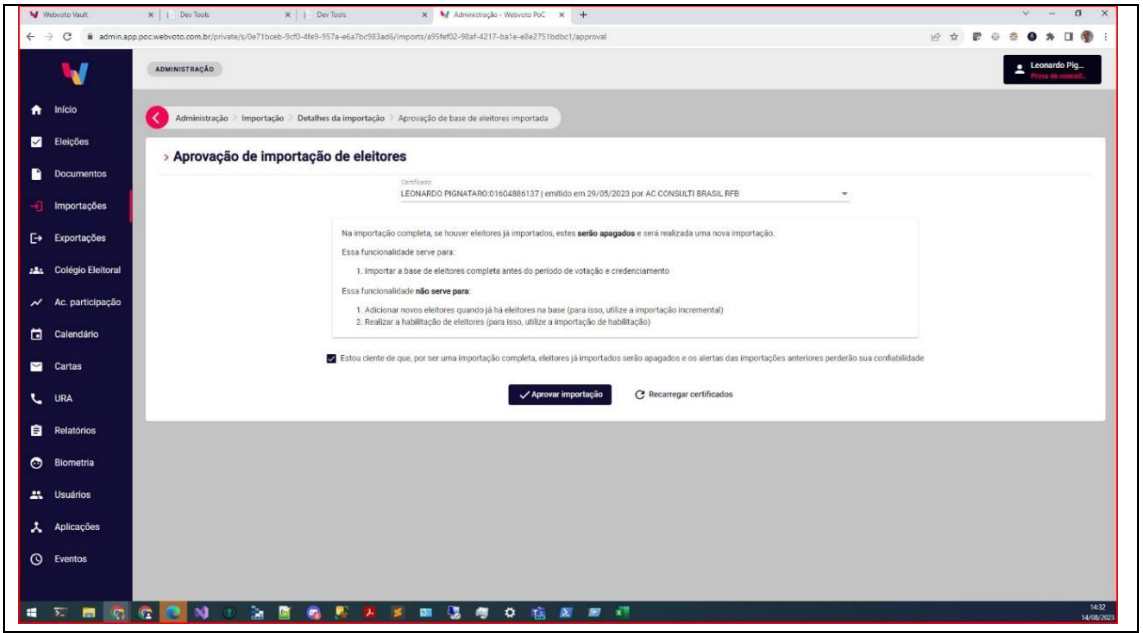
Tela de votação em andamento.

5.1.1.3. A simulação deverá:

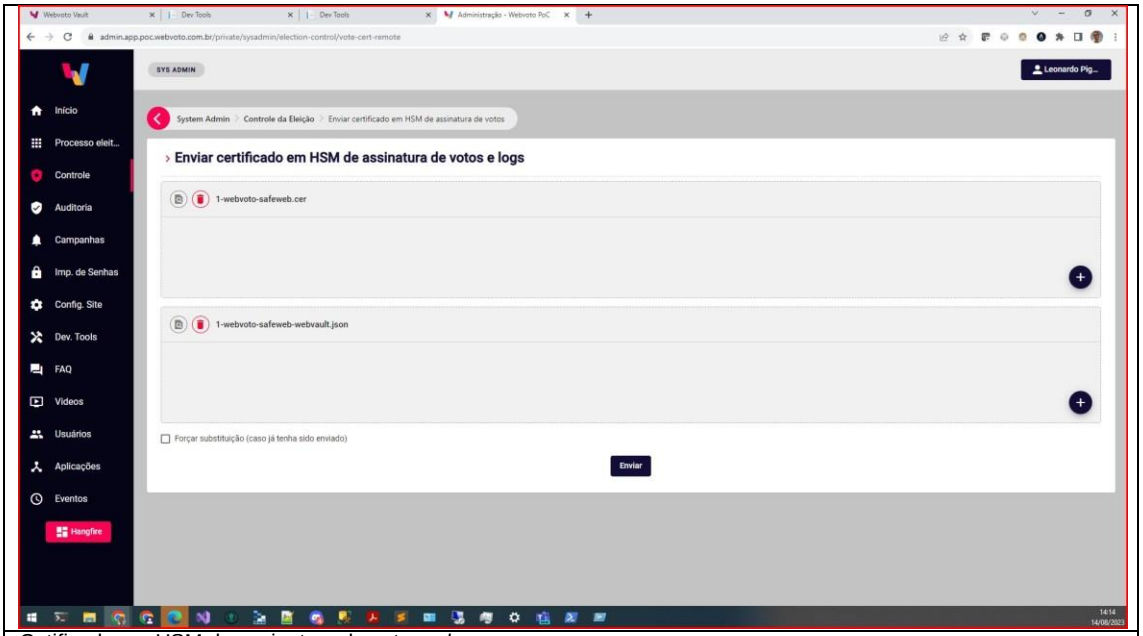
a) Gerar votos para cada um dos eleitores;



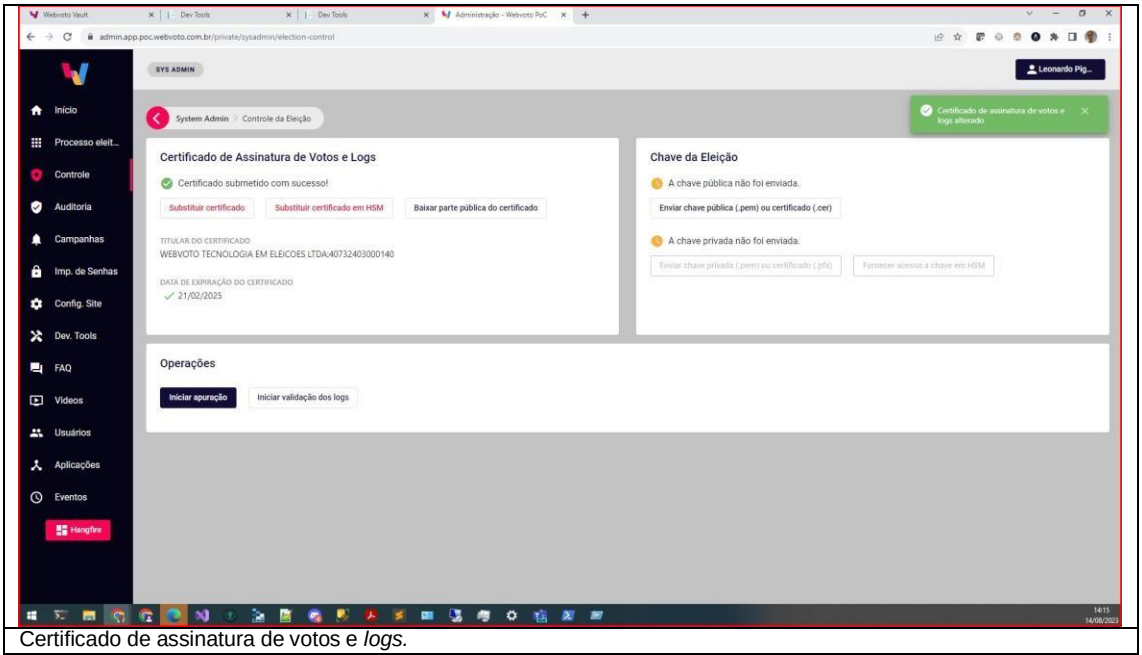
Importação e aprovação de eleitores.



Aprovação de importação de eleitores.

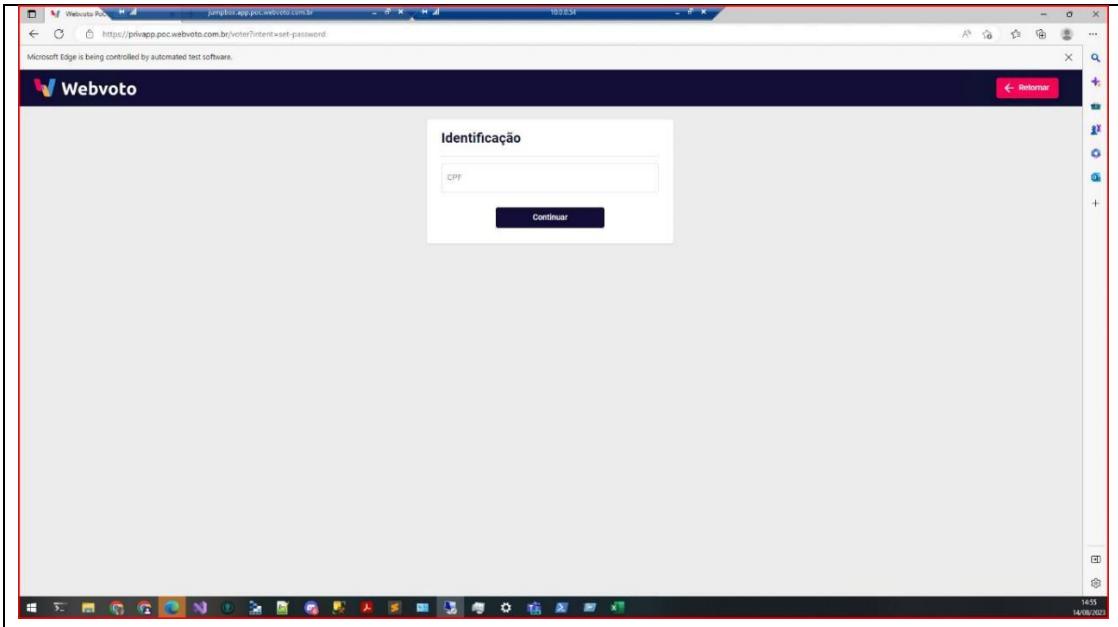


Cetificado em HSM de assinatura de votos e *logs*.

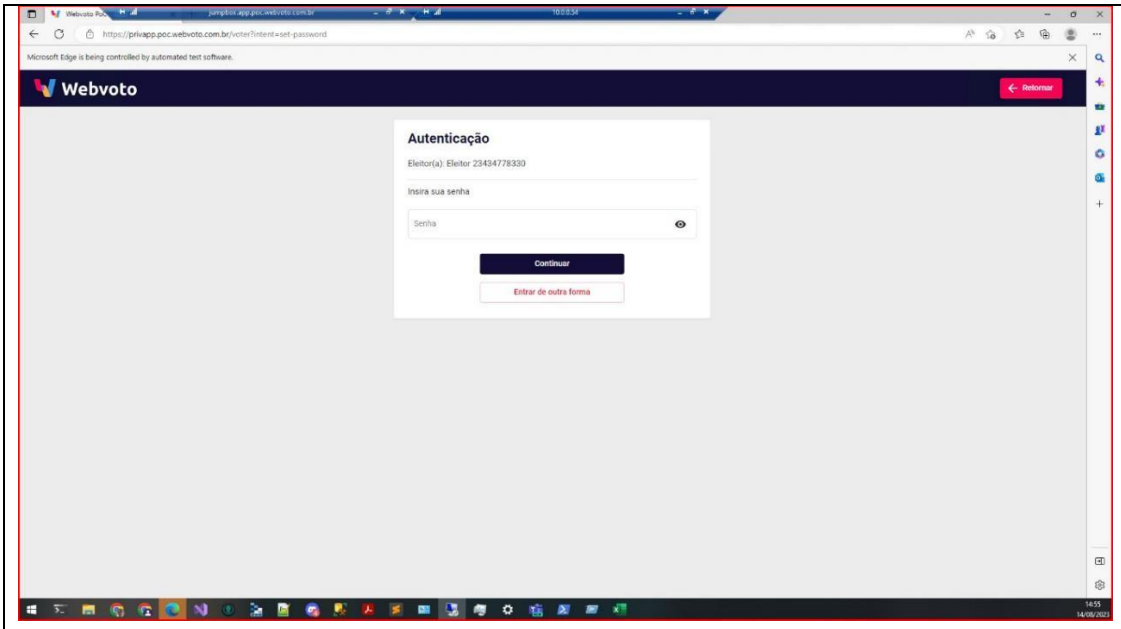


Certificado de assinatura de votos e *logs*.

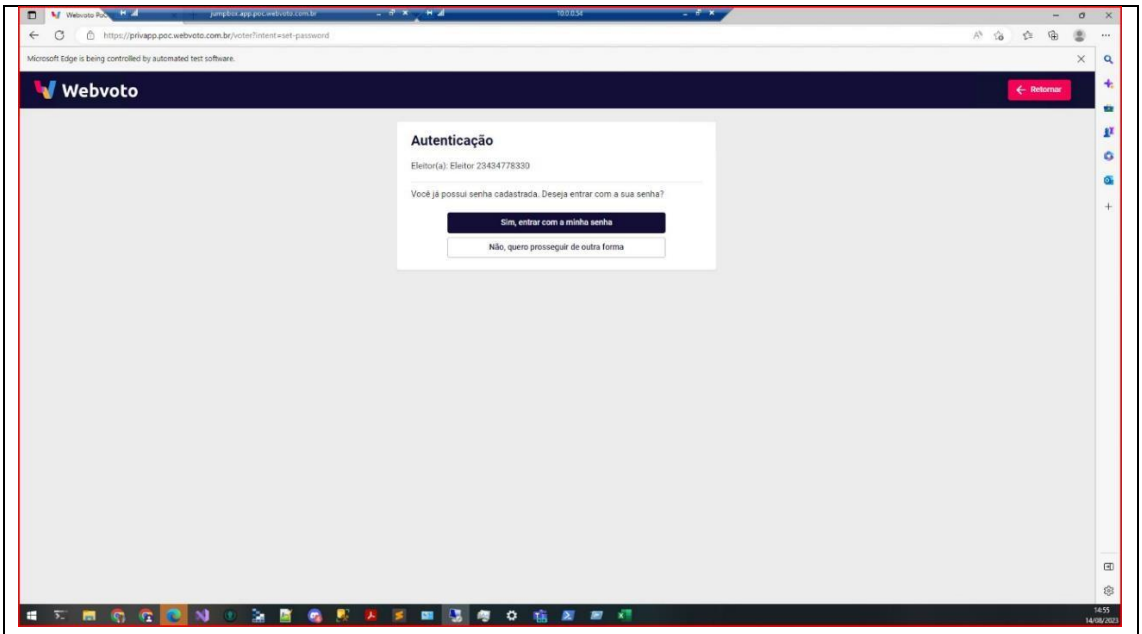
b) Realizar cada transação (votação) de forma completa, incluindo: Identificação do Eleitor, Alteração de senha, Votação com a nova senha e Emissão de comprovante eleitoral, apresentando as telas de cada operação, simulando na íntegra o comportamento do eleitor;



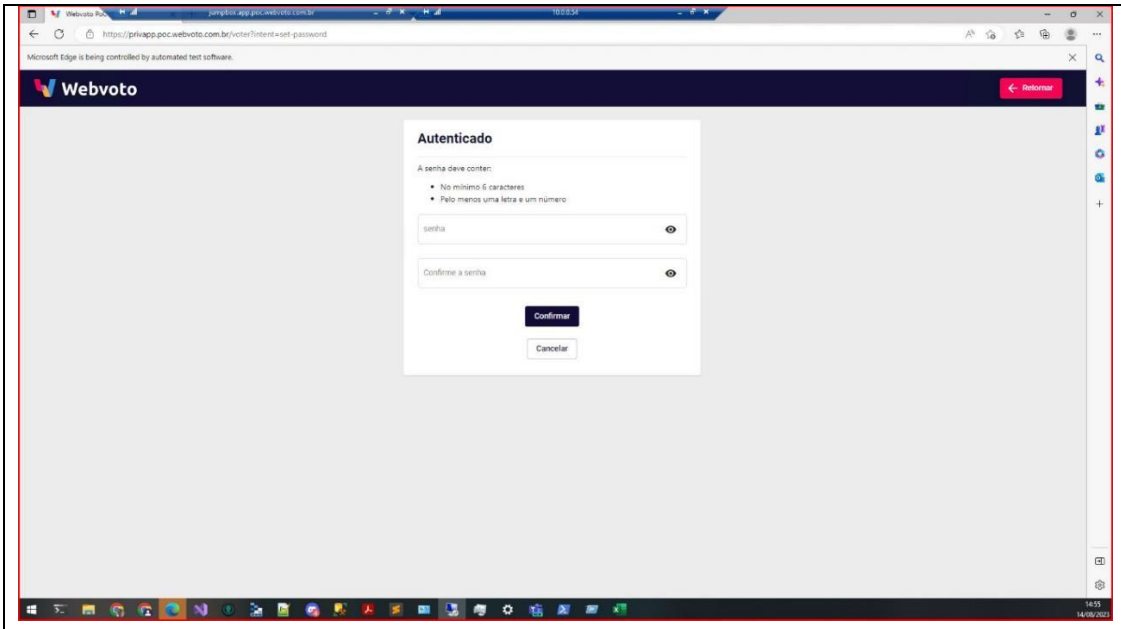
Identificação do eleitor.



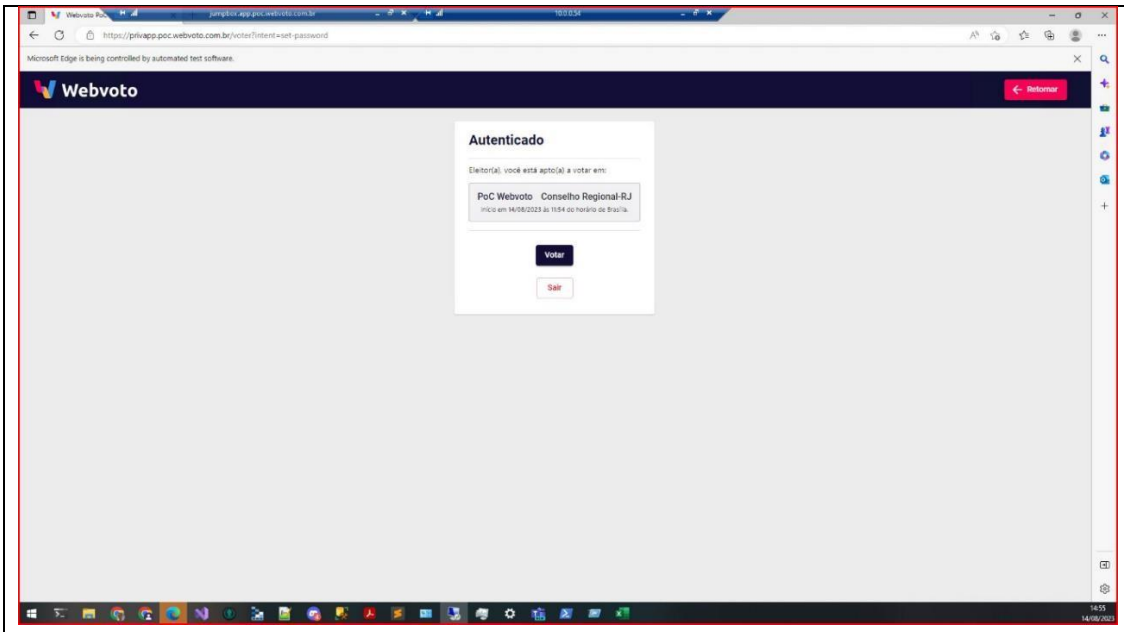
Eleitor inserindo senha.



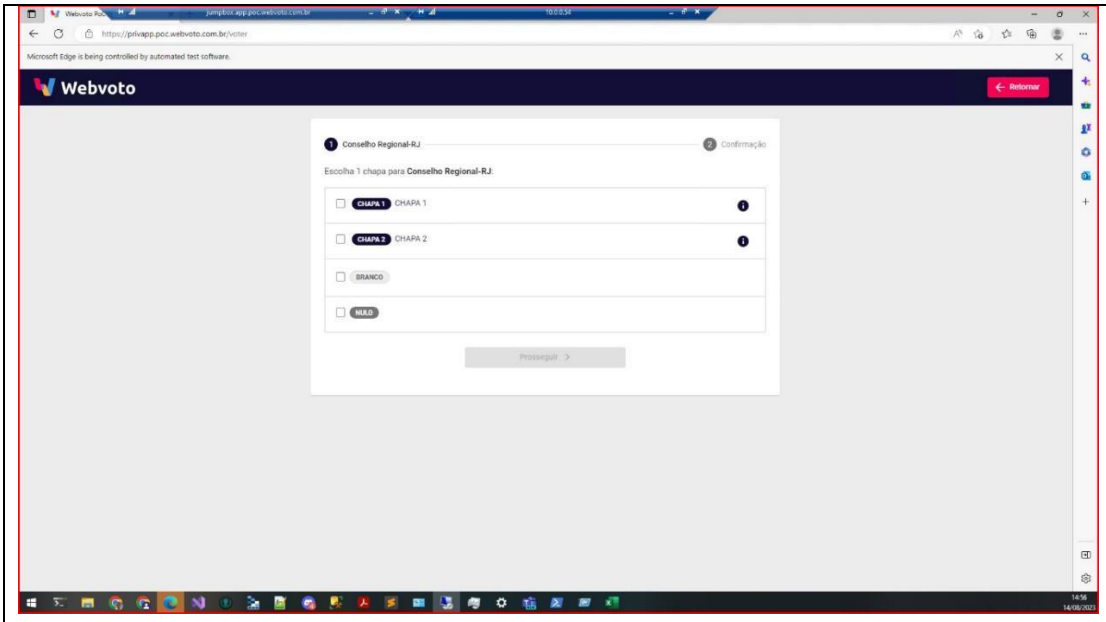
Autenticação do eleitor.



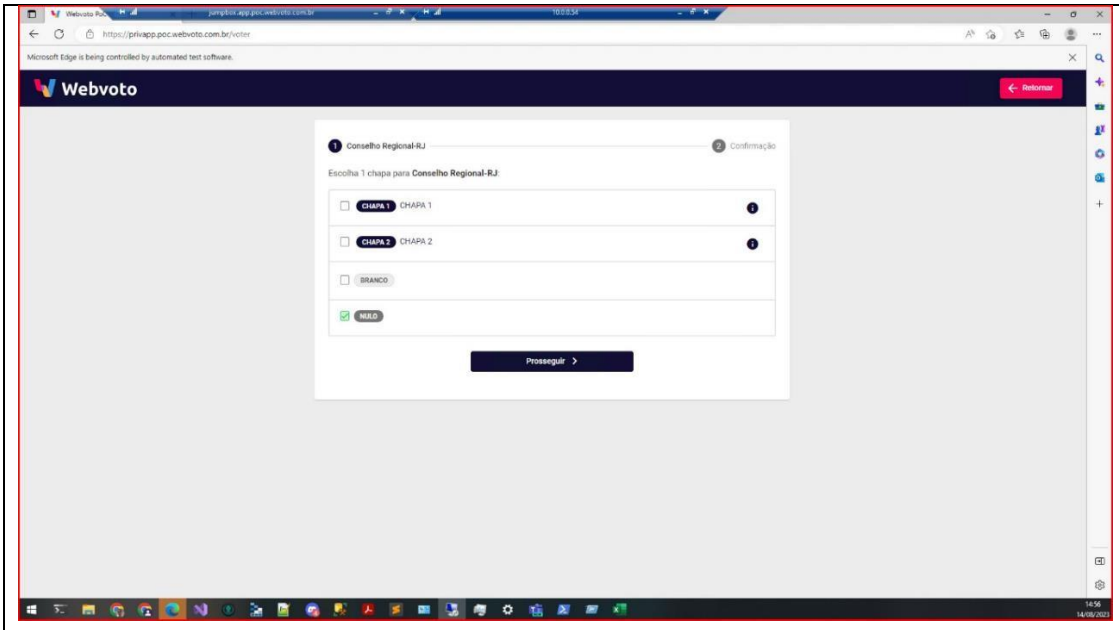
Alteração de senha.



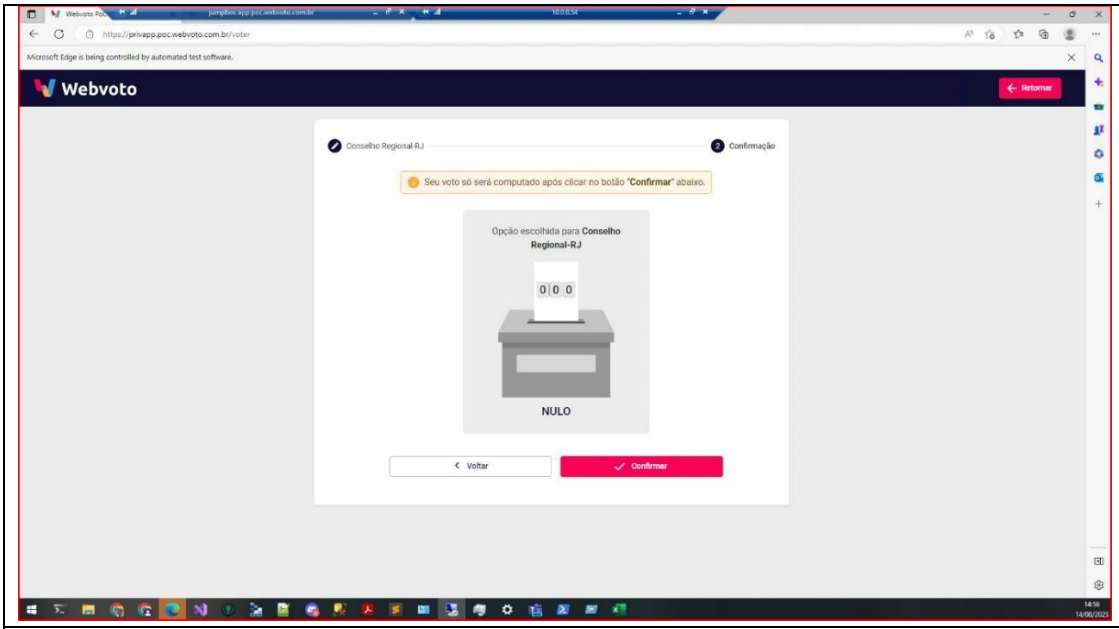
Eleitor autenticado.



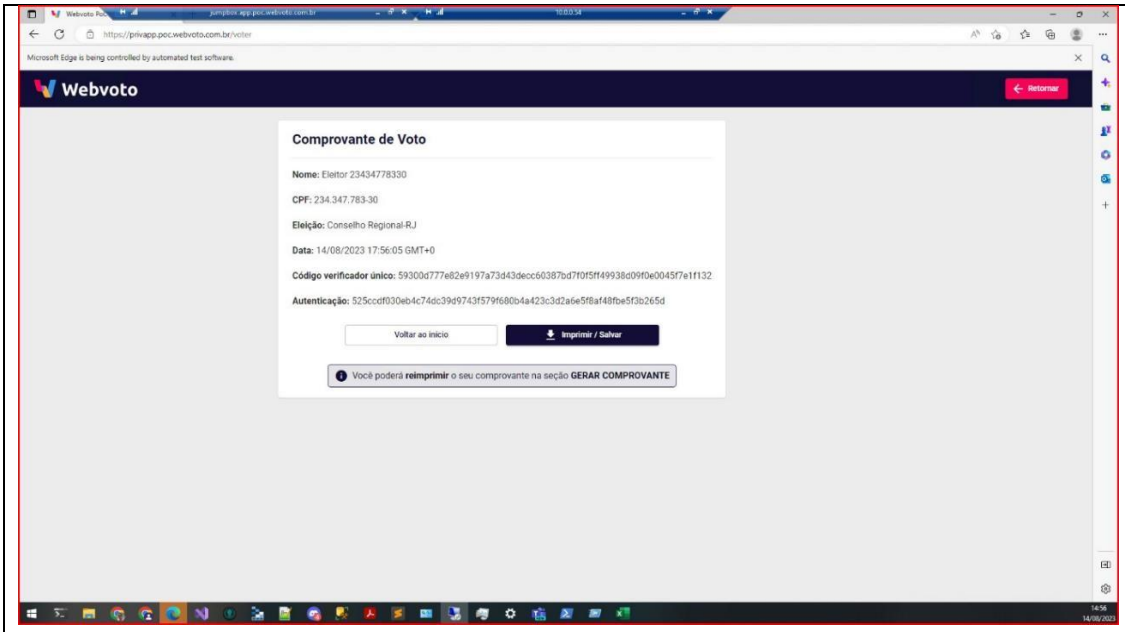
Processo de votação do eleitor.



Voto do eleitor.

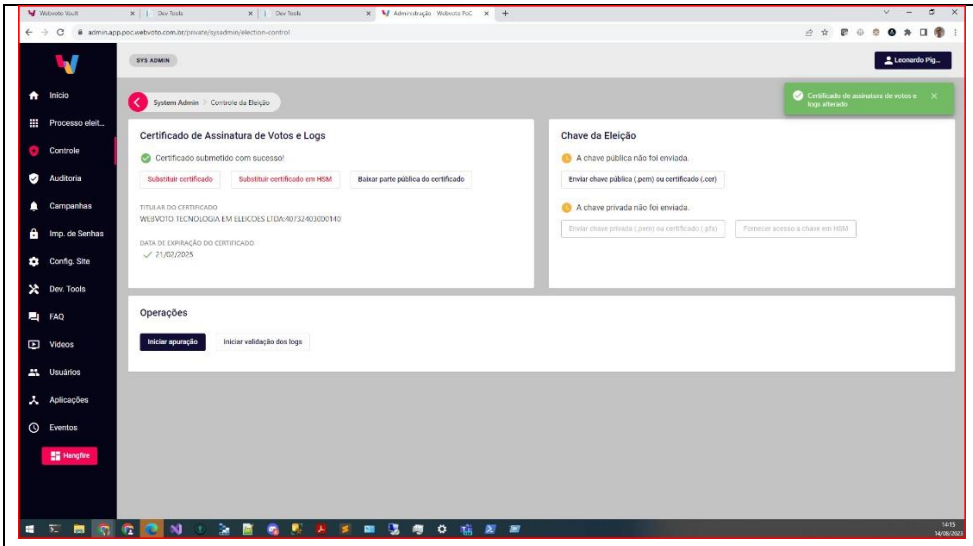


Voto nulo do eleitor.



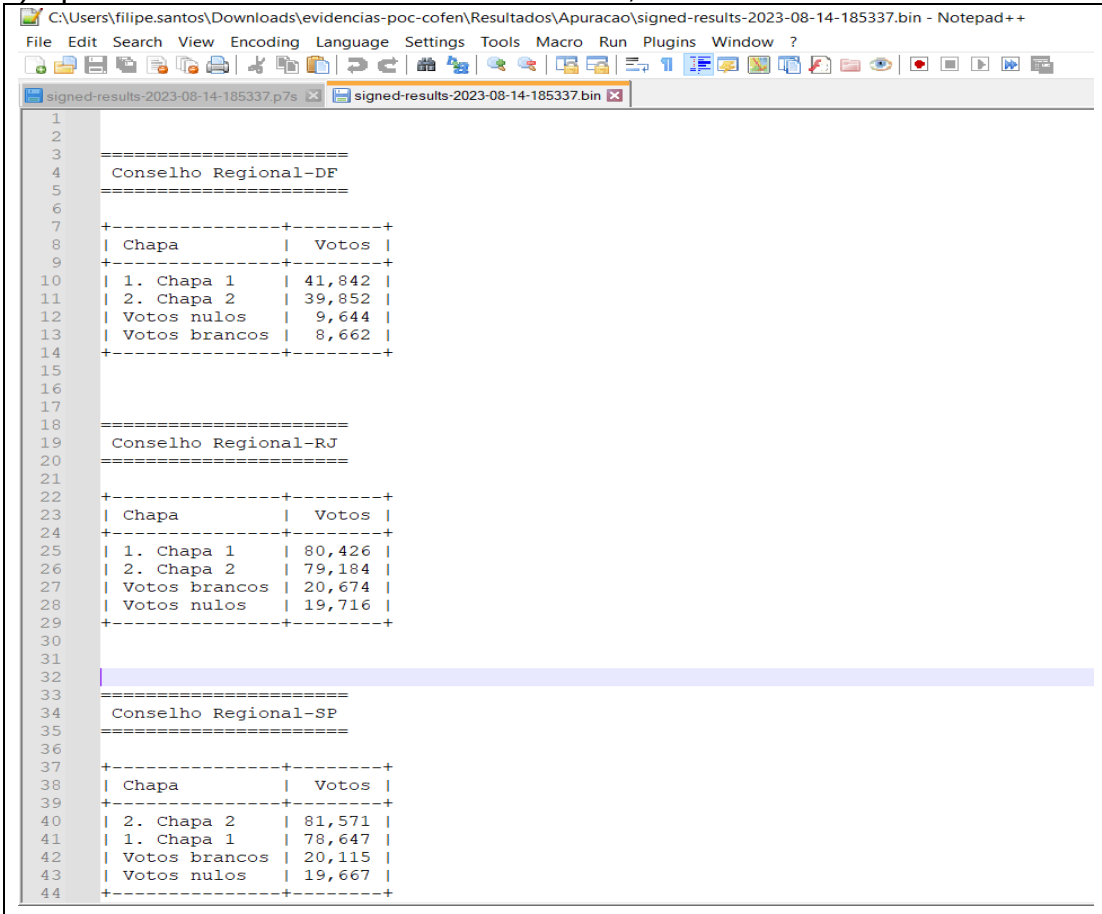
Comprovante de voto.

c) Realizar o processo de verificação de integridade das assinaturas dos votos;



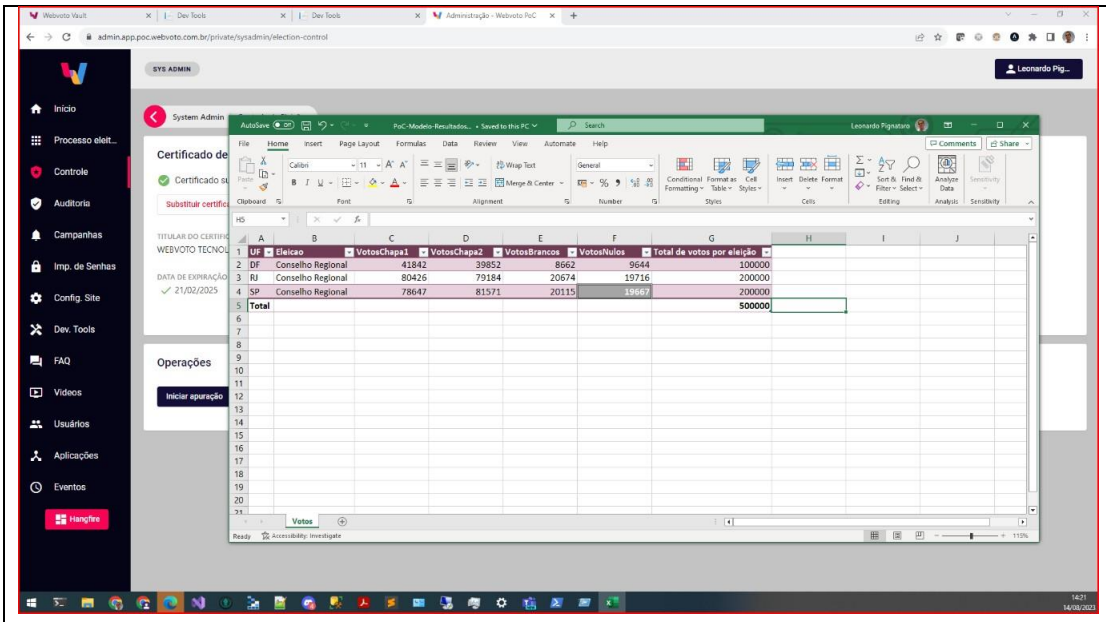
Integridade de *log* da eleição.

d) Apresentar relatório contendo o resultado;



Arquivo gerado após a finalização das votações.

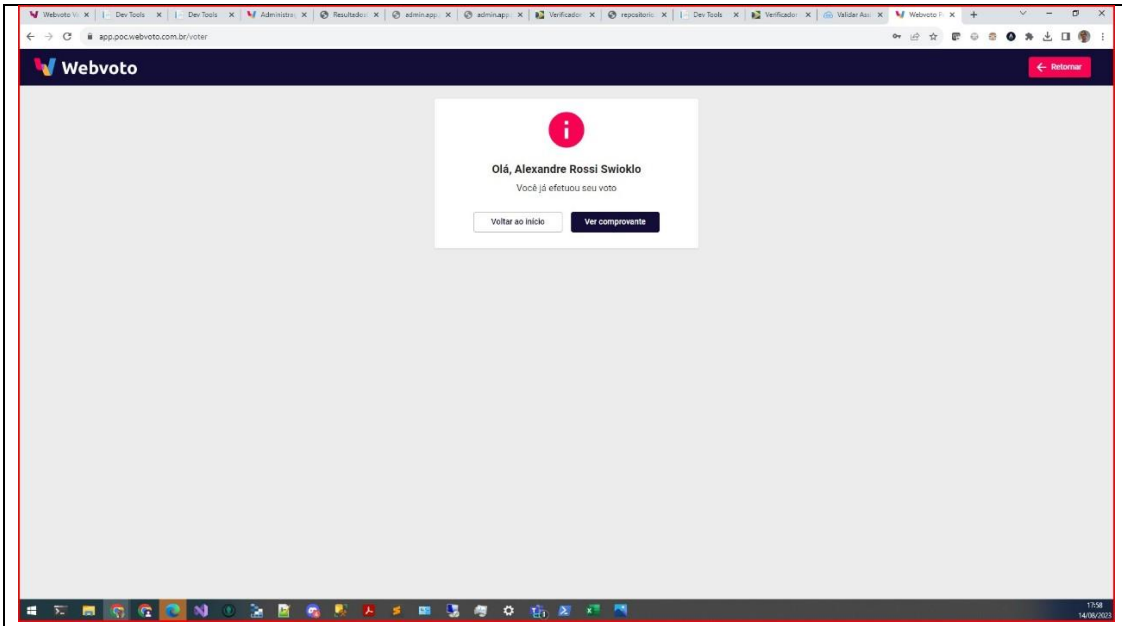
e) Deverá haver, dentre os votos gerados, votos válidos, brancos e nulos para todas as chapas;



UF	Eleicao	VotosChapa1	VotosChapa2	VotosBrancos	VotosNulos	Total de votos por eleição
DF	Conselho Regional	41842	39852	8662	9644	100000
RJ	Conselho Regional	80426	79184	20674	19716	200000
SP	Conselho Regional	78647	81571	20115	19667	200000
Total						500000

Tabela que foi utilizada para a automação dos votos.

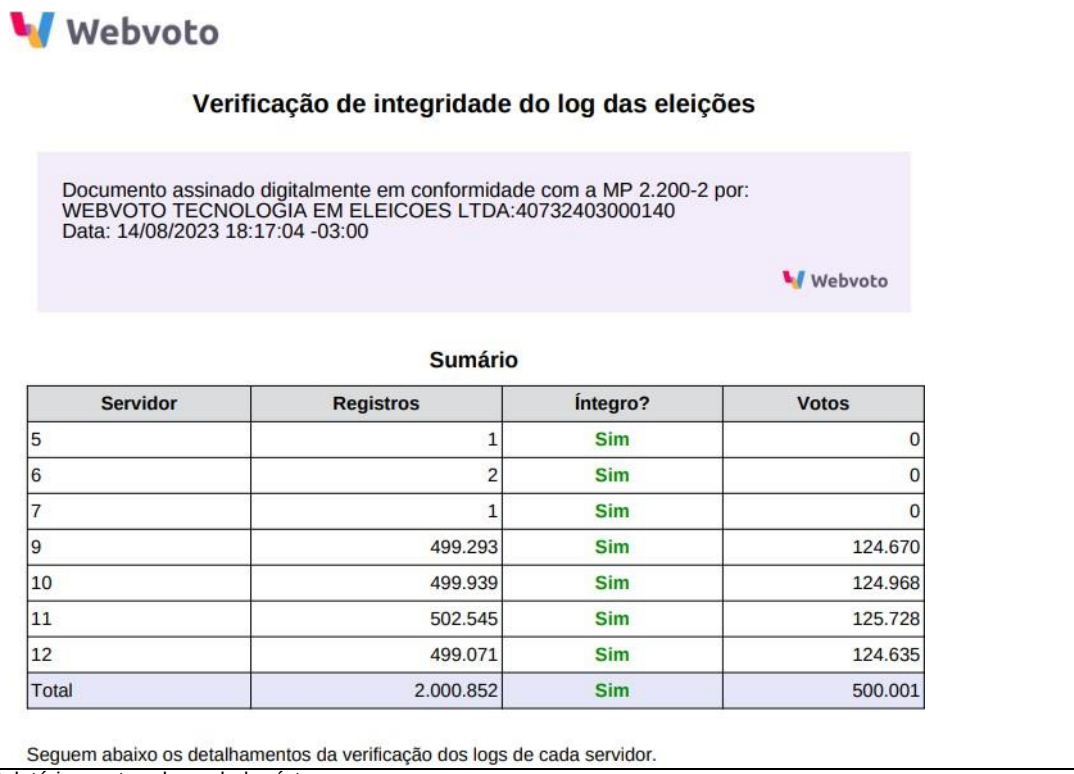
f) A solução deverá realizar os votos através das mesmas interfaces que serão disponibilizadas aos eleitores, ou seja, através de páginas *web*; e



Webvoto.

g) Não será admitida a inserção de votos diretamente no banco de dados, via *webservices* ou outros meios que não sejam páginas *web* que possam ser apresentadas aos eleitores.

Durante os testes, foi acrescentando um voto diretamente no banco de dados, quando se foi gerar uma prova de integridade, verificou-se que o sistema detectou a tentativa de adulteração na votação, e emitiu uma mensagem de falha, conforme a figura abaixo:



Webvoto

Verificação de integridade do log das eleições

Documento assinado digitalmente em conformidade com a MP 2.200-2 por:
WEBVOTO TECNOLOGIA EM ELEICOES LTDA:40732403000140
Data: 14/08/2023 18:17:04 -03:00

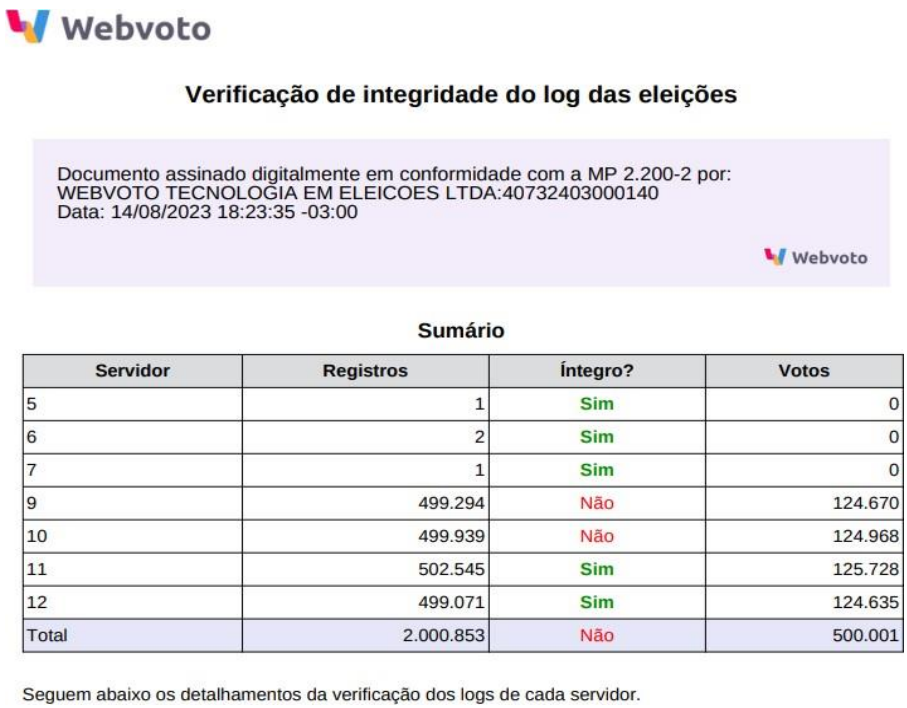
Webvoto

Sumário

Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.293	Sim	124.670
10	499.939	Sim	124.968
11	502.545	Sim	125.728
12	499.071	Sim	124.635
Total	2.000.852	Sim	500.001

Seguem abaixo os detalhamentos da verificação dos logs de cada servidor.

Relatório mostrando os dados íntegros.



Webvoto

Verificação de integridade do log das eleições

Documento assinado digitalmente em conformidade com a MP 2.200-2 por:
WEBVOTO TECNOLOGIA EM ELEICOES LTDA:40732403000140
Data: 14/08/2023 18:23:35 -03:00

Webvoto

Sumário

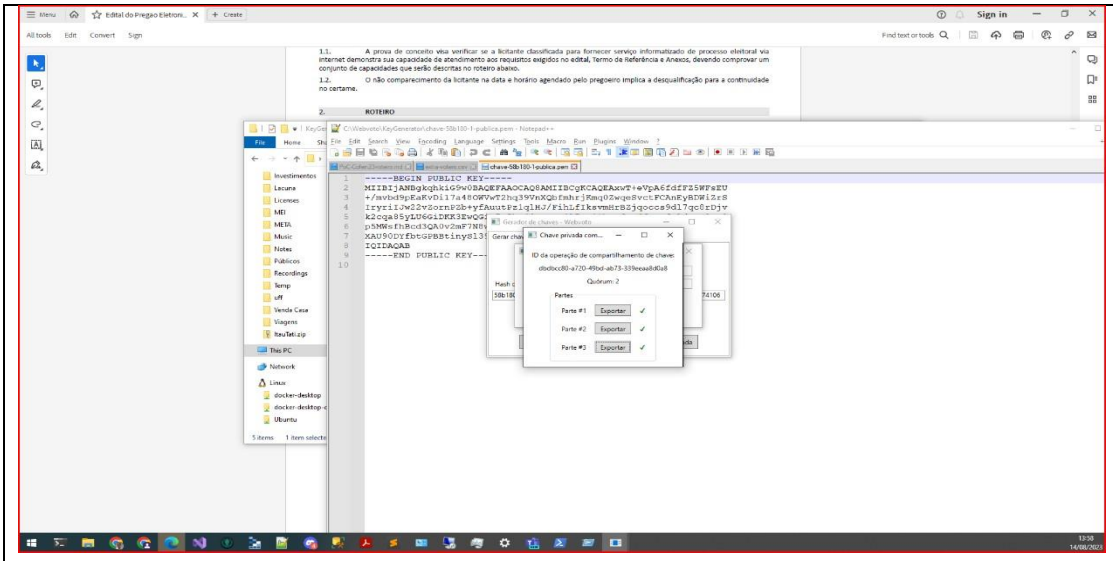
Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.294	Não	124.670
10	499.939	Não	124.968
11	502.545	Sim	125.728
12	499.071	Sim	124.635
Total	2.000.853	Não	500.001

Seguem abaixo os detalhamentos da verificação dos logs de cada servidor.

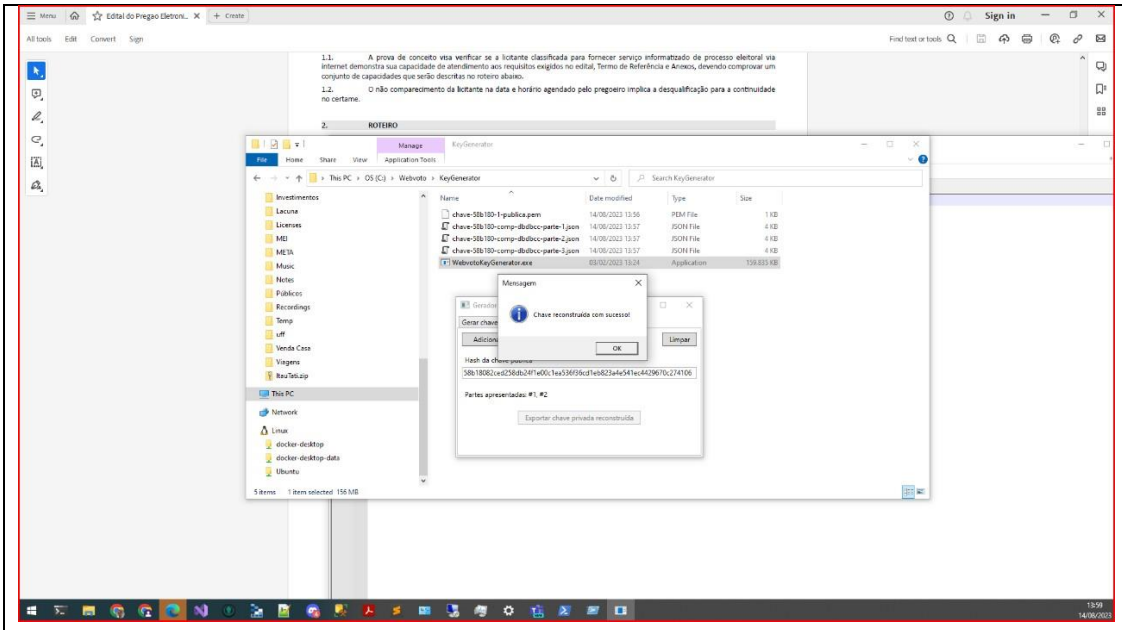
Relatório mostrando que foi acrescentado um voto no servidor 9, resultando na perda da integridade.

5.1.2. Segurança

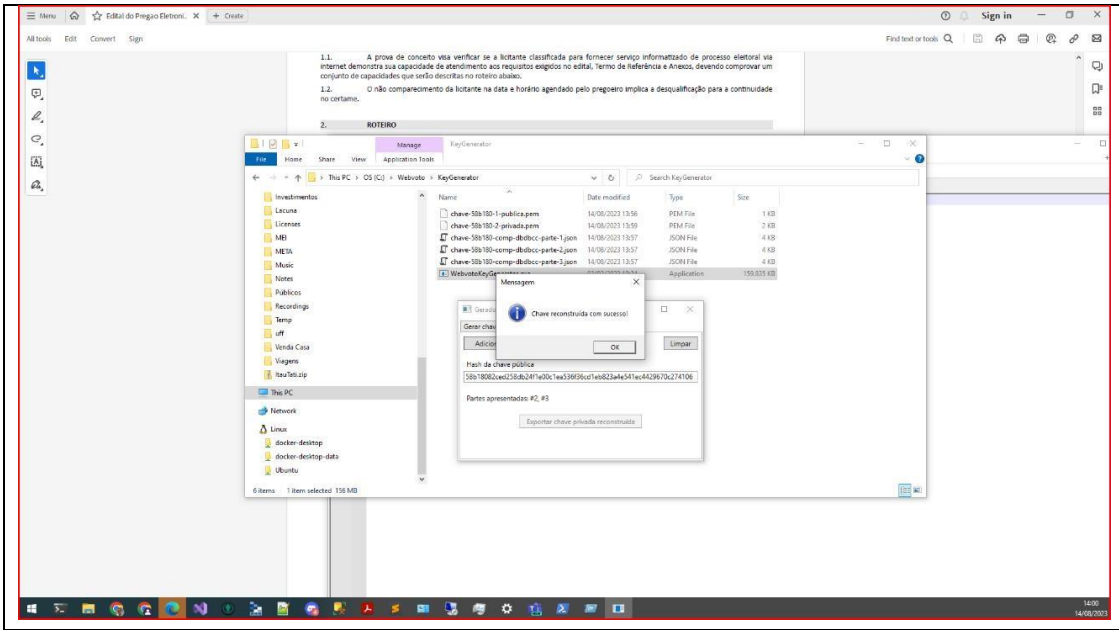
5.1.2.1. Antes do início da simulação, deve ser gerado um par de chaves padrão RSA sendo que a chave privada deve ser dividida utilizando o algoritmo Shamir Secret Sharing. A comissão julgadora poderá decidir como será feita a divisão da chave com no mínimo três partes, com duas obrigatórias.



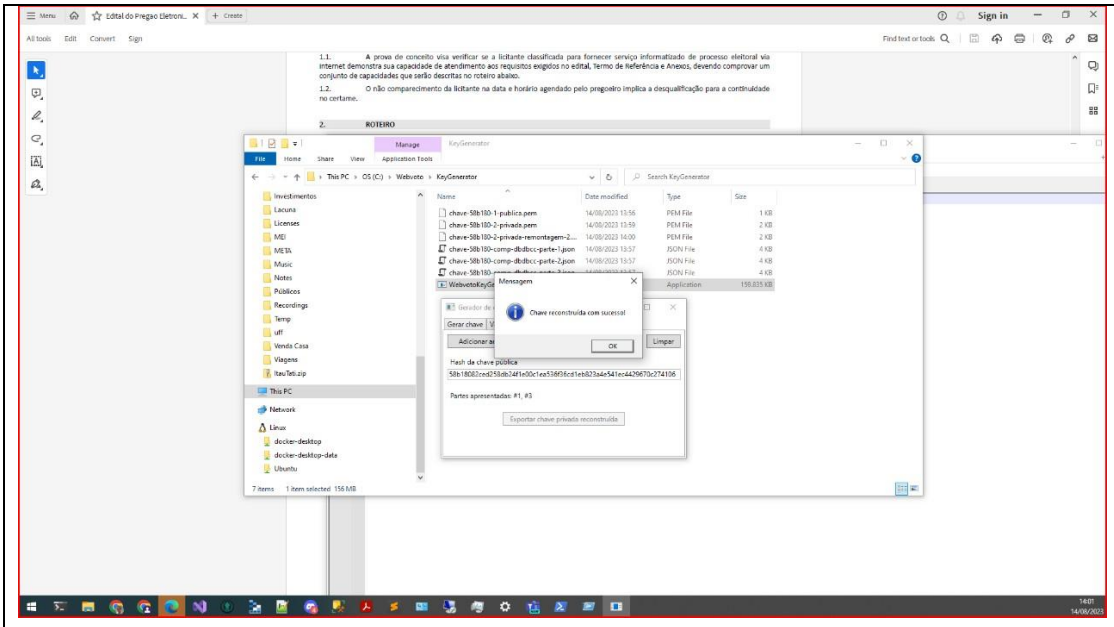
Processo de geração da chave em três segmentos distintos, sendo fundamental o emprego de duas dessas partes para viabilizar a sua reconstituição.



Realiza a reconstrução por meio da utilização exclusiva da Parte 1 e da Parte 2.

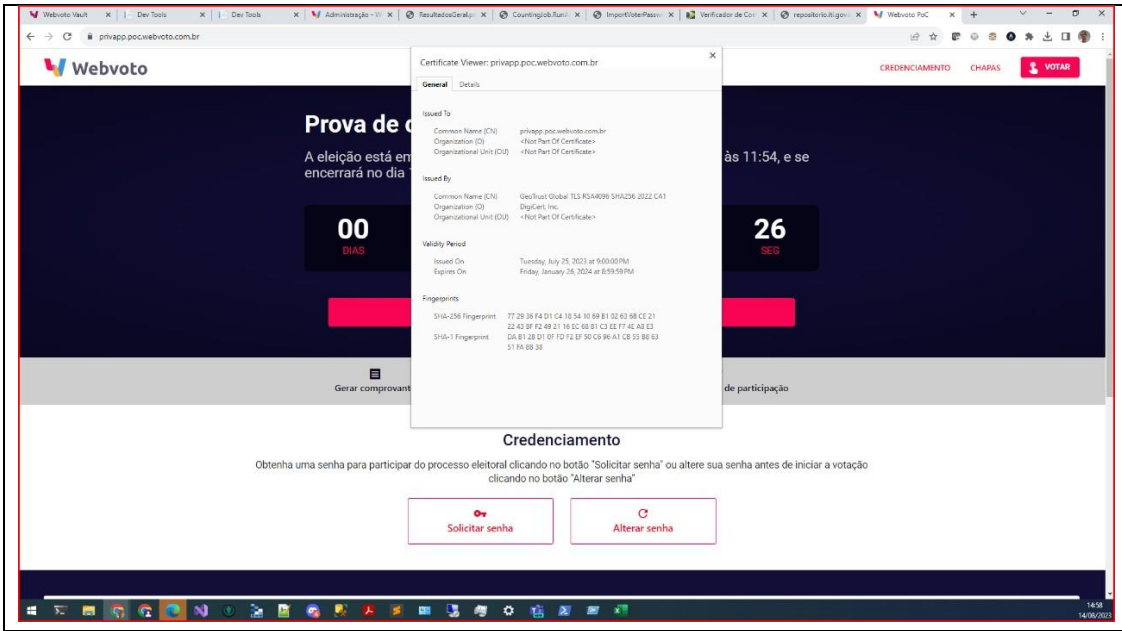


Realiza a reconstrução por meio da utilização exclusiva da Parte 2 e da Parte 3.



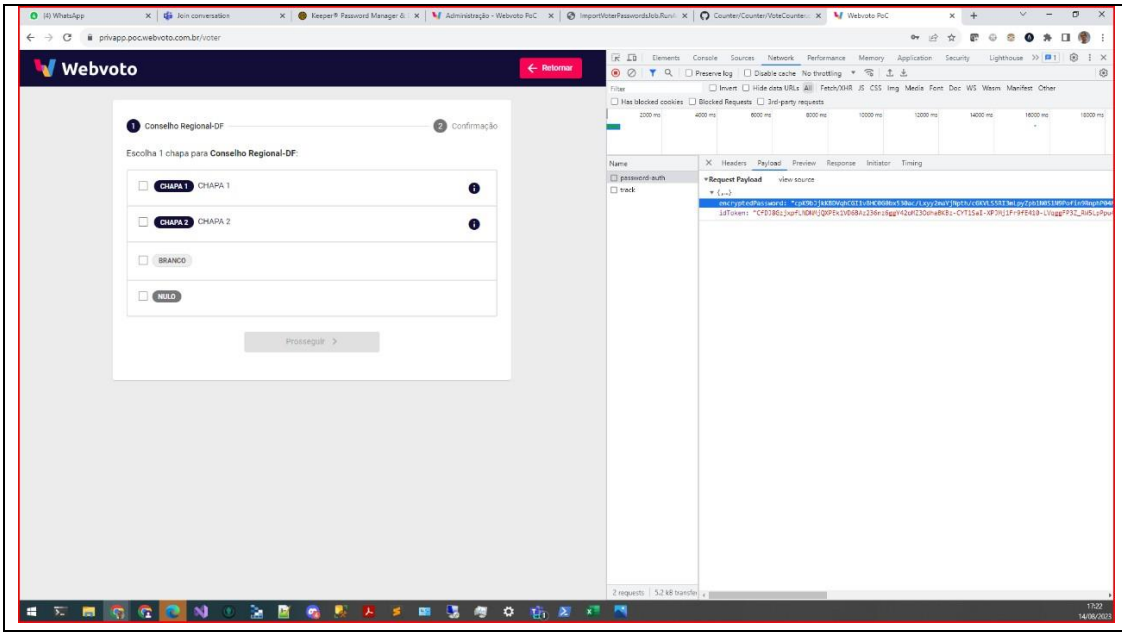
Realiza a reconstrução por meio da utilização exclusiva da Parte 1 e da Parte 3.

5.1.2.2. A solução deverá utilizar certificado de servidor (SSL) para criptografia da conexão com o servidor;



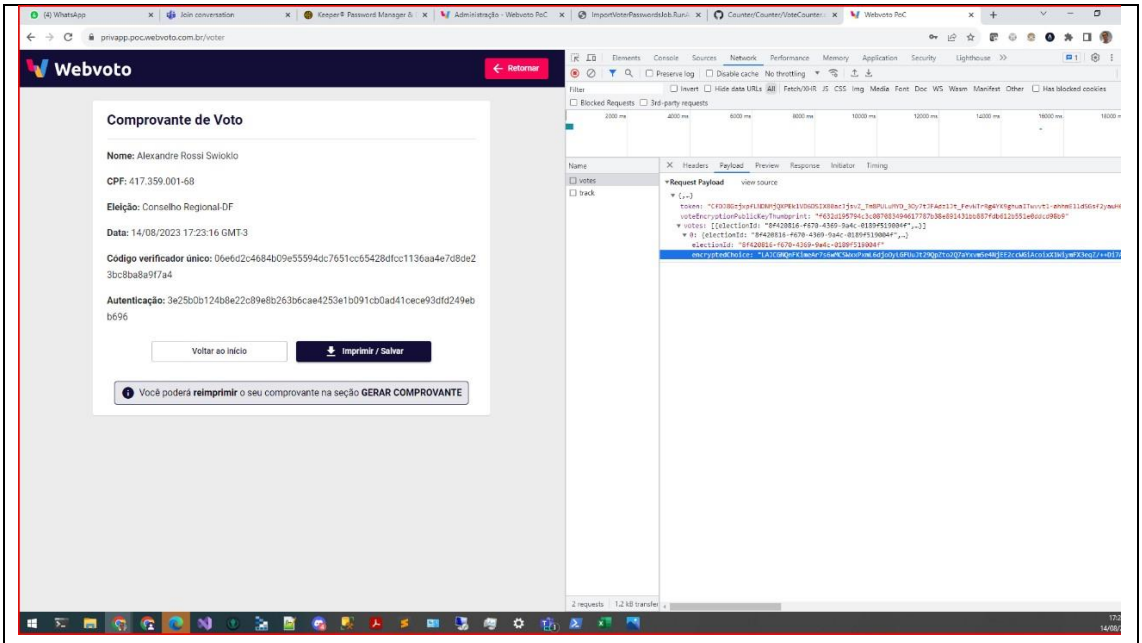
Certificado está valido.

5.1.2.3. Ao executar o *login*, a senha do eleitor não deve trafegar em texto claro entre o *browser* e o servidor, independente do uso de criptografia no canal de acesso (SSL);



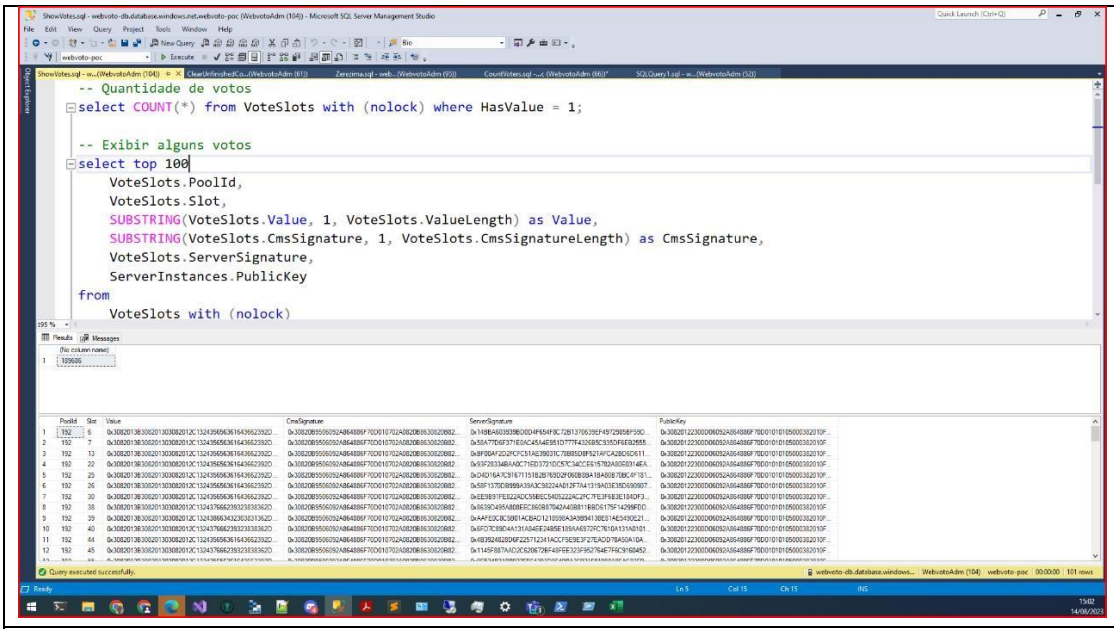
A senha se encontra submetida a um processo de criptografia.

5.1.2.4. Ao executar o voto, a escolha do eleitor não deve trafegar em texto claro entre o *browser* e o servidor, devendo este conteúdo estar encriptado com a chave fornecida através do certificado digital do tipo A3 emitido pelo ICP-Brasil fornecido antes do início da eleição;



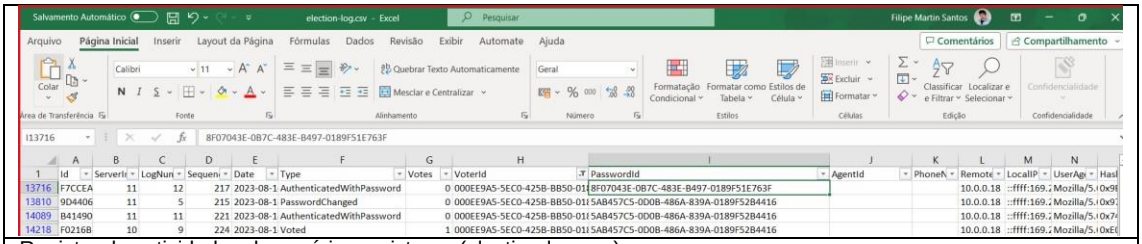
O voto se encontra submetida a um processo de criptografia.

5.1.2.5. A solução deverá armazenar o voto do eleitor encriptado em seu banco de dados e não poderá conhecer o resultado em nenhum momento;



Exibindo no banco alguns votos, mostrando que o valor está criptografado.

5.1.2.6. A solução deverá armazenar registro de *log* que apresente todos os acessos do eleitor ao sistema, informando a data/hora do evento, o endereço IP de origem e o tipo de navegador utilizado;



Registro das atividades do usuário no sistema (election-log.csv).

5.1.2.7. Os registros de *log* armazenados no sistema devem estar protegidos por mecanismos criptográficos que permitam verificar caso eles tenham sido alterados, removidos ou inseridos de alguma forma que não seja pelo próprio sistema;

Webvoto

Verificação de integridade do log das eleições

Documento assinado digitalmente em conformidade com a MP 2.200-2 por:
WEBVOTO TECNOLOGIA EM ELEICOES LTDA:40732403000140
Data: 14/08/2023 18:17:04 -03:00

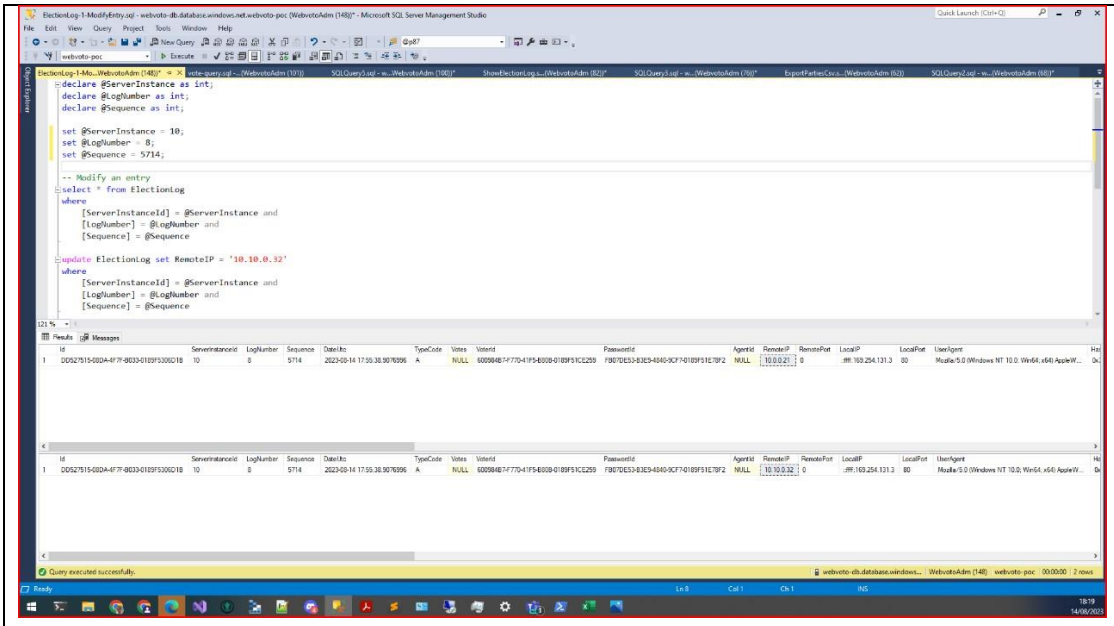
Webvoto

Sumário

Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.293	Sim	124.670
10	499.939	Sim	124.968
11	502.545	Sim	125.728
12	499.071	Sim	124.635
Total	2.000.852	Sim	500.001

Seguem abaixo os detalhamentos da verificação dos logs de cada servidor.

Relatório mostrando os dados íntegros.



Alteração do IP no servidor 10 de 10.0.0.21 para 10.10.0.32.

Verificação de integridade do log das eleições

Documento assinado digitalmente em conformidade com a MP 2.200-2 por:
WEBVOTO TECNOLOGIA EM ELEICOES LTDA:40732403000140
Data: 14/08/2023 18:20:30 -03:00

Webvoto

Sumário

Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.293	Sim	124.670
10	499.939	Não	124.968
11	502.545	Sim	125.728
12	499.071	Sim	124.635
Total	2.000.852	Não	500.001

Durante o processo de validação foi verificado que o servidor 10 não está integro.

Sumário

Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.294	Não	124.670
10	499.939	Não	124.968
11	502.545	Sim	125.728
12	499.071	Sim	124.635
Total	2.000.853	Não	500.001

É possível verificar que o servidor 9 sofreu um processo de inserção, pois no *log* anterior estava com 499.293 registros e depois ficou com 499.294. Assim respondendo como não integro.

Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.294	Não	124.670
10	499.939	Não	124.968
11	502.545	Sim	125.728
12	499.070	Não	124.635
Total	2.000.852	Não	500.001

É possível verificar que o servidor 12 sofreu um processo de remoção, pois no *log* anterior estava com 499.071 registros e depois ficou com 499.070. Assim respondendo como não integro.

5.1.2.8. A solução deverá assinar digitalmente todos os votos realizados e todos os logs do sistema conforme as normas vigentes da ICP-Brasil (vide DOC-ICP-15 em sua versão mais recente no ato da publicação do edital relativo a este Termo de Referência, publicado pelo ITI) utilizando certificado A3 e deverá permitir a verificação de sua assinatura no verificador no sítio do ITI.

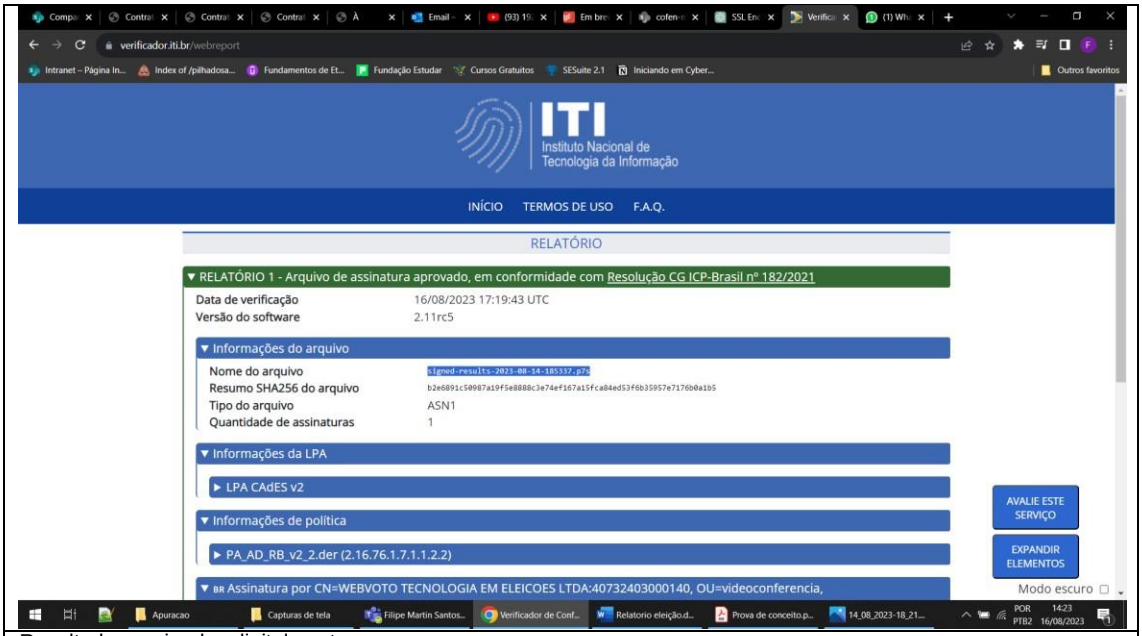
Assinatura digital dos votos.

5.1.2.9. Ao final da simulação todas as assinaturas de todos os votos devem ser entregues ao auditor em um arquivo compactado para conferência se todos os votos foram assinados corretamente;

4f22928c-881d-40e3-9f82-25e7f40bfbc7.bin	14/08/2023 17:39	Arquivo BIN	1 KB
4f22928c-881d-40e3-9f82-25e7f40bfbc7.p7s	14/08/2023 17:39	Assinatura PKCS nº...	77 KB
012-001-5718.p7s	14/08/2023 17:30	Assinatura PKCS nº...	3 KB
259e18e6-be32-420f-90c0-36c863377759.bin	14/08/2023 17:35	Arquivo BIN	1 KB
259e18e6-be32-420f-90c0-36c863377759.p7s	14/08/2023 17:35	Assinatura PKCS nº...	77 KB
converted-1692045118494.bin	14/08/2023 17:32	Arquivo BIN	1 KB
ResultadosGeral.pdf	14/08/2023 14:40	Documento do Ad...	256 KB
signed-results-2023-08-14-185337.bin	14/08/2023 15:57	Arquivo BIN	1 KB
signed-results-2023-08-14-185337.p7s	14/08/2023 15:53	Assinatura PKCS nº...	358 KB
ValidacaoLogEleicao (1).pdf	14/08/2023 18:20	Documento do Ad...	272 KB
ValidacaoLogEleicao (2).pdf	14/08/2023 18:23	Documento do Ad...	272 KB
ValidacaoLogEleicao (3).pdf	14/08/2023 18:26	Documento do Ad...	272 KB
ValidacaoLogEleicao.pdf	14/08/2023 18:17	Documento do Ad...	272 KB
vote-cms-signature.p7s	14/08/2023 15:06	Assinatura PKCS nº...	3 KB
vote-server-public-key.bin	14/08/2023 15:08	Arquivo BIN	1 KB
vote-server-signature.bin	14/08/2023 15:08	Arquivo BIN	1 KB
vote-value.bin	14/08/2023 15:06	Arquivo BIN	1 KB

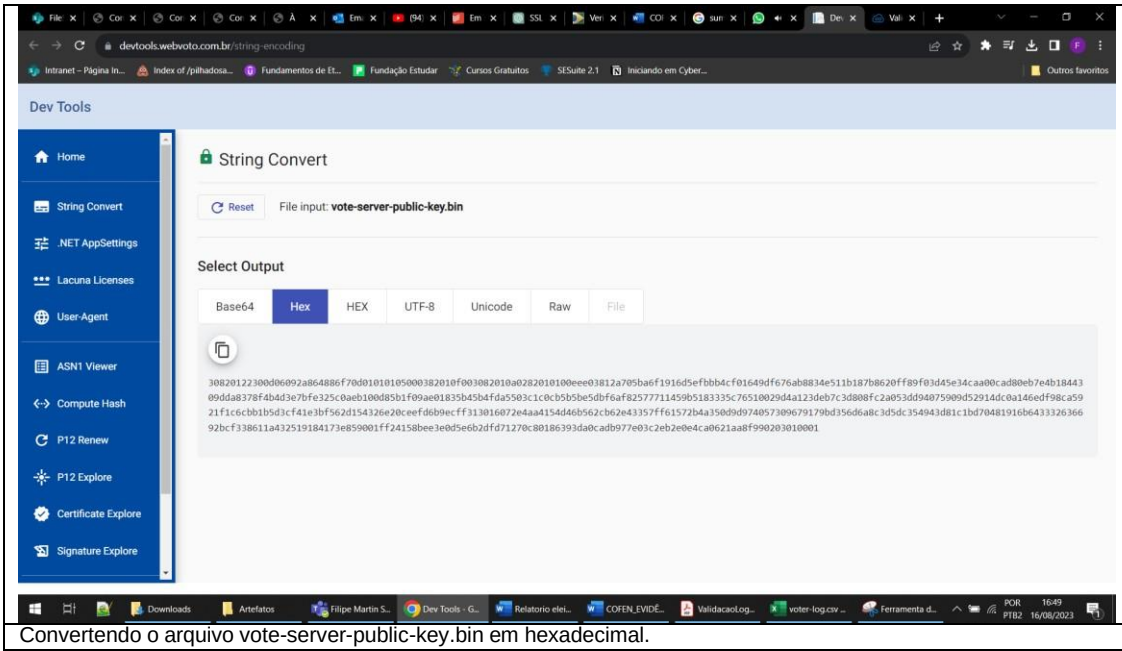
Todos os artefatos possuem assinaturas validas.

5.1.2.10. Demostrar que na autenticação utilizando certificado digital, foi gerada uma evidência assinada digitalmente e com adição de carimbo de tempo ICP-Brasil e com a possibilidade de ser validada no verificados de conformidade do ITI.

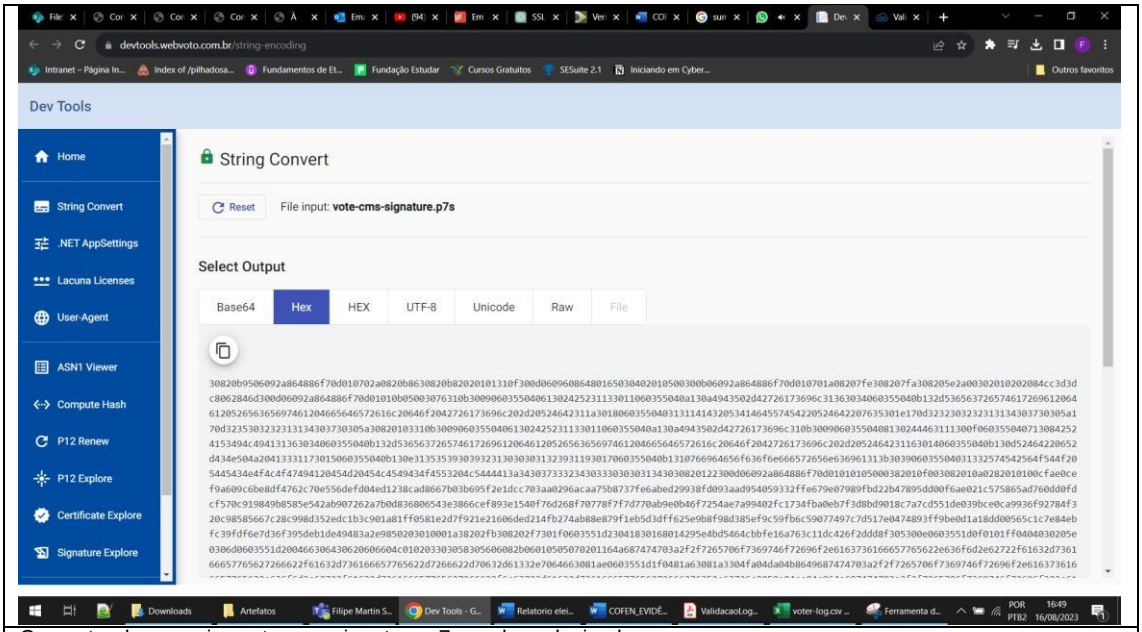


Resultados assinados digitalmente.

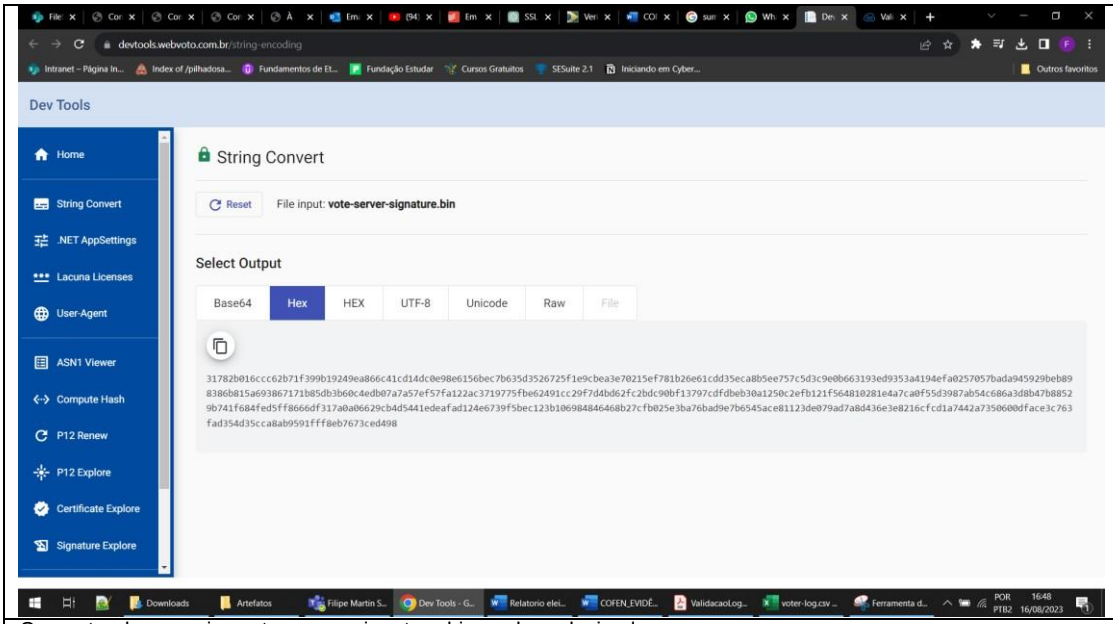
5.1.2.11. Demonstrar que realiza assinatura dupla dos votos, sendo a primeira realizada com certificado usado na solução ou da Auditoria ou da Comissão Eleitoral e a segunda realizada com chave efêmera no servidor.



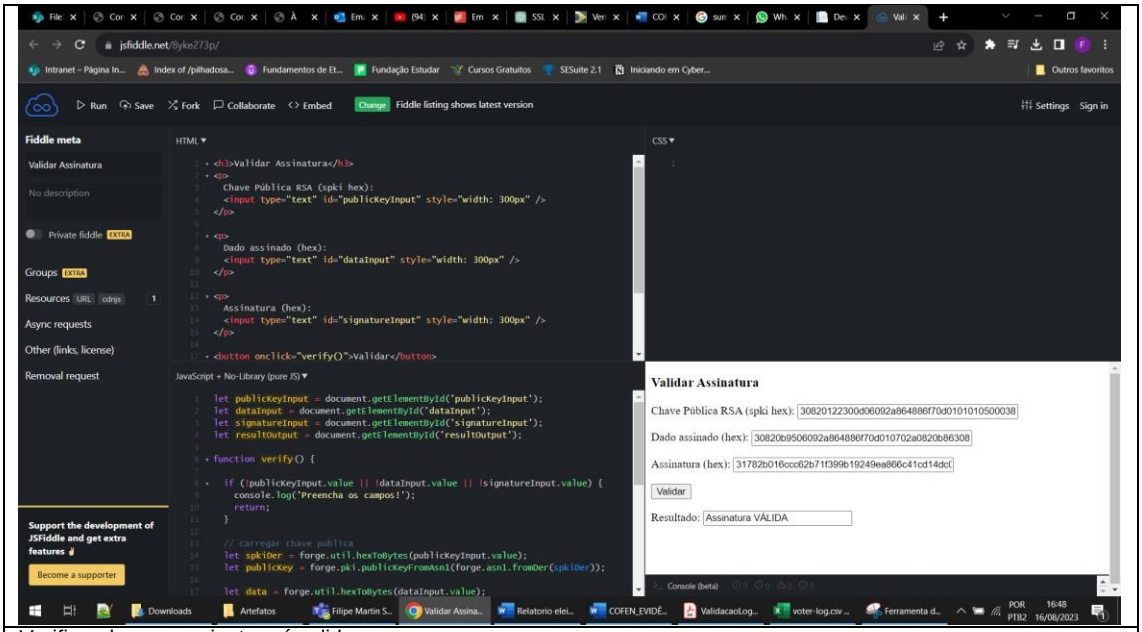
Convertendo o arquivo vote-server-public-key.bin em hexadecimal.



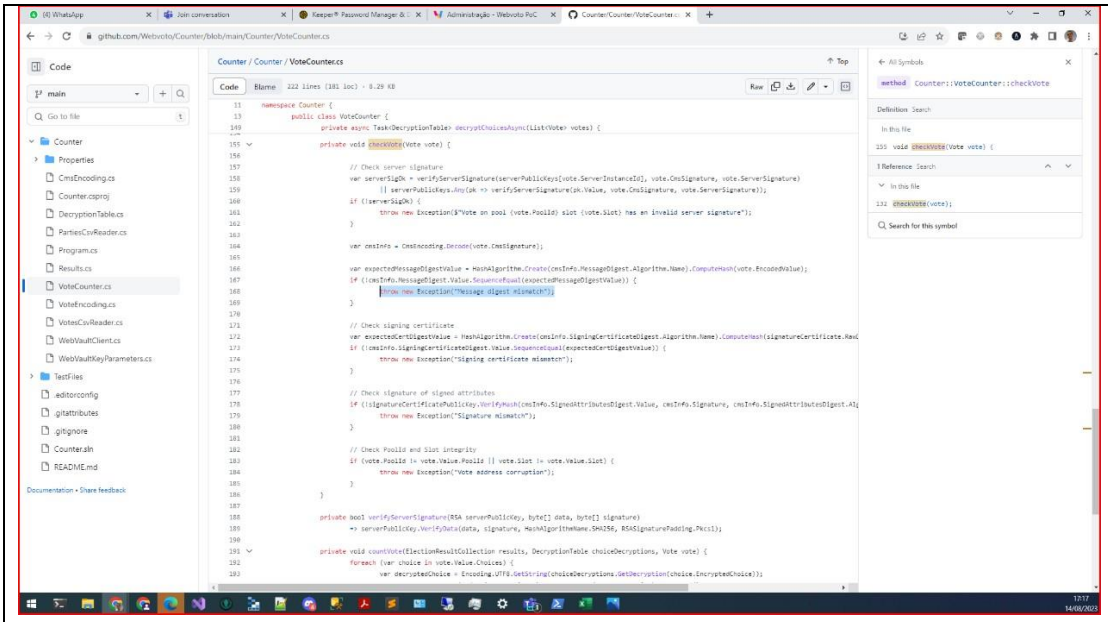
Convertendo o arquivo vote-cms-signature.p7s em hexadecimal.



Convertendo o arquivo vote-server-signature.bin em hexadecimal



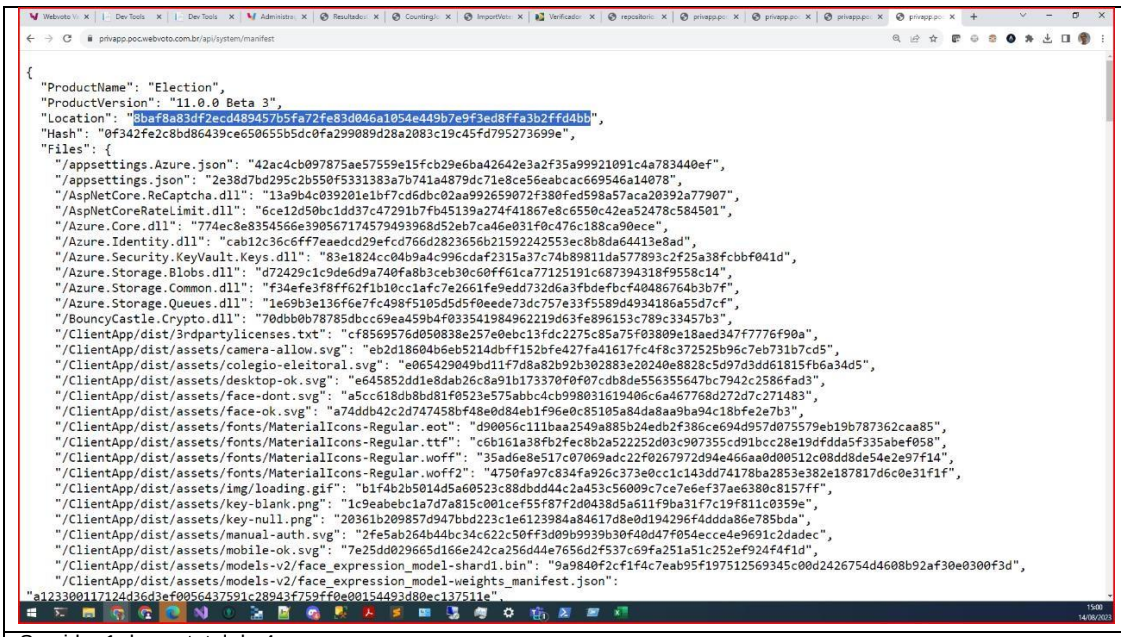
Verificando se a assinatura é valida



O contador procede à verificação de cada uma das assinaturas mediante a utilização da chave efêmera correspondente.

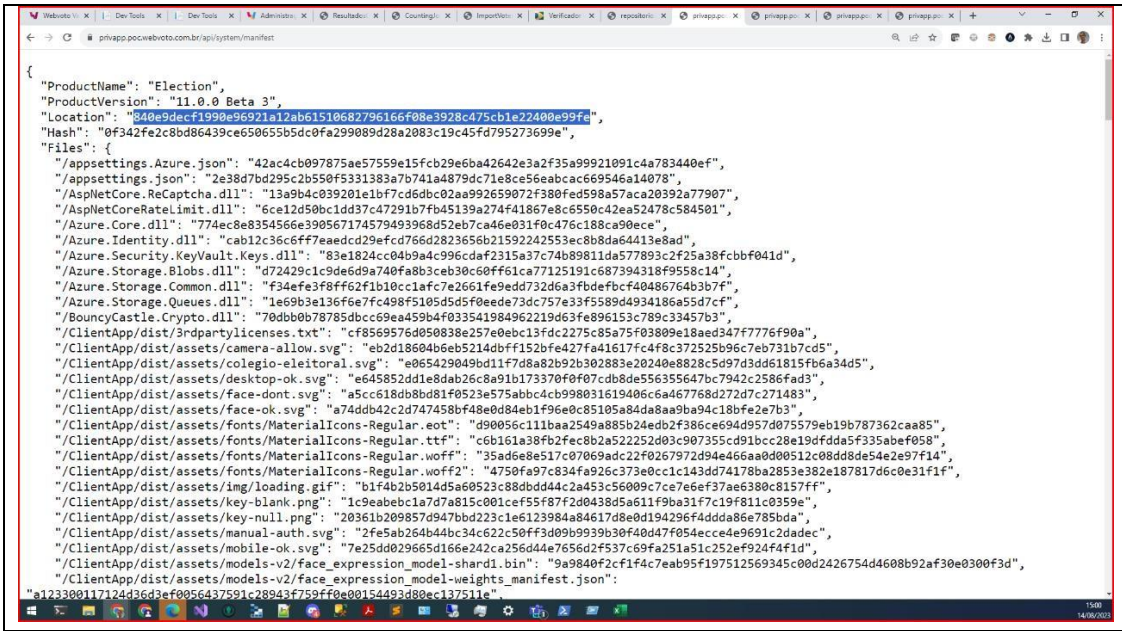
5.1.3. Disponibilidade

5.1.3.1. A solução deve conter pelo menos dois servidores web respondendo o mesmo endereço URL ou IP.

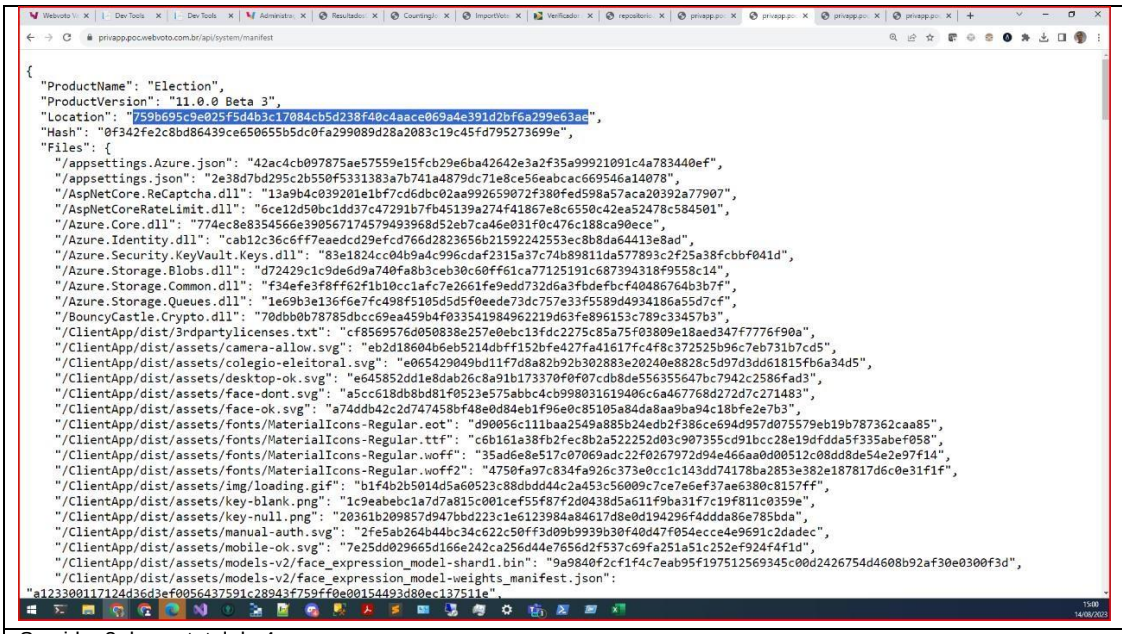



```
{
  "ProductName": "Election",
  "ProductVersion": "11.0.0 Beta 3",
  "Location": "8baf8a83df2ecd489457b5fa72fe83d046a1054e449b7e9f3ed8ffa3b2ffd4bb",
  "Hash": "0f342fe2c8bd86439ce650655b5dc0fa299089d28a2083c19c45fd795273699e",
  "Files": {
    "/appsettings.Azure.json": "42ac4cb097875ae57559e15fcb29e6ba42642e3a2f35a99921091c4a783440ef",
    "/appsettings.json": "2e38d7bd295c2b550f5331383a7b741a4879dc71e8ce56eabcac669546a14078",
    "/AspNetCore.ReCaptcha.dll": "13a9b4c039201e1bf7cd6dbc02aa992659072f380fed598a57aca20392a77907",
    "/AspNetCoreRateLimit.dll": "6ce12d50bc1dd37c47291b7fb45139a274f41867e8c6550c42ea52478c584501",
    "/Azure.Core.dll": "774ec8e8354566e3905671745794939368d52eb7ca46e031f0c476c188ca90ece",
    "/Azure.Identity.dll": "cab12c36c6ff7eaedcd29efcd766d2823656b21592242553ec8b8da64413e8ad",
    "/Azure.Security.KeyVault.Keys.dll": "83e1824cc04b9a4c996cdaf2315a37c74b89811da577893c2f25a38fcbbf041d",
    "/Azure.Storage.Blobs.dll": "d72429c1c9de6d9a740fa8b3ceb30c60ff61ca77125191c687394318f9558c14",
    "/Azure.Storage.Common.dll": "f34efe3f8ff62f1b10cc1afc7e2661fe9edd732d6a3fbdefbcf40486764b3b7f",
    "/Azure.Storage.Queues.dll": "1e69b3e136f6e7fc498f5105d5d5f0eede73dc757e33f5589d4934186a55d7cf",
    "/BouncyCastle.Crypto.dll": "70dbb0b78785dbcc69ea459b4f033541984962219d63fe896153c789c33457b3",
    "/ClientApp/dist/3rdpartylicenses.txt": "cf8569576d050838e257e0ebc13fdc2275c85a75f03809e18aed347f7776f90a",
    "/ClientApp/dist/assets/camera-allow.svg": "eb2d18604b6eb5214dbff152bfe427fa41617fc4f8c372525b96c7eb731b7cd5",
    "/ClientApp/dist/assets/colegio-eleitoral.svg": "e065429049bd11f7d8a82b92b302883e20240e8828c5d97d3dd61815fb6a34d5",
    "/ClientApp/dist/assets/desktop-ok.svg": "e645852dd1e8dab26c8a91b173370f0f07cdb8de556355647bc7942c2586fad3",
    "/ClientApp/dist/assets/face-dont.svg": "a5cc618db8bd81f0523e575abbc4cb998031619406c6a467768d272d7c271483",
    "/ClientApp/dist/assets/face-ok.svg": "a74ddb42c2d747458bf48e0d84eb1f96e0c85105a84da8aa9ba94c18bfe2e7b3",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.eot": "d90056c111baa2549a885b24edb2f386ce694d957d075579eb19b787362caa85",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.ttf": "c6b161a38fb2fec8b2a522252d03c907355cd91bcc28e19dfdda5f335abef058",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff": "35ad6e8e517c07069adc22f0267972d94e466aa0d00512c08dd8de54e2e97f14",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff2": "4750fa97c834fa926c373e0cc1c143dd74178ba2853e382e187817d6c0e31f1f",
    "/ClientApp/dist/assets/img/loading.gif": "b1f4b2b5014d5a60523c88dbdd44c2a453c56009c7ce7e6ef37ae6380c8157ff",
    "/ClientApp/dist/assets/key-blank.png": "1c9eabebc1a7d7a815c001cef55f87f2d0438d5a611f9ba31f7c19f811c0359e",
    "/ClientApp/dist/assets/key-null.png": "20361b209857d947bbd223c1e6123984a84617d8e0d194296f4ddda86e785bda",
    "/ClientApp/dist/assets/manual-auth.svg": "2fe5ab264b44bc34c622c50ff3d09b9939b30f40d47f054ecce4e9691c2dadec",
    "/ClientApp/dist/assets/mobile-ok.svg": "7e25dd029665d166e242ca256d44e7656d2f537c69fa251a51c252ef924f4f1d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-shard1.bin": "9a9840f2cf1f4c7eab95f197512569345c00d2426754d4608b92af30e0300f3d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-weights_manifest.json":
"a1233001171124d36d3ef0056437591c28943f759ff0e00154493d80ec137511e",
```

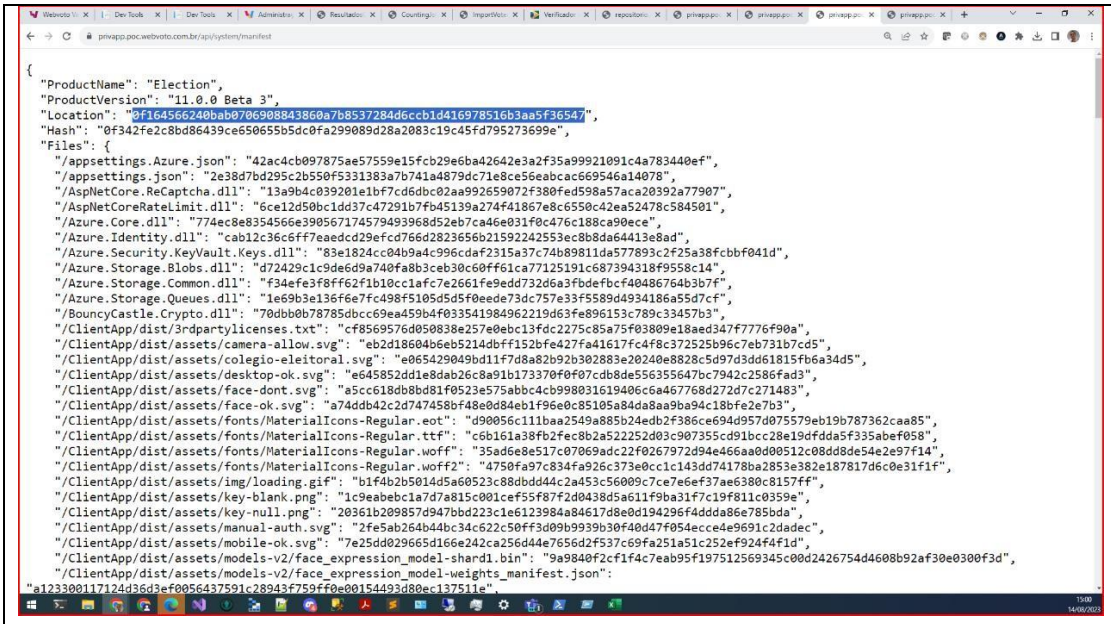

Servidor 1 de um total de 4.



Servidor 2 de um total de 4.



Servidor 3 de um total de 4.



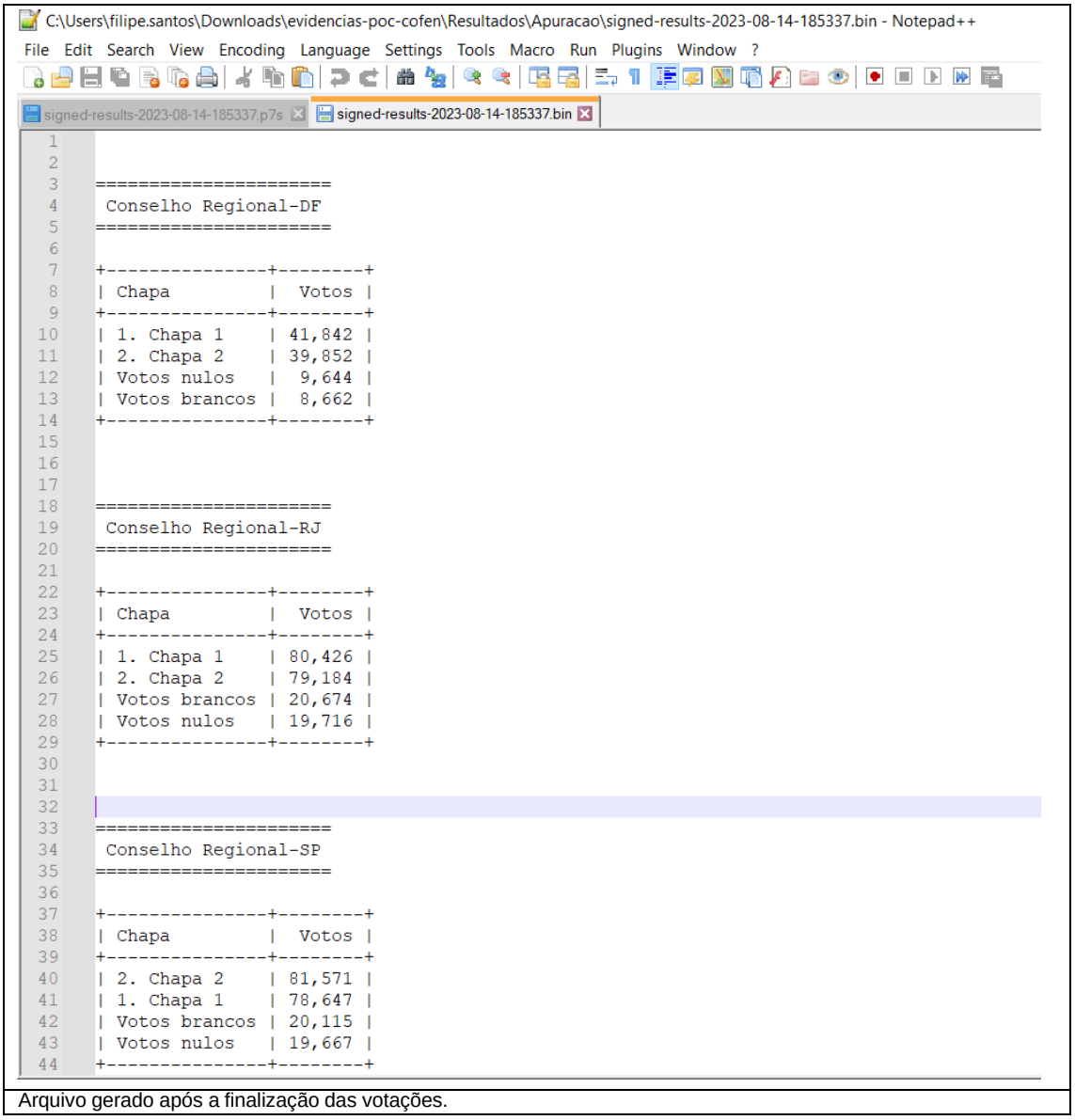
Servidor 4 de um total de 4.

5.1.4. Da aferição

5.1.4.1. O COFEN entregará à licitante, antes de iniciar a prova, o resultado esperado para confronto com o resultado obtido ao término da prova;

	A	B	C	D	E	F	G
1	UF	Eleicao	VotosChapa1	VotosChapa2	VotosBrancos	VotosNulos	Total de votos por eleição
2	DF	Conselho Regional	41842	39852	8662	9644	100000
3	RJ	Conselho Regional	80426	79184	20674	19716	200000
4	SP	Conselho Regional	78647	81571	20115	19667	200000
5	Total						500000

O resultado esperado entregue pelo COFEN.



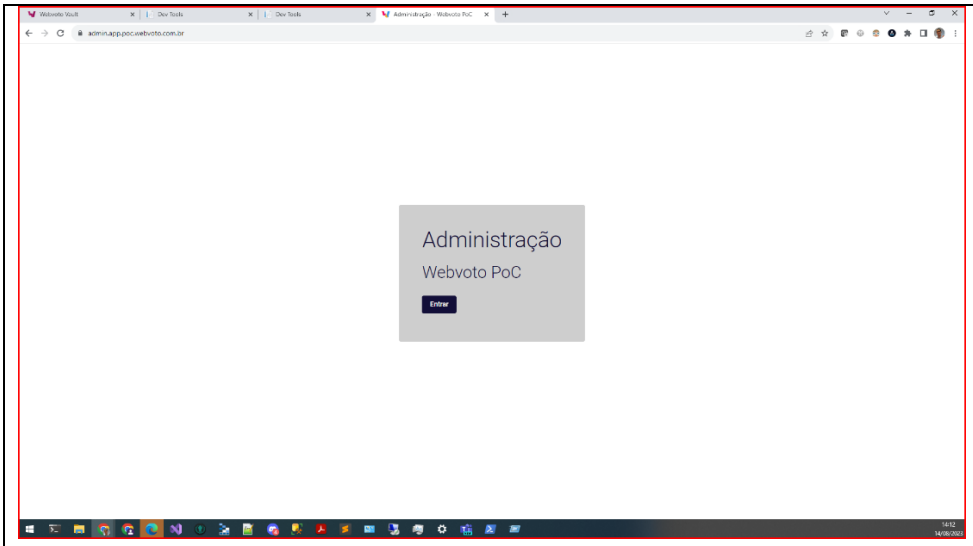
Arquivo gerado após a finalização das votações.

5.1.4.2. A empresa deverá realizar a autenticação de pelo menos três eleitores em todas as modalidades abaixo:

I - via login e senha;
II - biometria facial; e
III - certificado digital em nuvem.

Este teste foi realizado durante a prova de conceito, porém o procedimento foi realizado no celular, onde não foi possível gerar *print screens* das evidências. Porém, existem imagens gravadas da realização da eficácia destes testes.

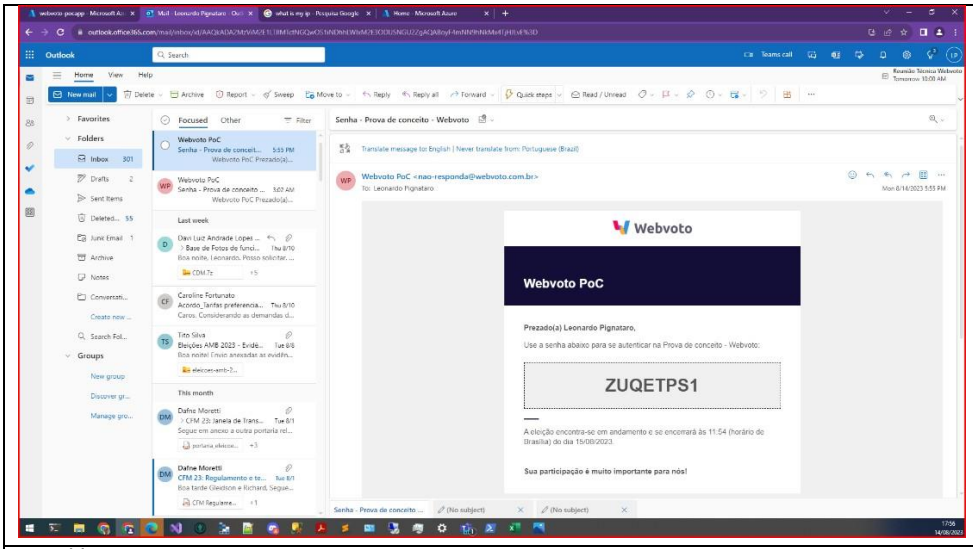
5.1.4.3. Deverá ser demonstrada a existência de um módulo de administração para importação e acompanhamento de base de dados, mediante a utilização de perfil de acesso seguro, autenticado com certificado digital, pelos responsáveis pela importação de bases de dados;



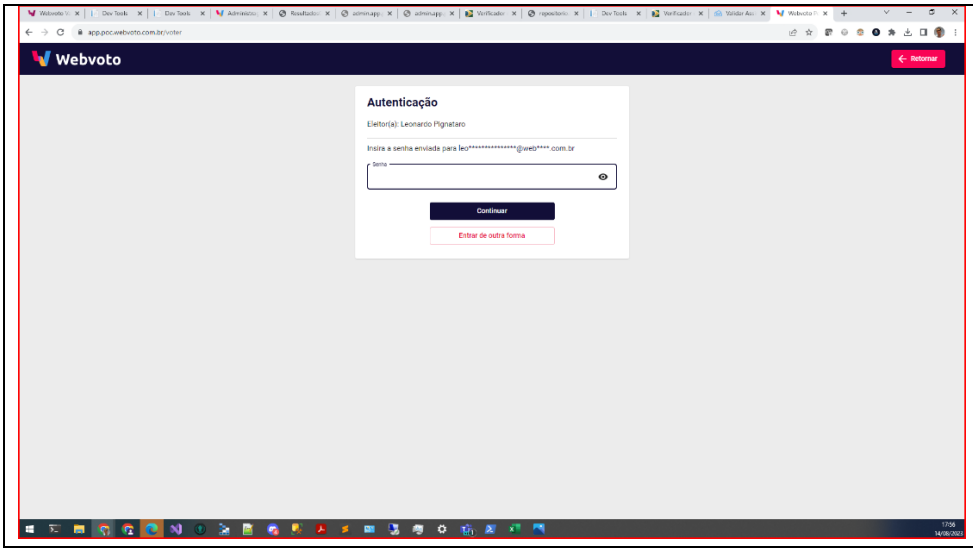
Módulo de administração do sistema Webvoto.

5.1.4.4. A solução deverá possuir interface de usuário (página *web*) que permita:

I - Recuperar o cadastro de um determinado Eleitor, apresentando informações como número de identificação e nome do eleitor;
II - Mecanismo que permita ao eleitor recuperar sua senha por meio de e-mail previamente cadastrado.



Recebimento.

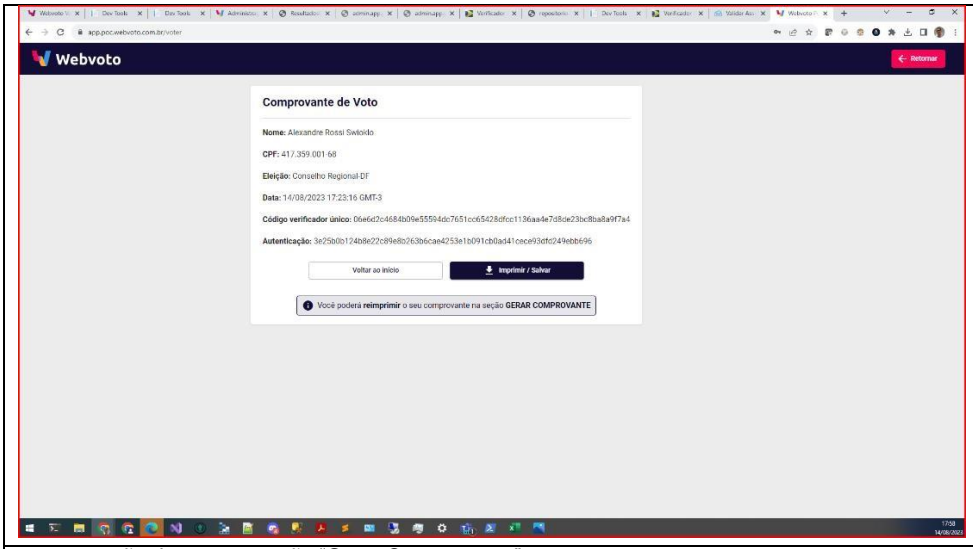


Autenticação do sistema.

III - Autenticação do eleitor através de biometria facial. Essa funcionalidade deverá ser demonstrada para, no mínimo, 12 casos com dados reais disponibilizados pelo Cofen. A solução deverá ser capaz de validar, de forma automática, a similaridade de no mínimo 10 casos.

> Resultado - Este teste foi realizado durante a prova de conceito. Porém, o procedimento foi realizado no celular, onde não foi possível gerar *print screens* das evidências. Contudo, existem imagens gravadas da realização da eficácia dos testes.

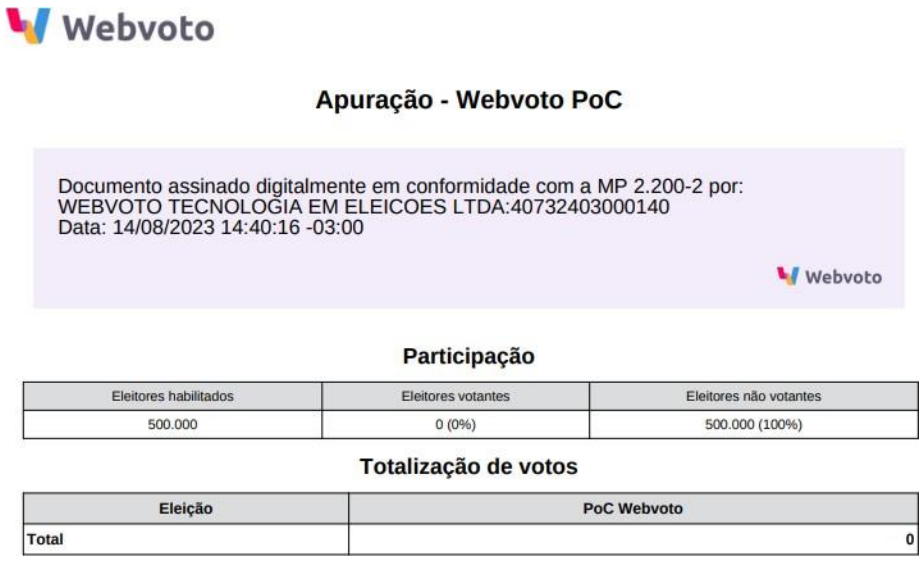
IV - Recuperar o comprovante do voto de um determinado eleitor.



Recuperação do voto na seção “Gerar Comprovante”.

5.1.4.5. Gerar relatórios assinados digitalmente conforme as normas vigentes da ICP-Brasil para:

I - Mostrar, por meio de relatório de zerézima, que a base de dados não possuía nenhum voto registrado antes do início da simulação da eleição;



Webvoto

Apuração - Webvoto PoC

Documento assinado digitalmente em conformidade com a MP 2.200-2 por:
WEBVOTO TECNOLOGIA EM ELEICOES LTDA:40732403000140
Data: 14/08/2023 14:40:16 -03:00

Webvoto

Participação

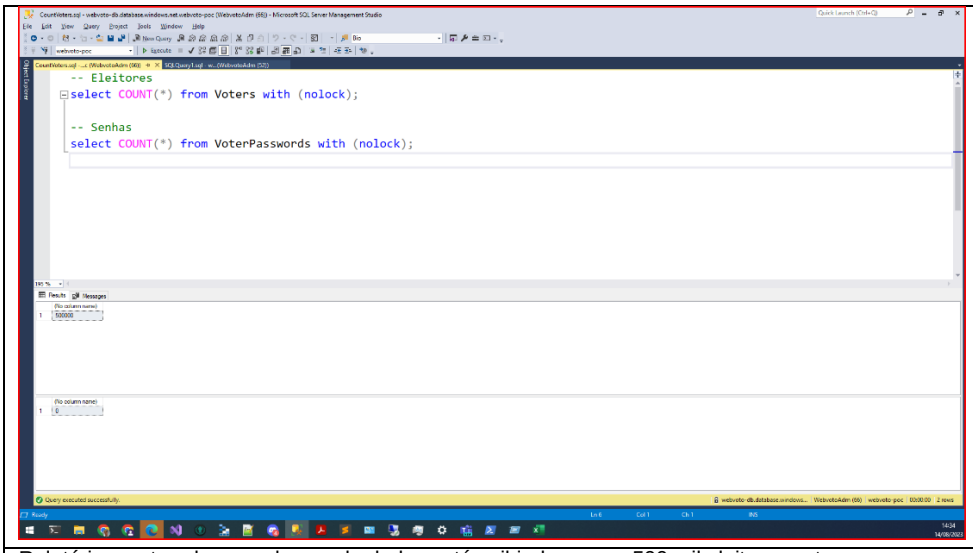
Eleitores habilitados	Eleitores votantes	Eleitores não votantes
500.000	0 (0%)	500.000 (100%)

Totalização de votos

Eleição	PoC Webvoto
Total	**0**

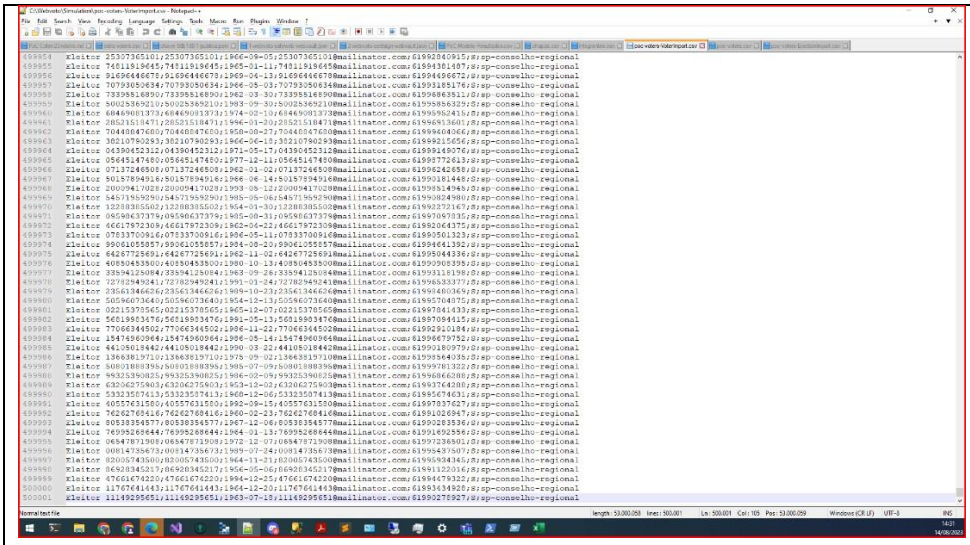
Relatório mostrando que o banco de dados está vazio.

II - Mostrar que a base de dados possuía todos os votos registrados no final da simulação da eleição;



Relatório mostrando que o banco de dados está exibindo que os 500 mil eleitores votaram.

III - Mostrar que a base de dados não possuía acesso aos votos de forma decriptada.



Votos estão encriptados.

5.1.4.6. Realizar a apuração do resultado obtido na prova de conceito de forma a:

I - Apresentar o resultado da eleição para ser comparado à base de simulação;

R - Evidência está no item 5.1.4.1.

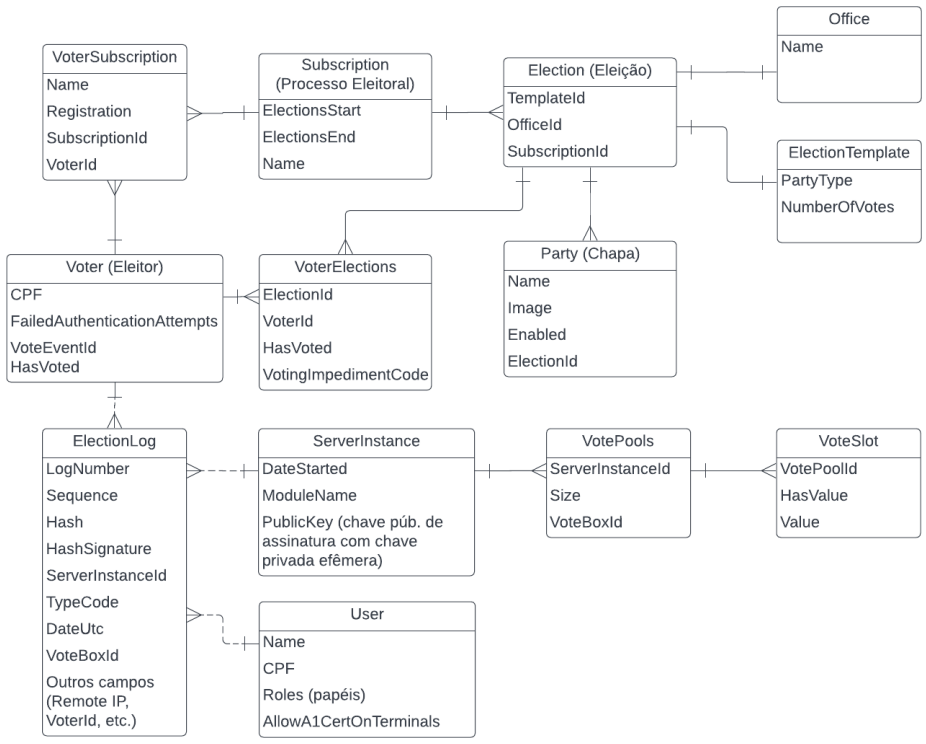
II - A apuração deverá ocorrer em equipamento separado, onde apenas a lista e votos encriptados deve ser obtida do sistema eleitoral;

R - Por exigência do edital, os votos foram encriptados com a chave pública do certificado A3 da Webvoto. Só é possível decriptar os votos tendo acesso à chave privada do certificado, a qual a Webvoto não poderá fornecer por motivos evidentes de segurança, já que se trata de um certificado ICP-Brasil válido emitido em nome da empresa.

III - Apenas este equipamento de apuração poderá ter acesso a chave privativa do certificado digital do tipo A3 emitido pelo ICP-Brasil fornecido antes do início da eleição;

R - Por exigência do edital, os votos foram encriptados com a chave pública do certificado A3 da Webvoto, só é possível decriptar os votos tendo acesso à chave privada do certificado, a qual não Webvoto não poderá fornecer por motivos evidentes de segurança, já que se trata de um certificado ICP-Brasil válido emitido em nome da empresa.

IV - A Licitante deve apresentar o projeto do sistema ou o modelo de dados do sistema ou qualquer outra informação que permita a verificação do sigilo e da unicidade de cada voto.



Modelo Entidade-Relacionamento do sistema.

6. CONCLUSÃO

Concluímos que o sistema de votação da empresa **Webvoto tecnologia em eleições ltda**, sediada em Asa Norte CLN 110 BL A Sala 203 - A - Asa Norte, Brasília - DF, 70753-510, 2ª colocada no **PREGÃO ELETRÔNICO Nº 14/2023** apresentou condições de CONFORMIDADE com os requisitos descritos no "**2.1. Demonstração prática das funcionalidades previstas por meio de procedimento automatizado"** do TERMO DE REFERÊNCIA, ANEXO B.