

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

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

SUMÁRIO

1. OBJETIVO	4
2. ESCOPO	4
3. METODOLOGIA.....	4
4. CONCEITUAÇÃO	4
4.1. OBJETO.....	4
4.2. PROCESSO ELEITORAL	4
5. ANÁLISE DE CONFORMIDADE.....	5
5.1. EVIDÊNCIAS.....	5
5.1.1. Desempenho.....	5
5.1.2. Segurança	18
5.1.3. Disponibilidade.....	29
5.1.4. Da aferição	31
6. CONCLUSÃO.....	38

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

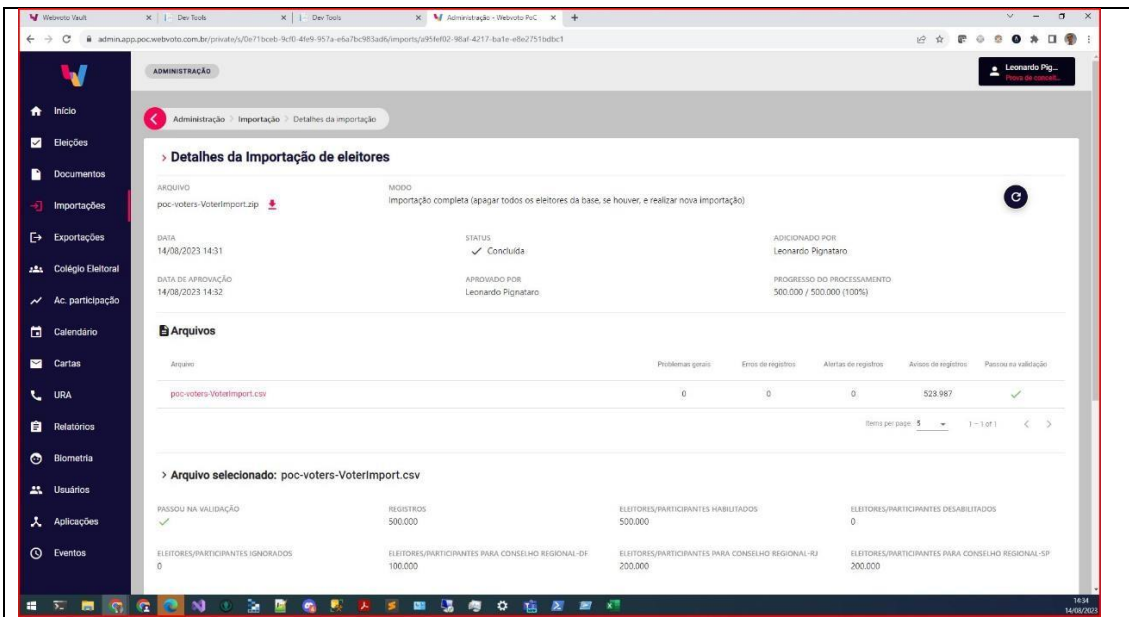
5.1. EVIDÊNCIAS

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;



The screenshot shows the 'Detalhes da Importação de eleitores' page in the Webvoto system. The page displays the following information:

- ARQUIVO:** poc-voters-Voterimport.zip
- MODO:** Importação completa (apagar todos os eleitores da base, se houver, e realizar nova importação)
- STATUS:** Concluída
- ADICIONADO POR:** Leonardo Pignataro
- DATA:** 14/08/2023 14:31
- APROVADO POR:** Leonardo Pignataro
- PROGRESSO DO PROCESSAMENTO:** 500.000 / 500.000 (100%)
- DATA DE APROVAÇÃO:** 14/08/2023 14:32

Below the details, there is a table of counts for different regions:

Arquivo	Problemas gerais	Erros de registros	Alertas de registros	Aviões de registros	Passou na validação
poc-voters-Voterimport.csv	0	0	0	523.987	✓

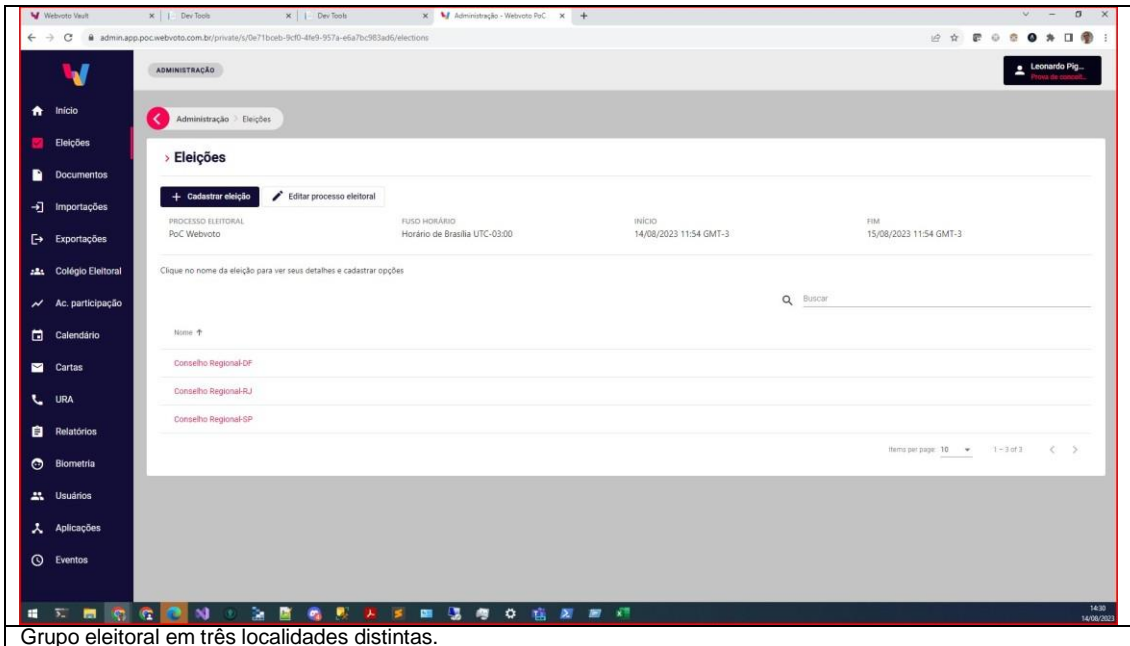
Item per page: 5 | 1 - 1 of 1

> Arquivo selecionado: poc-voters-Voterimport.csv

PASSOU NA VALIDAÇÃO	REGISTROS	ELEITORES/PARTICIPANTES HABILITADOS	ELEITORES/PARTICIPANTES DESABILITADOS
✓	500.000	500.000	0
ELEITORES/PARTICIPANTES IGNORADOS	0	ELEITORES/PARTICIPANTES PARA CONSELHO REGIONAL-DF	190.000
		ELEITORES/PARTICIPANTES PARA CONSELHO REGIONAL-RJ	200.000
		ELEITORES/PARTICIPANTES PARA CONSELHO REGIONAL-SP	200.000

14:34
14/08/2023

Importação de 500.000,00 eleitores.



ADMINISTRAÇÃO

Eleições

[+ Cadastrar eleição](#) [✎ Editar processo eleitoral](#)

PROCESSO ELEITORAL	FUSO HORÁRIO	INÍCIO	FIM
PoC Webvoto	Horário de Brasília UTC-03:00	14/08/2023 11:54 GMT-3	15/08/2023 11:54 GMT-3

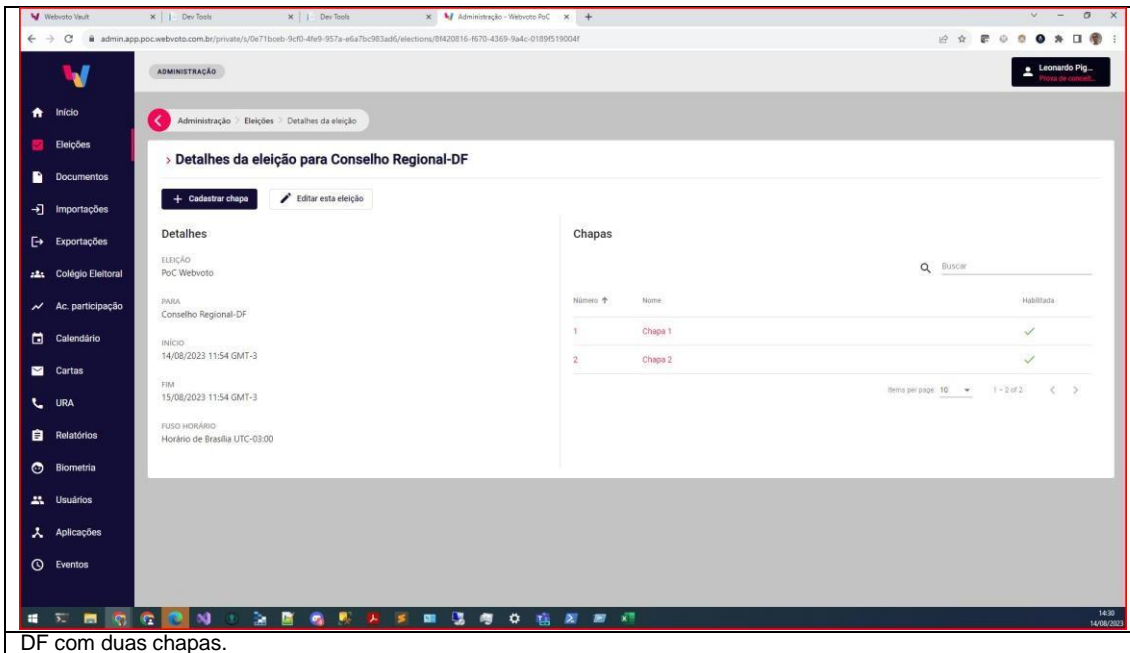
Clique no nome da eleição para ver seus detalhes e cadastrar opções

Nome ↑

- Conselho Regional-DF
- Conselho Regional-RJ
- Conselho Regional-SP

Item por página: 10 1 - 3 of 3

Grupo eleitoral em três localidades distintas.



ADMINISTRAÇÃO

Eleições > Detalhes da eleição

> Detalhes da eleição para Conselho Regional-DF

[+ Cadastrar chapa](#) [✎ Editar esta eleição](#)

Detalhes

ELEIÇÃO
PoC Webvoto

PARA
Conselho Regional-DF

INÍCIO
14/08/2023 11:54 GMT-3

FIM
15/08/2023 11:54 GMT-3

FUSO HORÁRIO
Horário de Brasília UTC-03:00

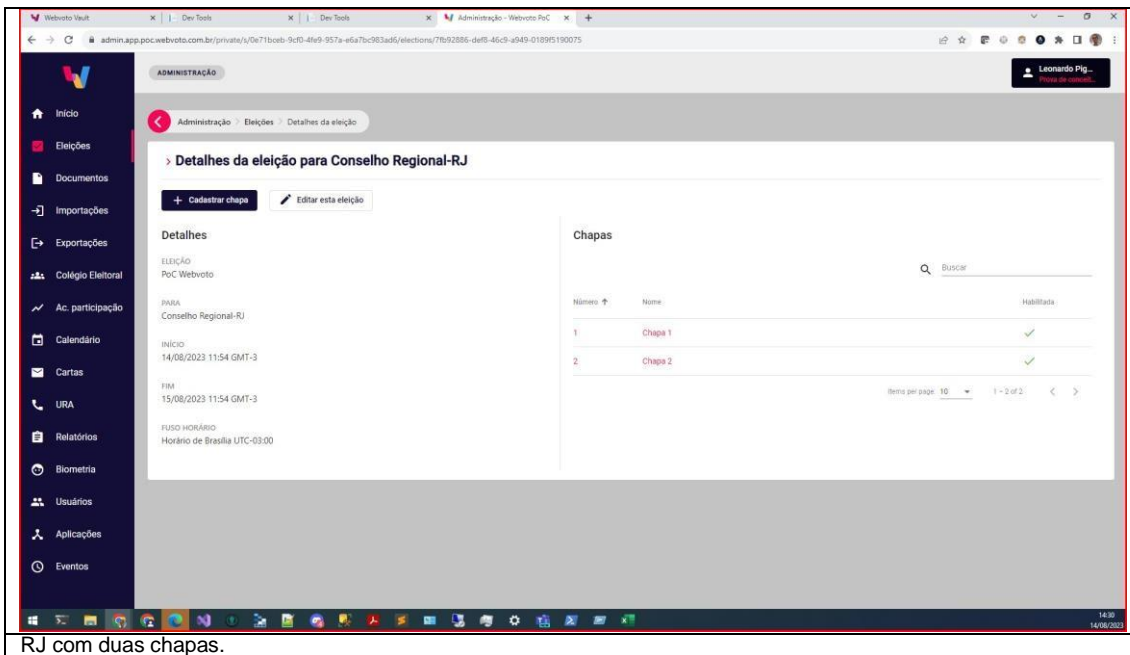
Chapas

Nome ↑

Número	Nome	Habilitada
1	Chapa 1	✓
2	Chapa 2	✓

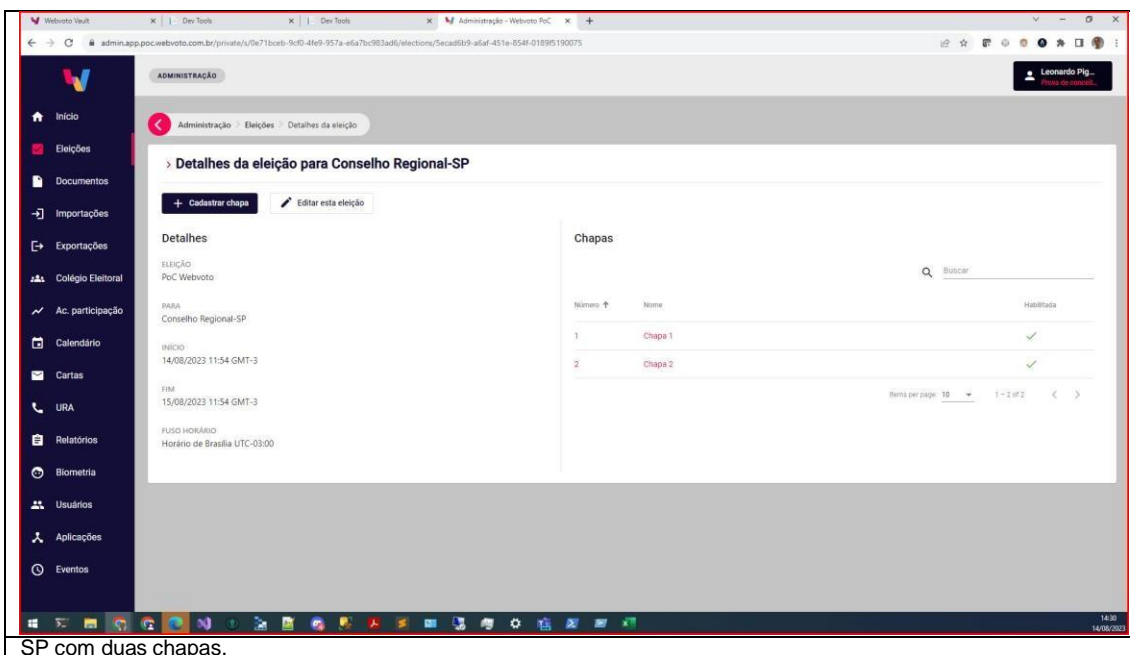
Item por página: 10 1 - 2 of 2

DF com duas chapas.



The screenshot shows the 'Detalhes da eleição para Conselho Regional-RJ' page. The left sidebar contains navigation options like 'Início', 'Eleições', 'Documentos', etc. The main content area is divided into 'Detalhes' and 'Chapas'. The 'Detalhes' section includes fields for 'ELEIÇÃO' (PoC Webvoto), 'PARA' (Conselho Regional-RJ), 'INÍCIO' (14/08/2023 11:54 GMT-3), 'FIM' (15/08/2023 11:54 GMT-3), and 'FUSO HORÁRIO' (Horário de Brasília UTC-03:00). The 'Chapas' section features a search bar and a table with two entries: 'Chapa 1' and 'Chapa 2', both with 'Habilitada' status indicated by a green checkmark.

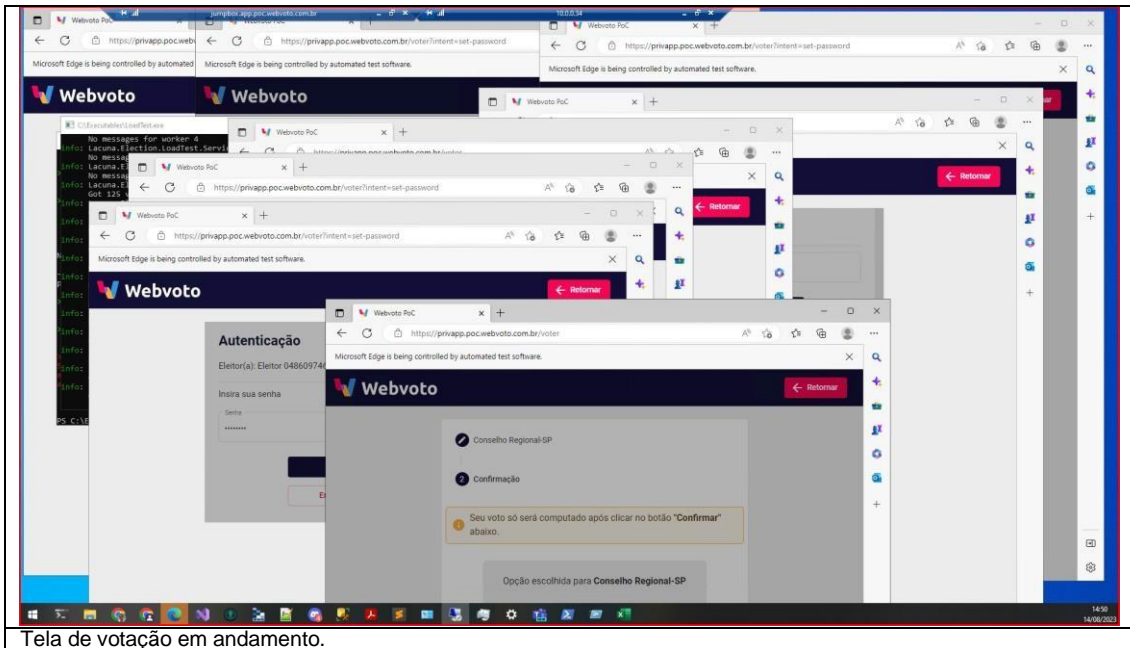
RJ com duas chapas.



The screenshot shows the 'Detalhes da eleição para Conselho Regional-SP' page. The layout is identical to the RJ version, but the 'PARA' field is set to 'Conselho Regional-SP'. The 'Chapas' table also shows two entries: 'Chapa 1' and 'Chapa 2', both with 'Habilitada' status.

SP com duas chapas.

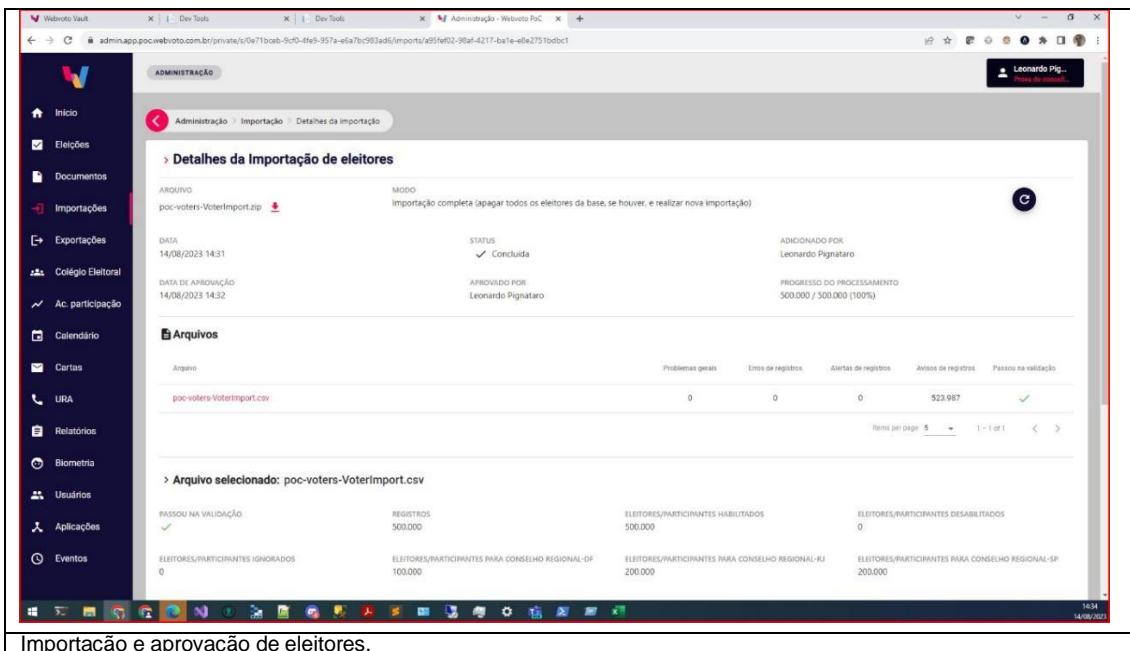
5.1.1.2. Simular uma eleição completa com o colégio eleitoral acima descrito em até duas horas ininterruptas com todos os procedimentos envolvidos, com concorrência mínima de 400 eleitores simultâneos durante o processo;



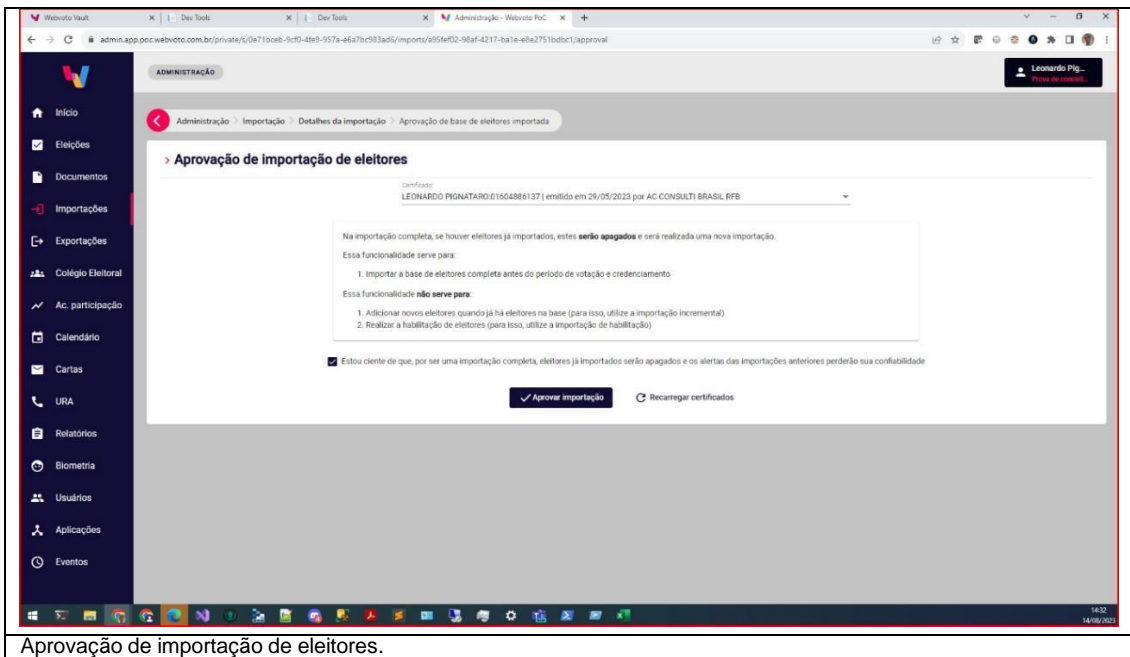
Tela de votação em andamento.

5.1.1.3. A simulação deverá:

- a) Gerar votos para cada um dos eleitores;

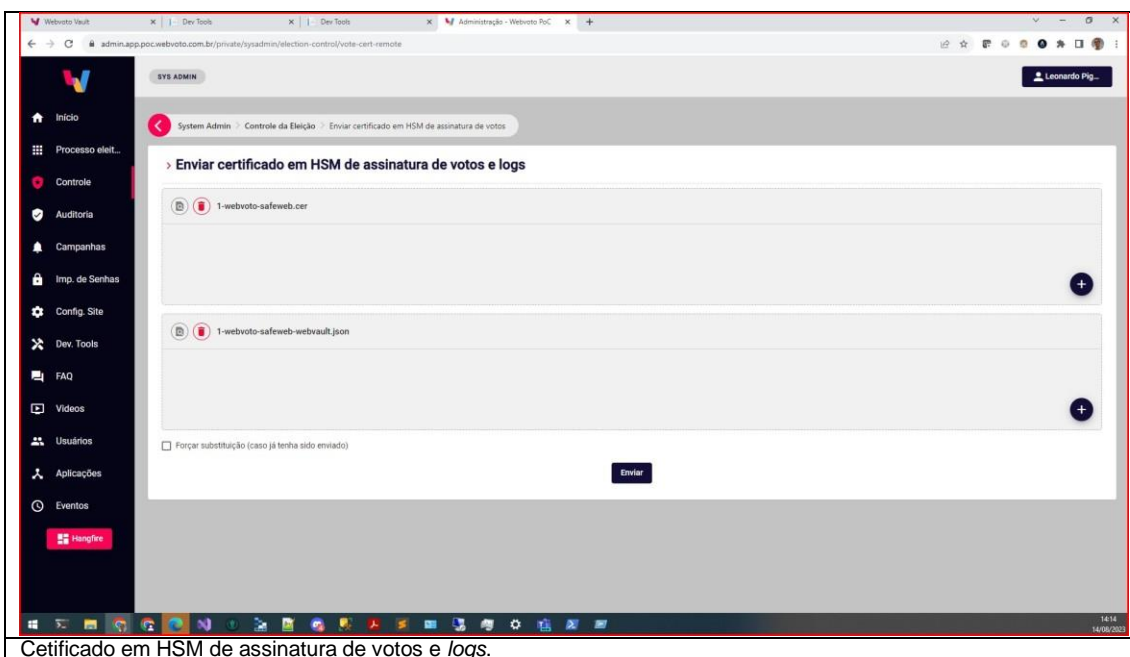


Importação e aprovação de eleitores.



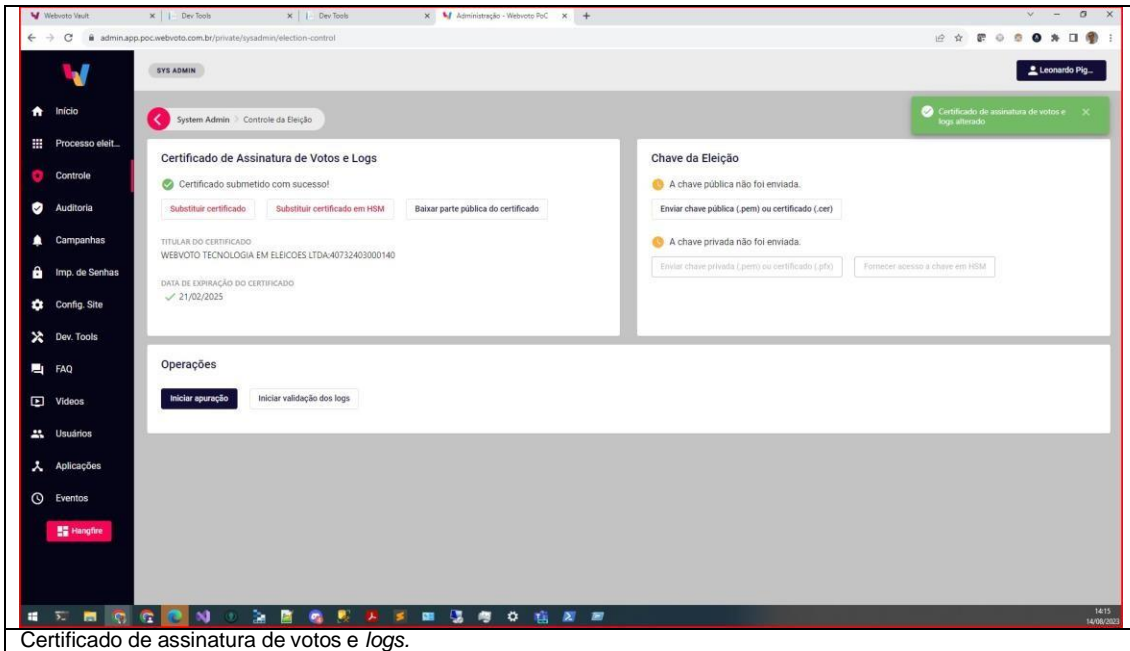
The screenshot shows a web browser window with the URL `admin.app.poc.webvoto.com.br/private/s/0e71bceb-9cd0-46f9-857a-a6a70c933ad5/imports/a95af02-98af-4217-ba1e-41e2751bd0c1/approval`. The page title is 'ADMINISTRAÇÃO' and the user is 'Leonardo Pig...'. The main content area is titled 'Aprovação de importação de eleitores' and shows a dropdown menu with the selected option 'Certificado: LEONARDO PIGNATARO:01604886137 | emitido em 29/05/2023 por AC CONSULTI BRASIL RFB'. Below this, there is a text box with instructions: 'Na importação completa, se houver eleitores já importados, estes serão apagados e será realizada uma nova importação. Essa funcionalidade serve para: 1. Importar a base de eleitores completa antes do período de votação e credenciamento. Essa funcionalidade não serve para: 1. Adicionar novos eleitores quando já há eleitores na base (para isso, utilize a importação incremental) 2. Realizar a habilitação de eleitores (para isso, utilize a importação de habilitação)'. There is a checkbox 'Estou ciente de que, por ser uma importação completa, eleitores já importados serão apagados e os alertas das importações anteriores perderão sua confiabilidade' which is checked. At the bottom, there are two buttons: 'Aprovar importação' and 'Recarregar certificados'.

Aprovação de importação de eleitores.

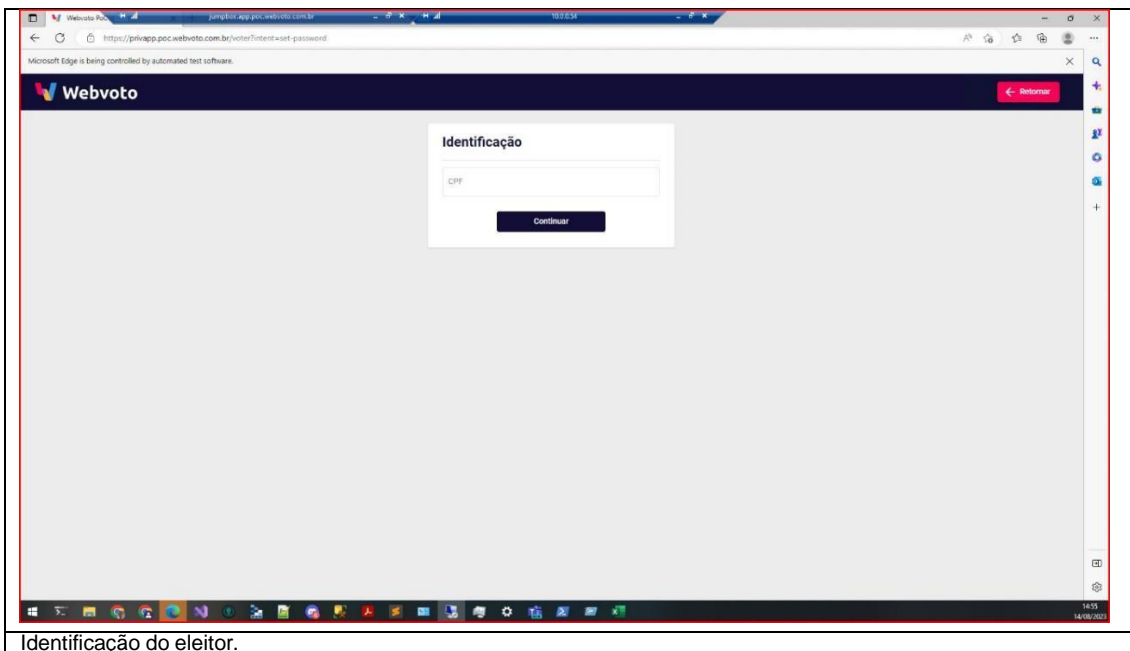


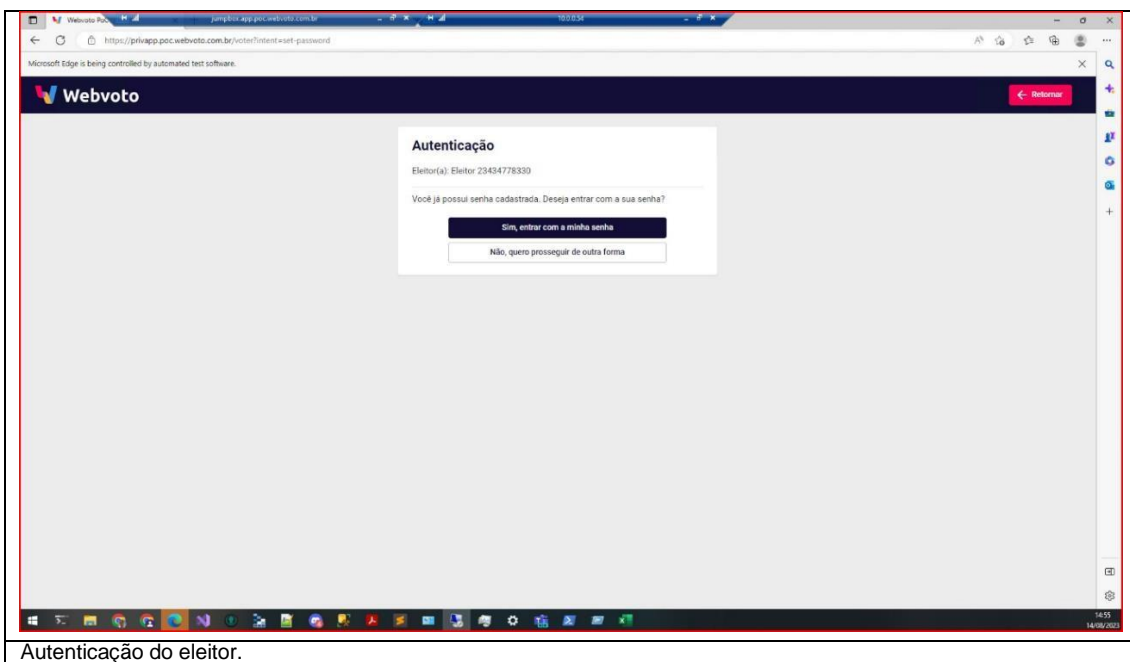
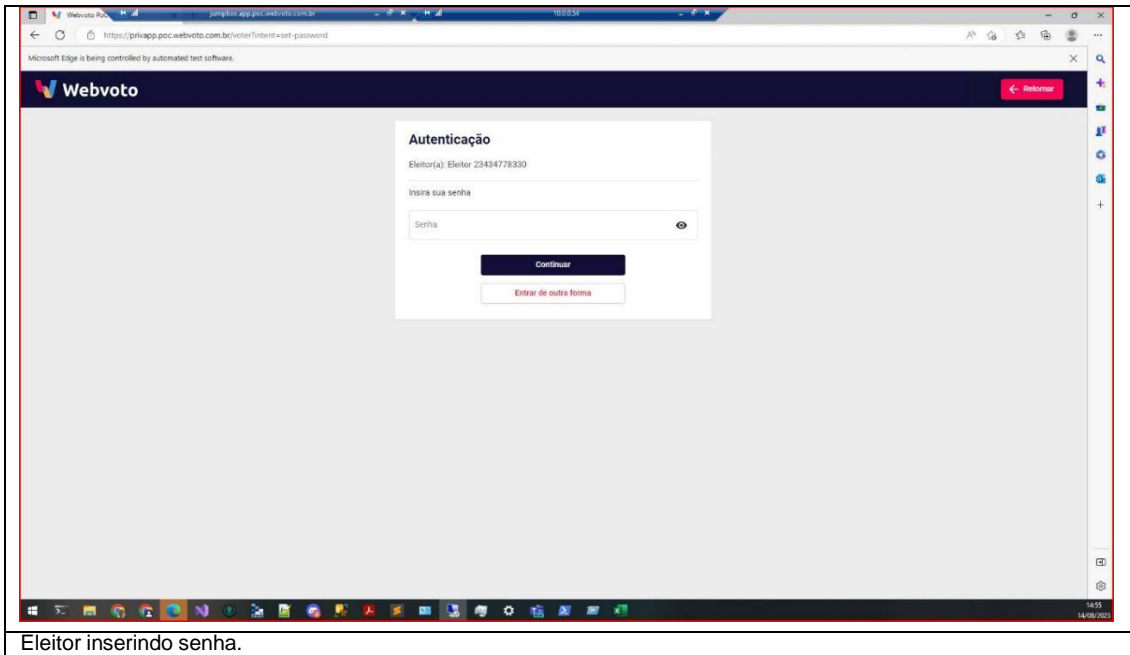
The screenshot shows a web browser window with the URL `admin.app.poc.webvoto.com.br/private/hysadmin/selection-control/vote-cert-remoto`. The page title is 'SYS ADMIN' and the user is 'Leonardo Pig...'. The main content area is titled 'Enviar certificado em HSM de assinatura de votos e logs'. It features two rows of input fields, each with a dropdown menu and a plus sign button. The first row has the value '1-webvoto-safeweb.cer' and the second row has '1-webvoto-safeweb-webvault.json'. Below these fields, there is a checkbox 'Forçar substituição (caso já tenha sido enviado)' which is unchecked. At the bottom, there is a button labeled 'Enviar'.

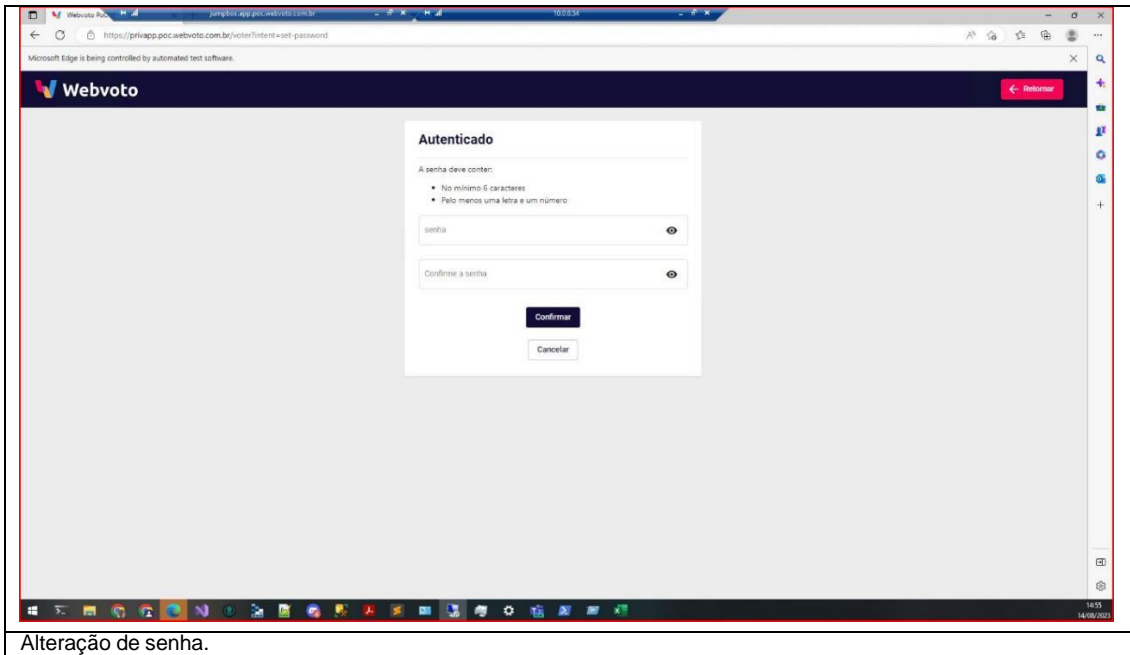
Certificado em HSM de assinatura de votos e logs.



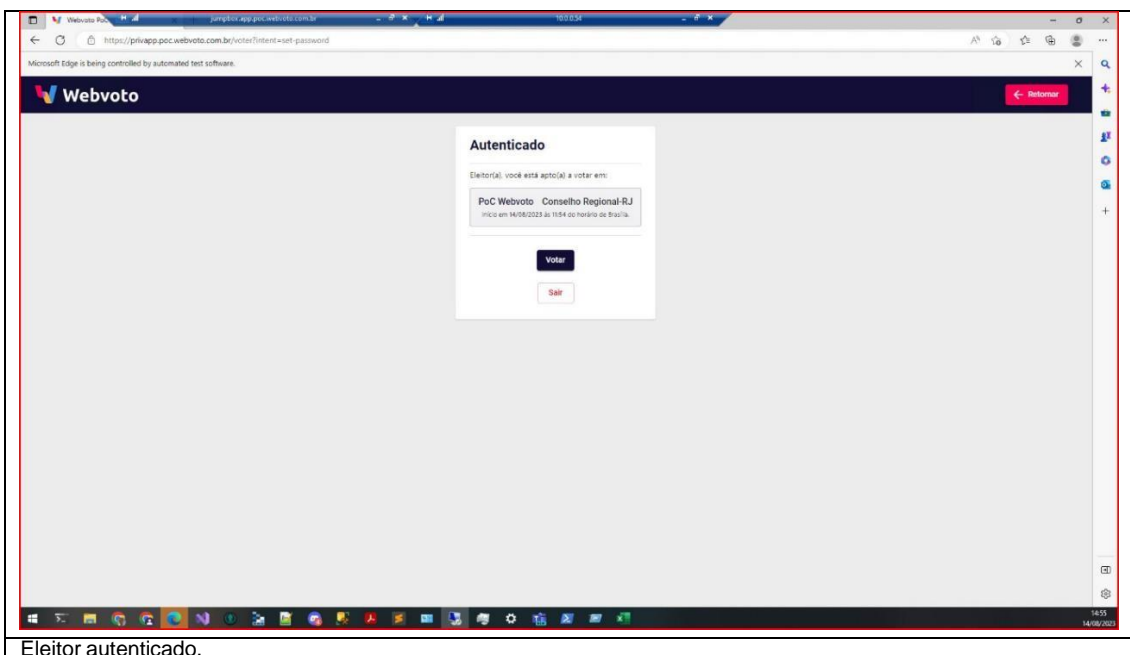
b) Realizar cada transação (votação) de forma completa, incluindo: Identificação do Eleitor, Alteração de senha, Votação com a nova senha e Emissão de comprovante eleitoral, apresentando as telas de cada operação, simulando na íntegra o comportamento do eleitor;



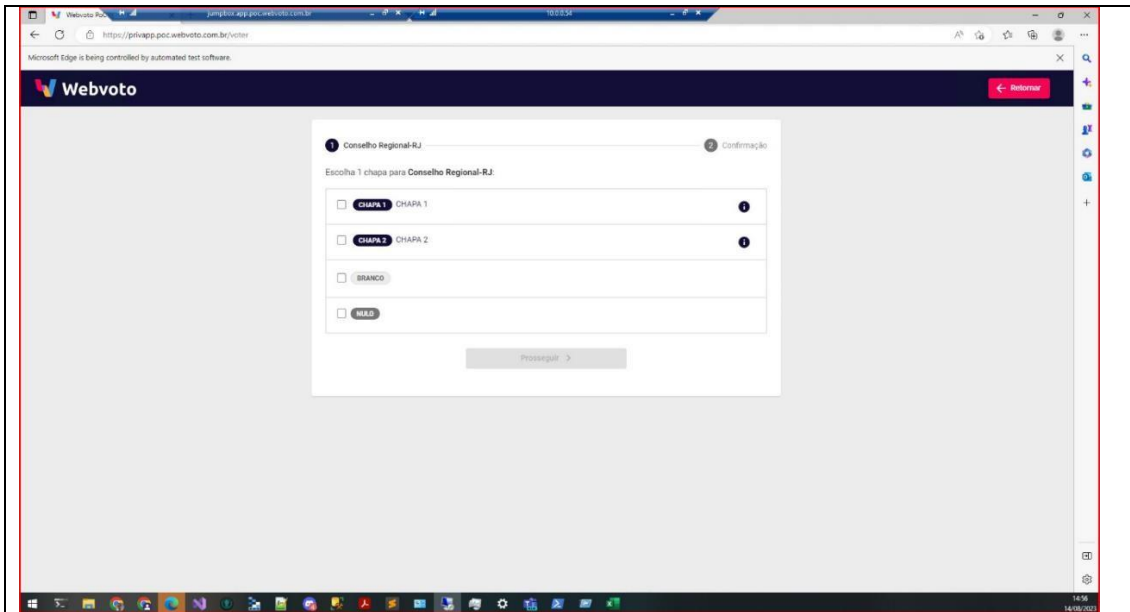




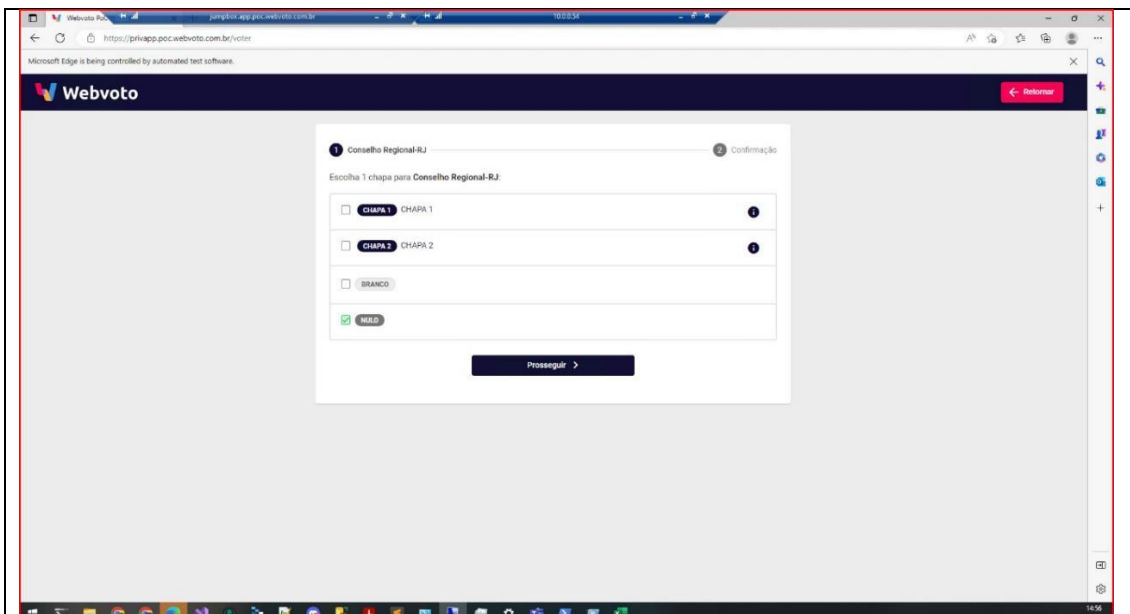
Alteração de senha.



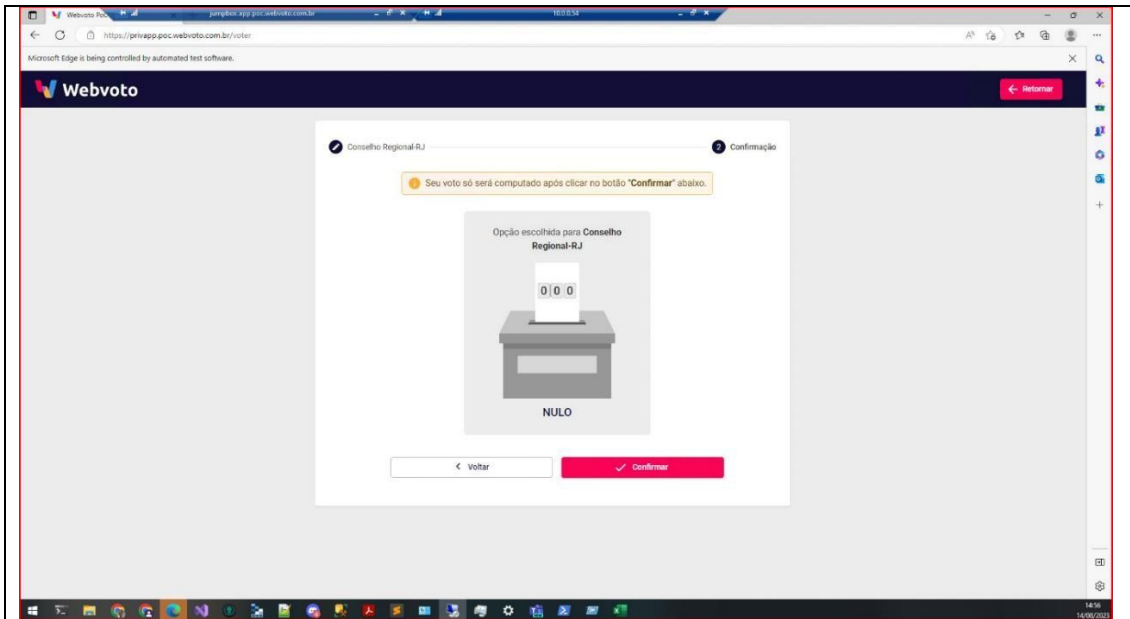
Eleitor autenticado.



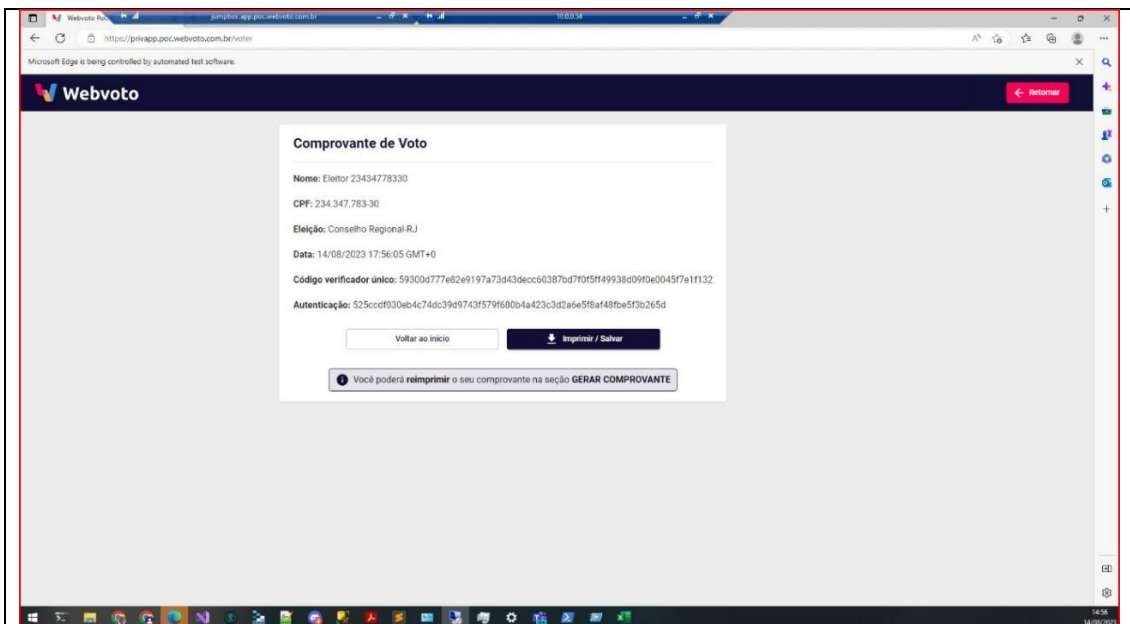
Processo de votação do eleitor.



Voto do eleitor.

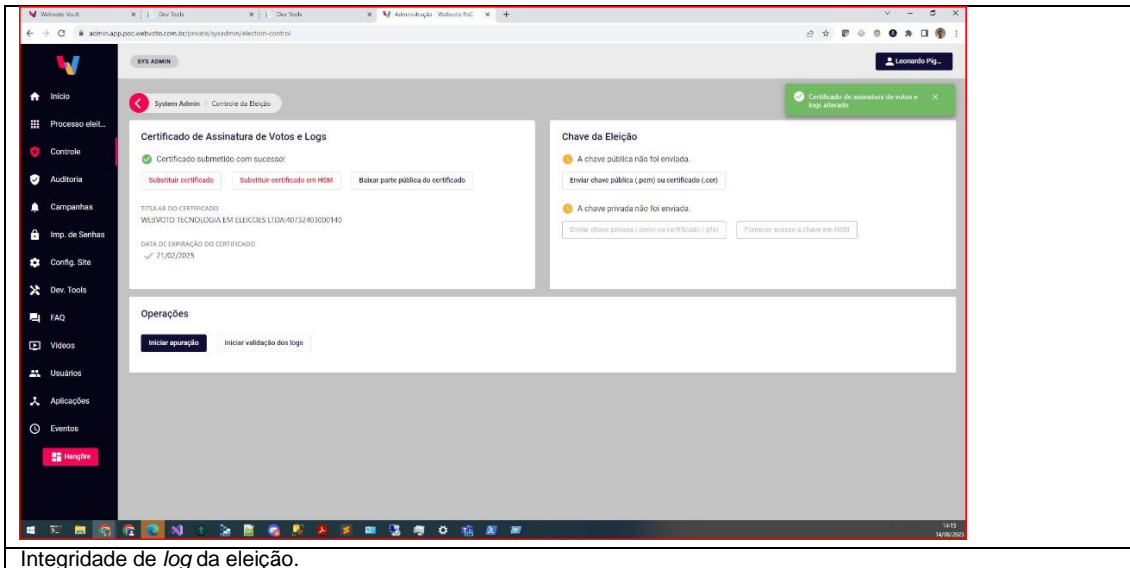


Voto nulo do eleitor.



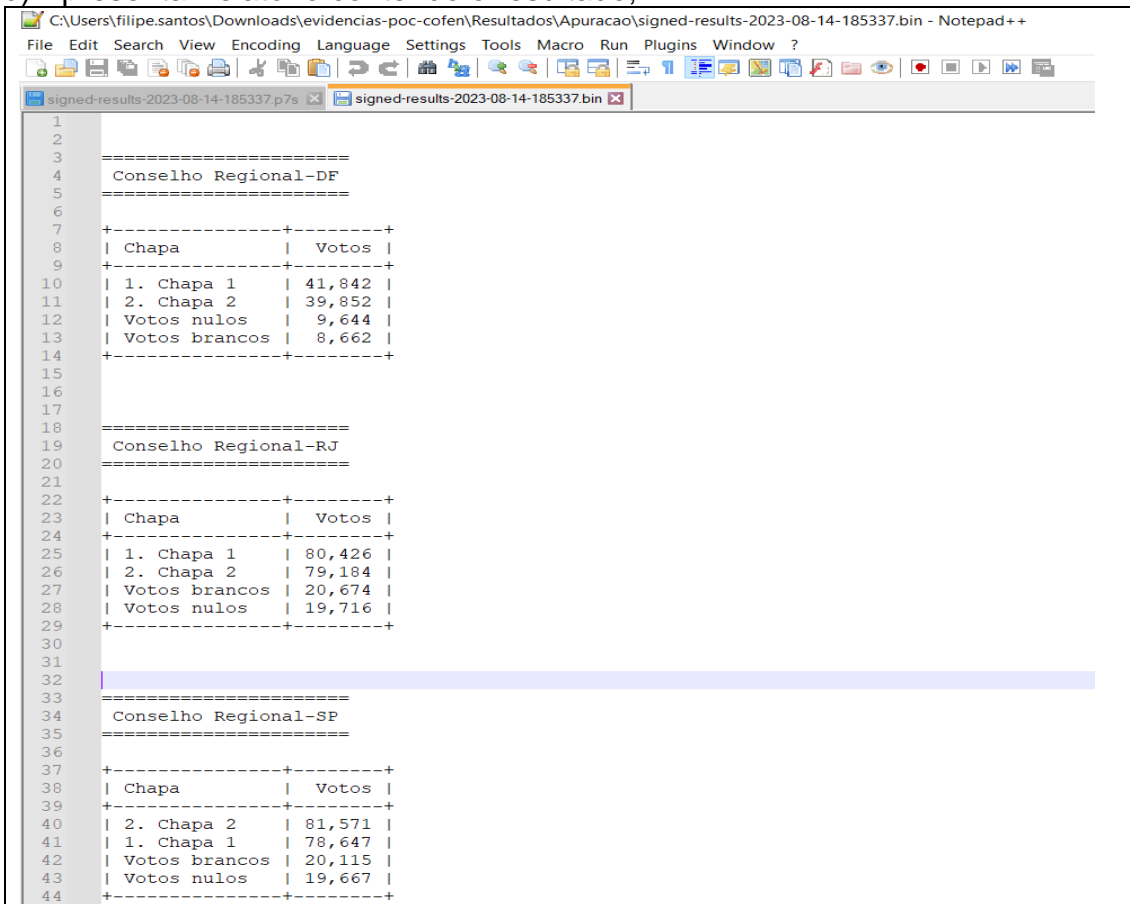
Comprovante de voto.

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



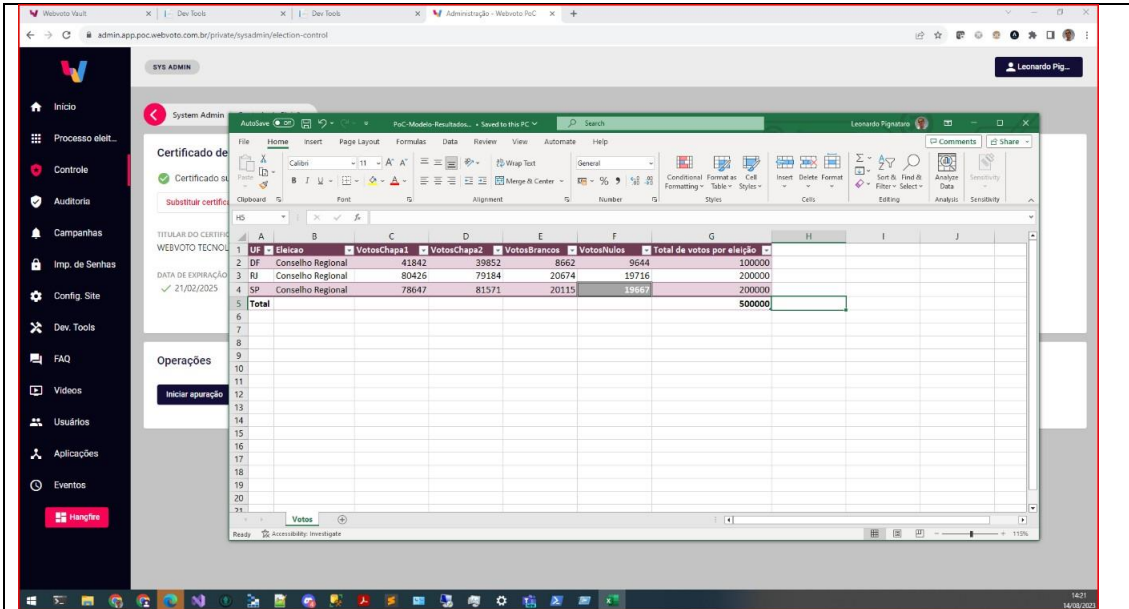
Integridade de log da eleição.

d) Apresentar relatório contendo o resultado;



Arquivo gerado após a finalização das votações.

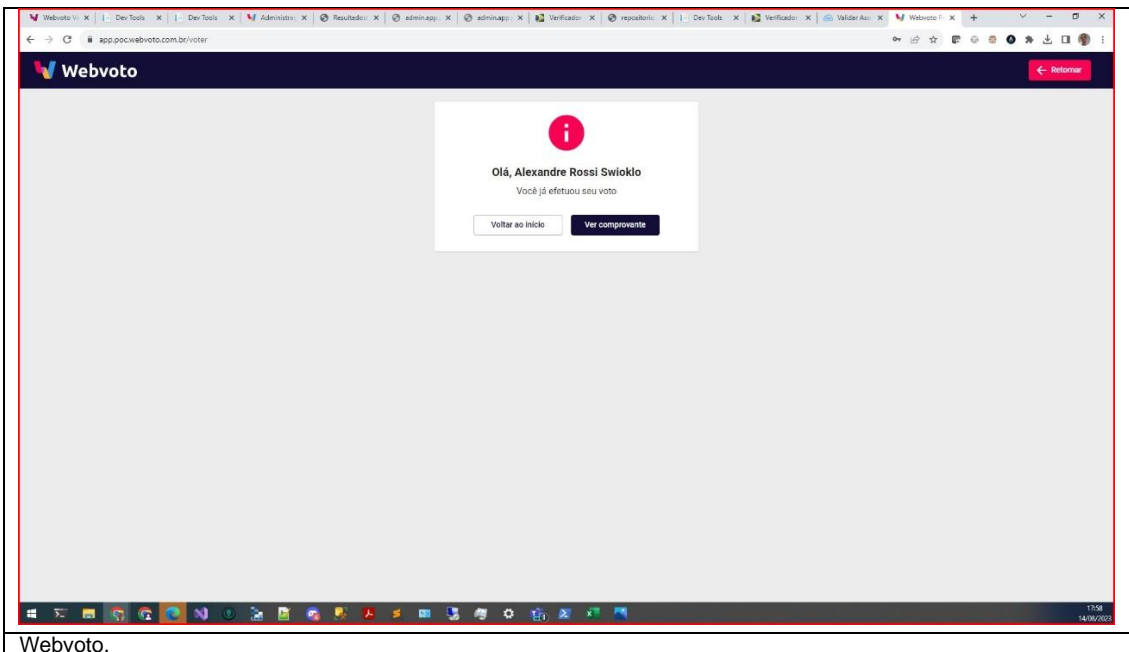
e) Deverá haver, dentre os votos gerados, votos válidos, brancos e nulos para todas as chapas;



UF	Estáncia	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:



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



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.



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



Sumário

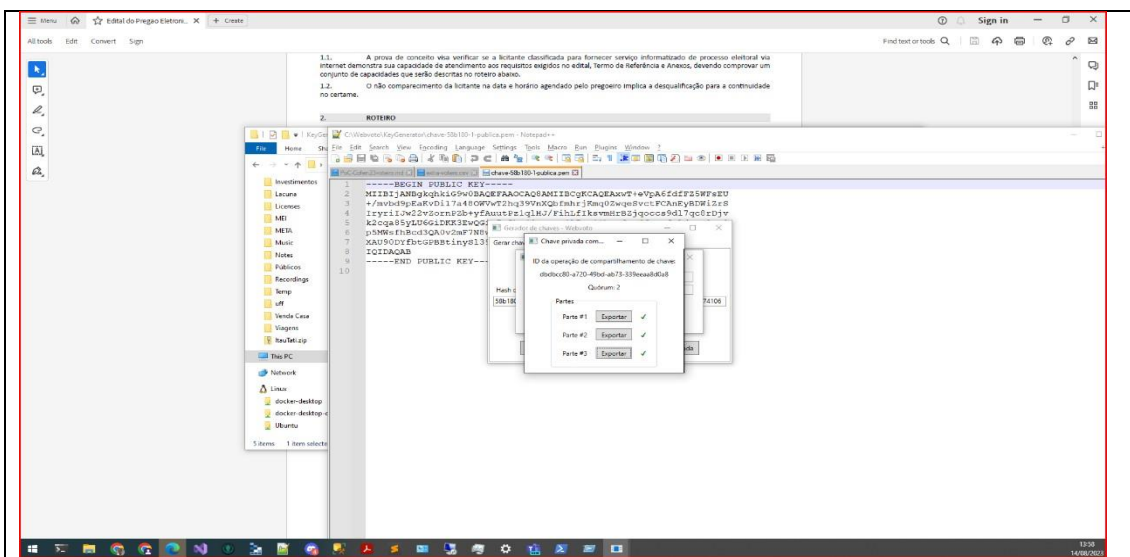
Servidor	Registros	Íntegro?	Votos
5	1	Sim	0
6	2	Sim	0
7	1	Sim	0
9	499.294	Não	124.670
10	499.939	Não	124.968
11	502.545	Sim	125.728
12	499.071	Sim	124.635
Total	2.000.853	Não	500.001

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

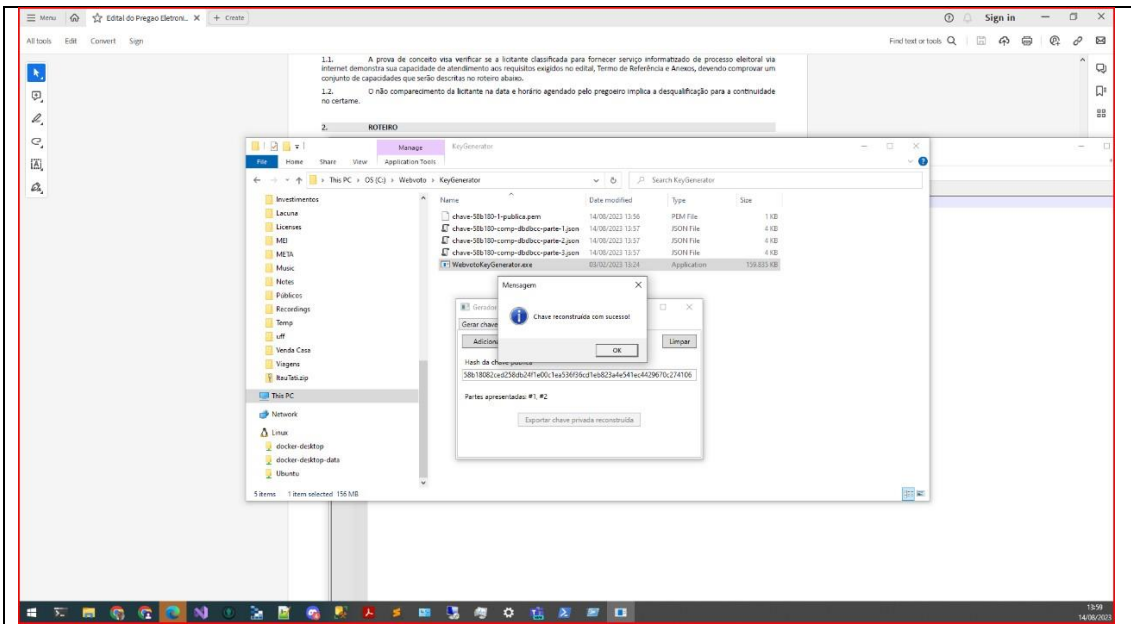
Relatório mostrando que foi acrescentado um voto no servidor 9, resultando na perda da integridade.

5.1.2. Segurança

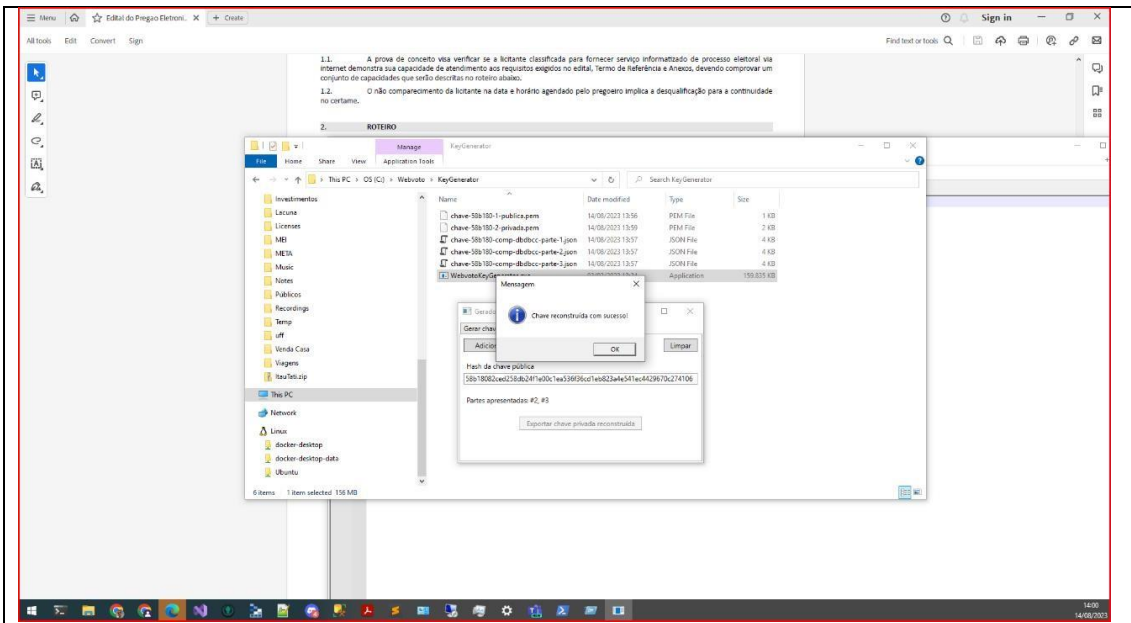
5.1.2.1. Antes do início da simulação, deve ser gerado um par de chaves padrão RSA sendo que a chave privada deve ser dividida utilizando o algoritmo Shamir Secret Sharing. A comissão julgadora poderá decidir como será feita a divisão da chave com no mínimo três partes, com duas obrigatórias.



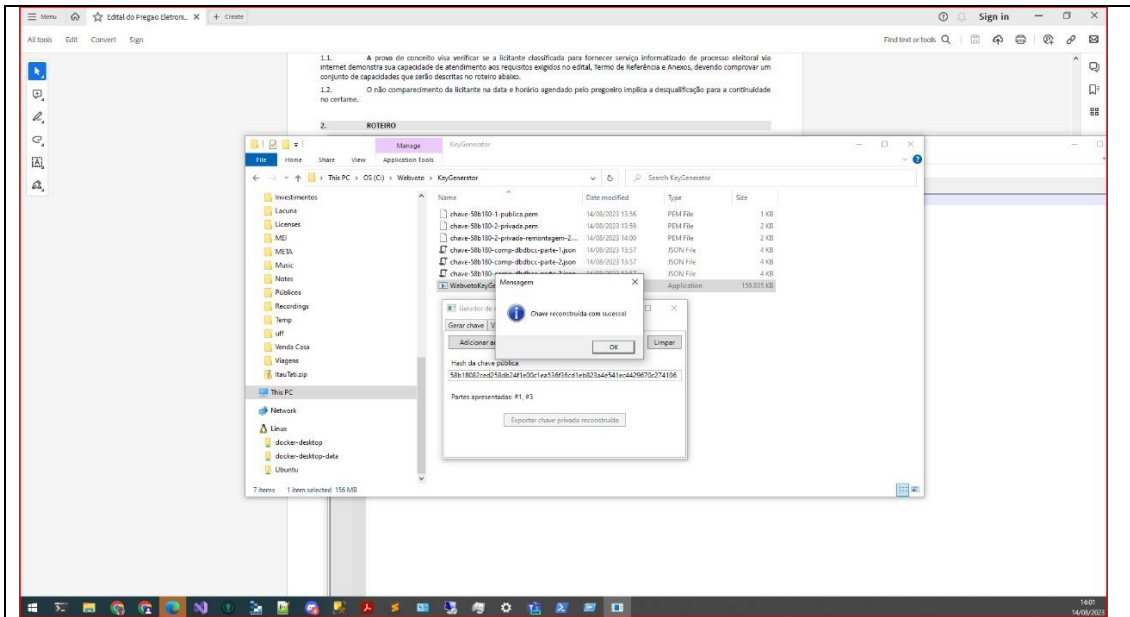
Processo de geração da chave em três segmentos distintos, sendo fundamental o emprego de duas dessas partes para viabilizar a sua reconstrução.



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

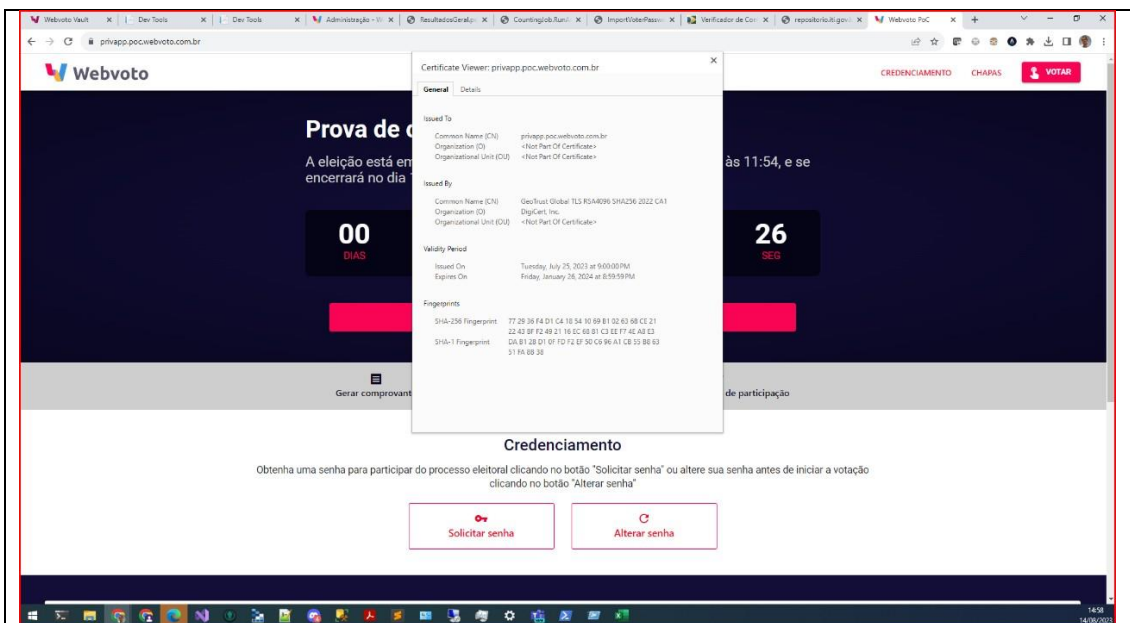


Realiza a reconstrução por meio da utilização exclusiva da Parte 2 e da Parte 3.



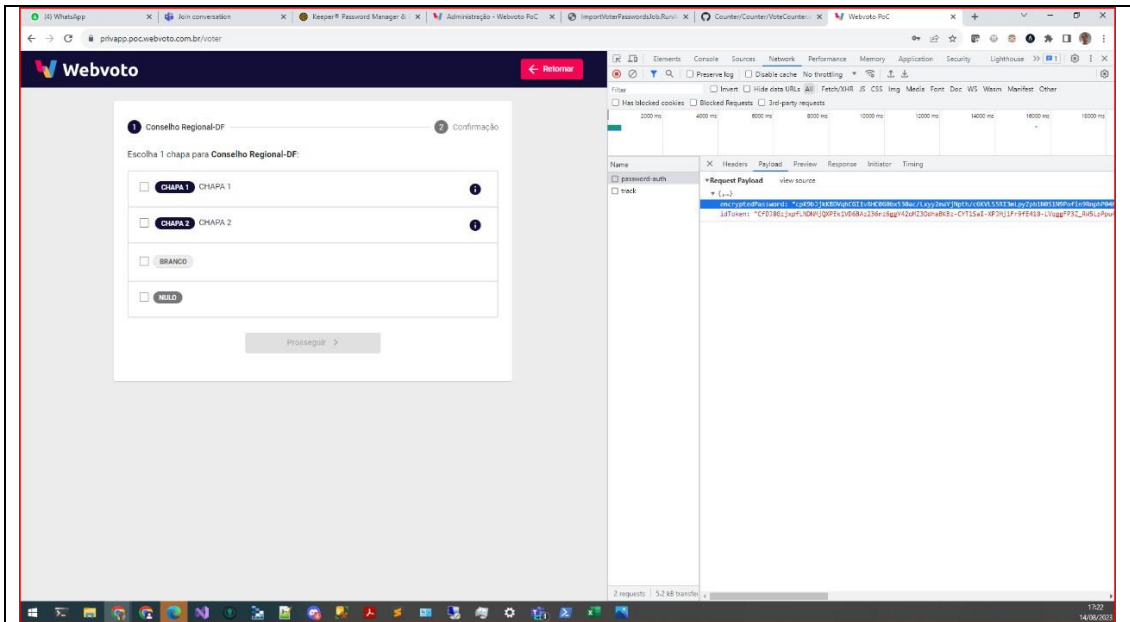
Realiza a reconstrução por meio da utilização exclusiva da Parte 1 e da Parte 3.

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



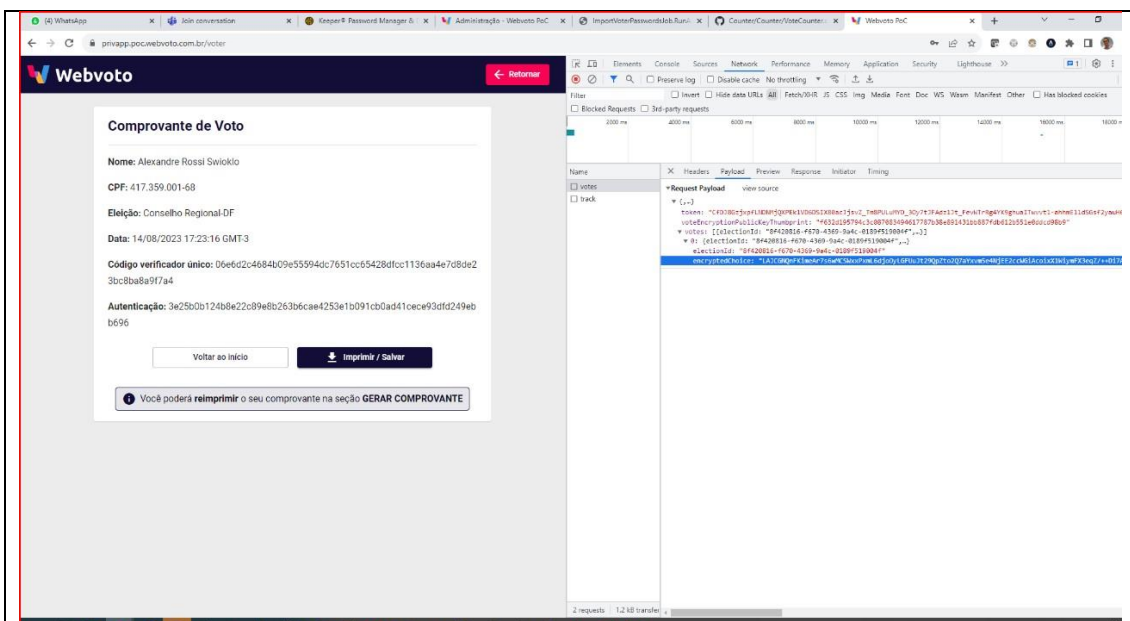
Certificado está válido.

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);



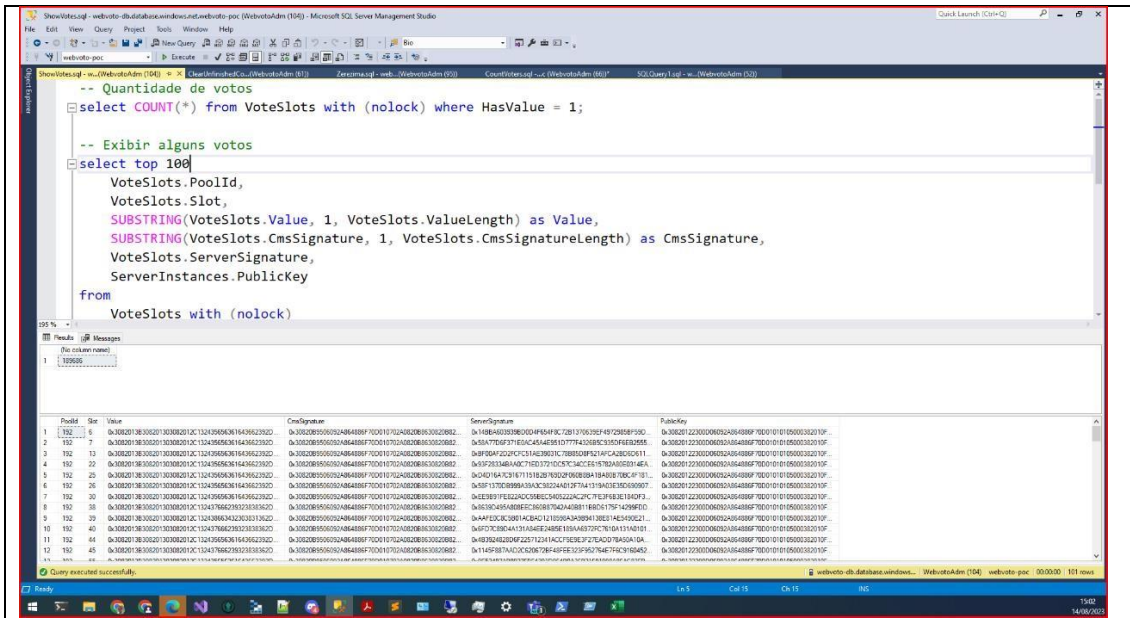
A senha se encontra submetida a um processo de criptografia.

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 encryptado 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;



```

-- Quantidade de votos
select COUNT(*) from VoteSlots with (nolock) where HasValue = 1;

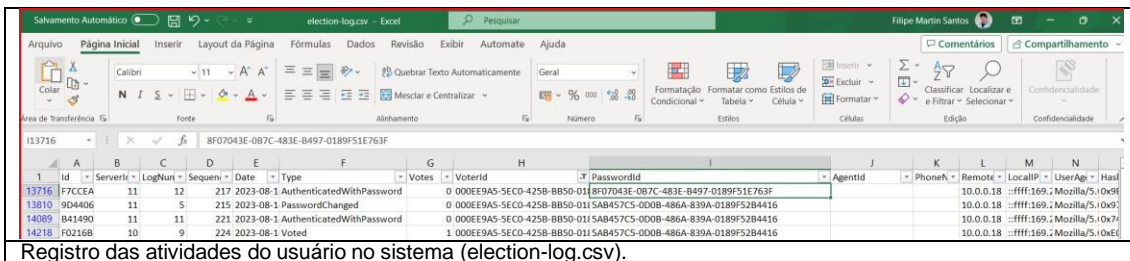
-- Exibir alguns votos
select top 100
VoteSlots.PoolId,
VoteSlots.Slot,
SUBSTRING(VoteSlots.Value, 1, VoteSlots.ValueLength) as Value,
SUBSTRING(VoteSlots.CmsSignature, 1, VoteSlots.CmsSignatureLength) as CmsSignature,
VoteSlots.ServerSignature,
ServerInstances.PublicKey
from
VoteSlots with (nolock)

```

PoolId	Slot	Value	CmsSignature	ServerSignature	PublicKey
1	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x108403038602044954937081370078974972968f930	0x308201220010000201846898f7000101010000302019f...
2	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x04307607f1e3c444480107744308050000000000000	0x308201220010000201846898f7000101010000302019f...
3	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x0f08a202f0c114e29937c7880008924fca0c05011	0x308201220010000201846898f7000101010000302019f...
4	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x107203480ac710217310257c3ac2e5780a000014e4	0x308201220010000201846898f7000101010000302019f...
5	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x021f474201e11918207020f00000000000000000000	0x308201220010000201846898f7000101010000302019f...
6	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x0f1170c0899a3a3c30244e13f71a119140e03000007	0x308201220010000201846898f7000101010000302019f...
7	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x0e98f1f822cc0580c4032242c7c7f3f83e1840f3	0x308201220010000201846898f7000101010000302019f...
8	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x030004040000000000000000000000000000000000	0x308201220010000201846898f7000101010000302019f...
9	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0xaaff0c0c00814c8a01210209a4080013081a0540021	0x308201220010000201846898f7000101010000302019f...
10	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x07070804411404248485180440570c76da1140101	0x308201220010000201846898f7000101010000302019f...
11	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x0300040400000000000000000000000000000000	0x308201220010000201846898f7000101010000302019f...
12	192	0x000018030020130000201c11a396563616496239202	0x3002080500124844889f700010702402080103020802	0x114828f0c0c00078f8f000120f95704270003162452	0x308201220010000201846898f7000101010000302019f...

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;



Id	ServerId	LogNum	Sequen	Date	Type	Votes	VoterId	PasswordId	AgentId	PhoneN	Remote	LocalIP	UserAg	Host
13716	F7CEA	11	5	215 2023-08-1	AuthenticatedWithPassword	0	000EE9A5-5ECO-4258-B850-018F07043E-0B7C-483E-8497-0189F51E763F				10.0.0.18	::ffff:169.;	Mozilla/5.0	0x0
13810	9D4406	11	5	215 2023-08-1	PasswordChanged	0	000EE9A5-5ECO-4258-B850-018F07043E-0B7C-483E-8497-0189F51E763F				10.0.0.18	::ffff:169.;	Mozilla/5.0	0x9
14089	B41490	11	11	221 2023-08-1	AuthenticatedWithPassword	0	000EE9A5-5ECO-4258-B850-018F07043E-0B7C-483E-8497-0189F51E763F				10.0.0.18	::ffff:169.;	Mozilla/5.0	0x7
14218	F02168	10	9	224 2023-08-1	Voted	1	000EE9A5-5ECO-4258-B850-018F07043E-0B7C-483E-8497-0189F51E763F				10.0.0.18	::ffff:169.;	Mozilla/5.0	0x6


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;



Verificação de integridade do log das eleições

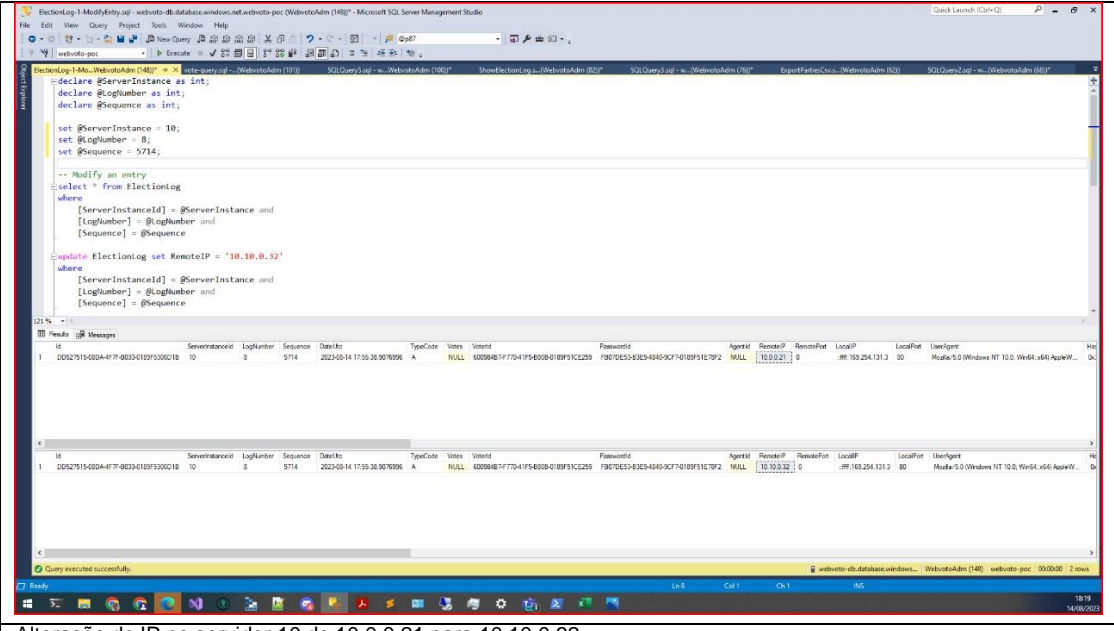
Documento assinado digitalmente em conformidade com a MP 2.200-2 por:
WEBVOTO TECNOLOGIA EM ELEICOES LTDA:40732403000140
 Data: 14/08/2023 18:17:04 -03:00



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



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 íntegro.

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 íntegro.

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 íntegro.

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.



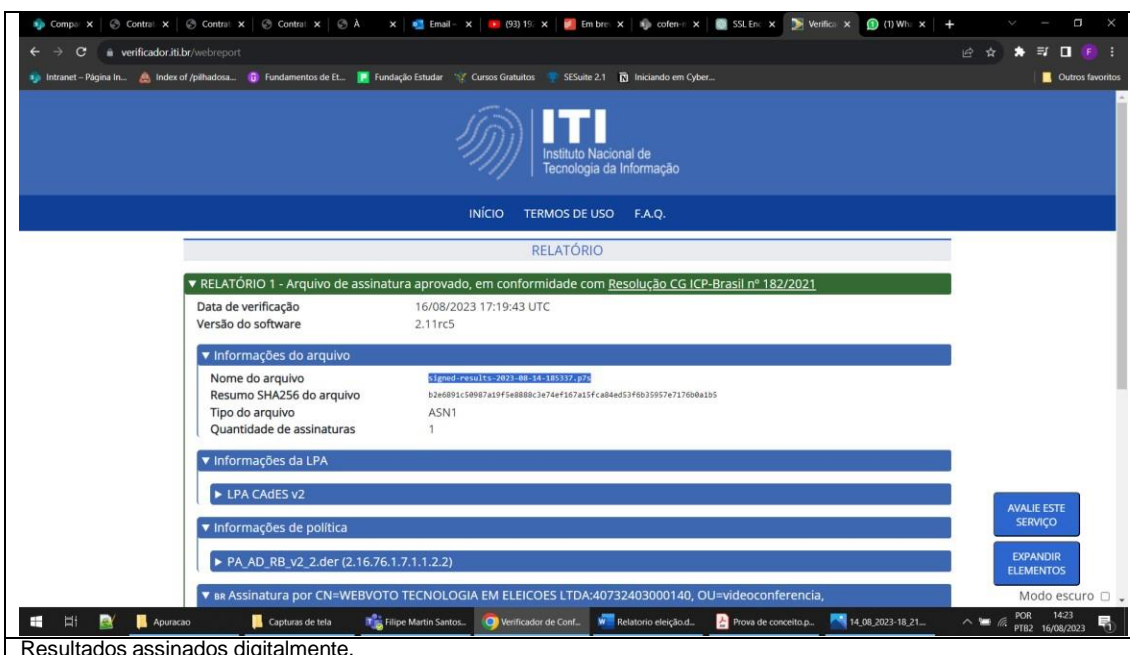
Assinatura digital dos votos.

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;

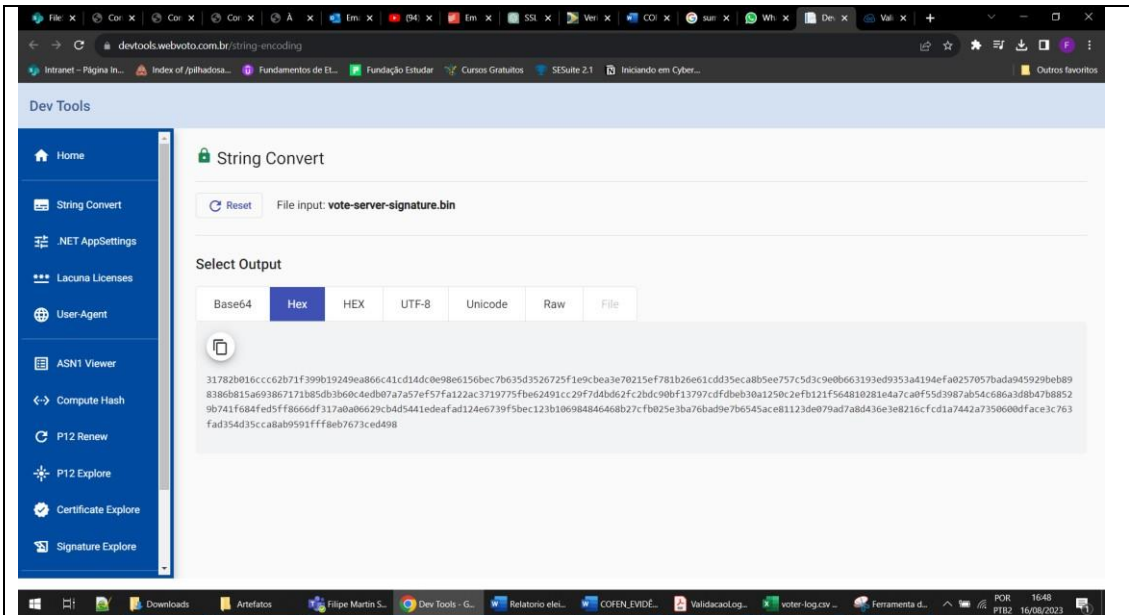
<input type="checkbox"/> 4f22928c-881d-40e3-9f82-25e7f40bfb7c.bin	14/08/2023 17:39	Arquivo BIN	1 KB
<input type="checkbox"/> 4f22928c-881d-40e3-9f82-25e7f40bfb7c.p7s	14/08/2023 17:39	Assinatura PKCS nº...	77 KB
<input type="checkbox"/> 012-001-5718.p7s	14/08/2023 17:30	Assinatura PKCS nº...	3 KB
<input type="checkbox"/> 259e18e6-be32-420f-90c0-36c863377759.bin	14/08/2023 17:35	Arquivo BIN	1 KB
<input type="checkbox"/> 259e18e6-be32-420f-90c0-36c863377759.p7s	14/08/2023 17:35	Assinatura PKCS nº...	77 KB
<input type="checkbox"/> converted-1692045118494.bin	14/08/2023 17:32	Arquivo BIN	1 KB
ResultadosGeral.pdf	14/08/2023 14:40	Documento do Ad...	256 KB
<input type="checkbox"/> signed-results-2023-08-14-185337.bin	14/08/2023 15:57	Arquivo BIN	1 KB
<input type="checkbox"/> 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
<input type="checkbox"/> vote-cms-signature.p7s	14/08/2023 15:06	Assinatura PKCS nº...	3 KB
<input type="checkbox"/> vote-server-public-key.bin	14/08/2023 15:08	Arquivo BIN	1 KB
<input type="checkbox"/> vote-server-signature.bin	14/08/2023 15:08	Arquivo BIN	1 KB
<input type="checkbox"/> vote-value.bin	14/08/2023 15:06	Arquivo BIN	1 KB

Todos os artefatos possuem assinaturas validas.

5.1.2.10. Demonstrar 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.



String Convert

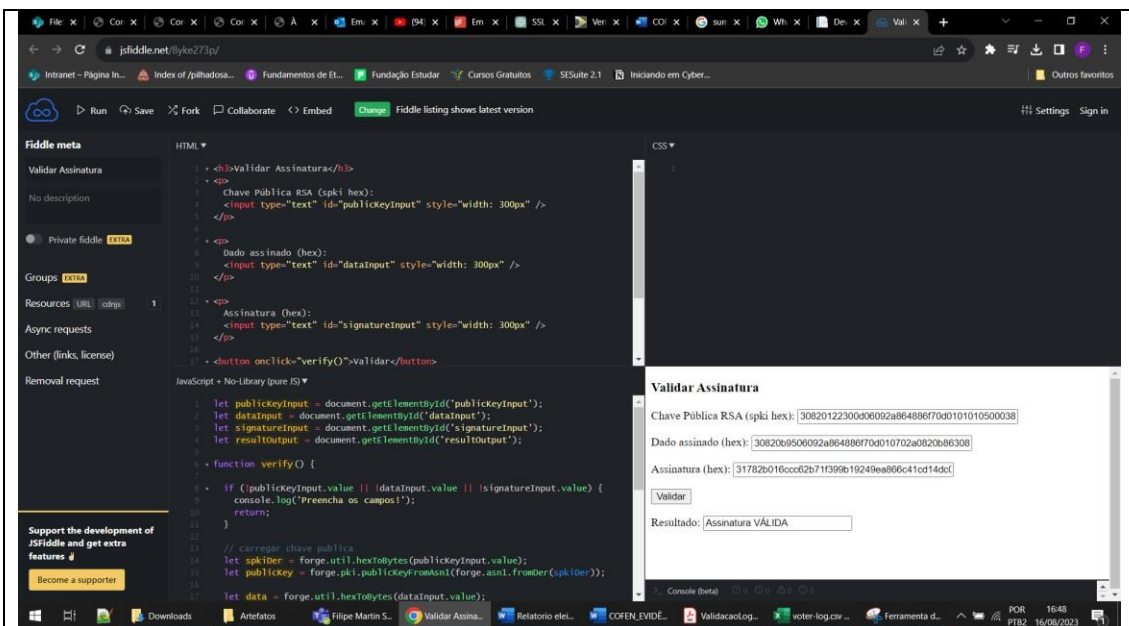
File input: `vote-server-signature.bin`

Select Output

Base64 **Hex** HEX UTF-8 Unicode Raw File

```
3172d2016cc62b71f399b19249ea866c41cd14dc0e98b6156bec7b635f3526725f1e0cbea3e70215ef781b26e61dd35eca8b5ee757543c9e9b663193ed9353aa194eFa0257057bad045929b89
8386b815a693867171b85db3b6c4ed807a7a57f57fa122ac3719775f8e2491cc29f7d4b62f2c2bd90bf13797cdfdbeb30a1250c2f8121f564810281e4a7ca0f59d3987ab54c686a3d8b47b8852
9b741f684fed5f8666df317a0a0629c845441edeafad124e6739f5bec123b106984846468b27cfb025e3ba76bad9e7b6545ace811236e079ad7abd436e3e8216cfd1a7442a7350600dfac3c763
fad354d35ca8ab9591fff8eb7673ced498
```

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



JSFiddle.net

Run Save Fork Collaborate Embed Change Fiddle listing shows latest version

Fiddle meta

Validar Assinatura

No description

Private fiddle

Groups

Resources

Async requests

Other (links, license)

Removal request

```
JavaScript - No-Library (pure JS)
let publicKeyInput = document.getElementById("publickeyInput");
let dataInput = document.getElementById("dataInput");
let signatureInput = document.getElementById("signatureInput");
let resultOutput = document.getElementById("resultOutput");

function verify () {
  if (publicKeyInput.value || dataInput.value || signatureInput.value) {
    console.log("Preencha os campos!");
    return;
  }

  // carregar chave pública
  let spkIder = forge.util.hexToBytes(publicKeyInput.value);
  let publicKey = forge.pki.publicKeyFromAsn1(forge.asn1.fromDer(spkIder));

  let data = forge.util.hexToBytes(dataInput.value);
  let signature = forge.util.hexToBytes(signatureInput.value);

  let result = publicKey.verify(data, signature);

  resultOutput.innerHTML = result ? "Assinatura VÁLIDA" : "Assinatura INVÁLIDA";
}
```

Validar Assinatura

Chave Pública RSA (spki hex): `30820122300006092a86488f70d0101010500038`

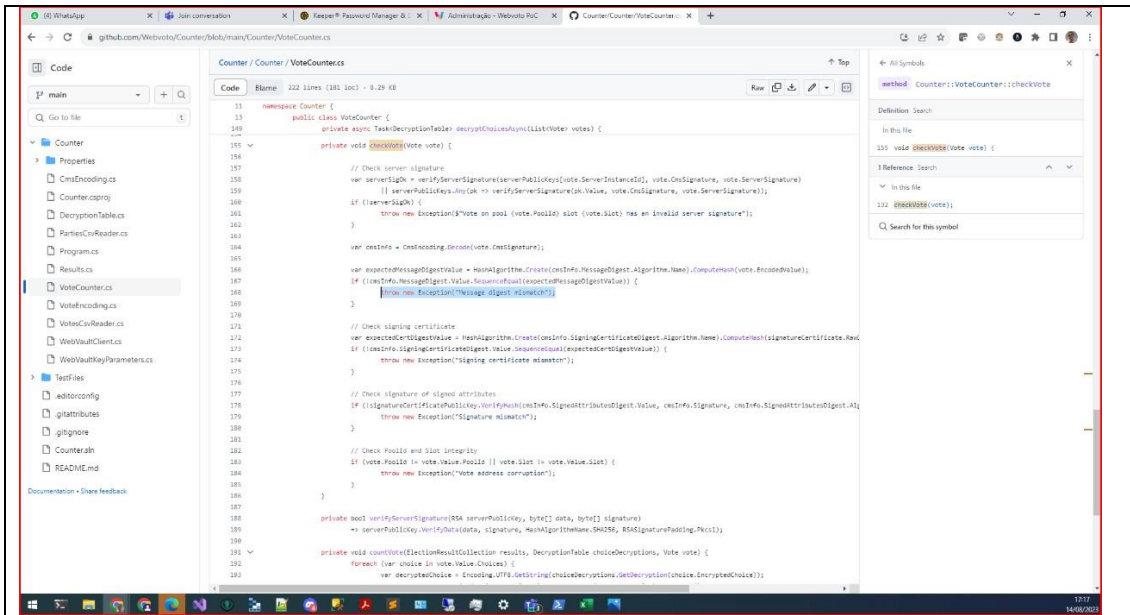
Dado assinado (hex): `3082069506092a86488f70d010702a0820b86308`

Assinatura (hex): `31782b016ccc62b71f399b19249ea866c41cd14dc`

Validar

Resultado: Assinatura VÁLIDA

Verificando se a assinatura é válida



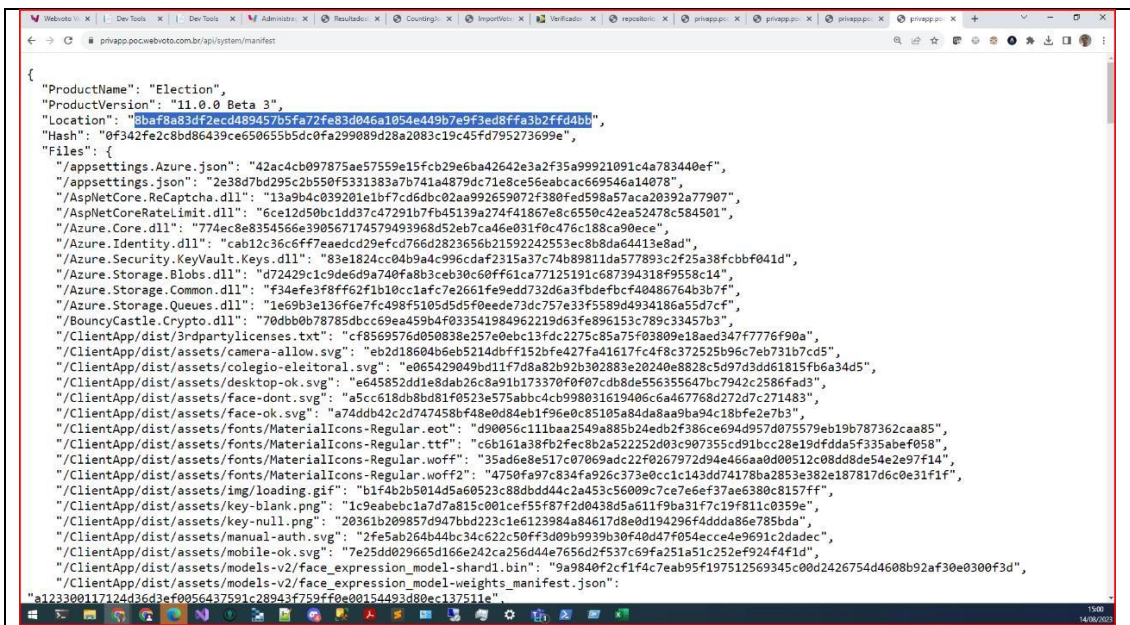
```

namespace Counter {
    public class VoteCounter {
        private async Task<DescriptionFolde> decryptChoicesAsync(List<Vote> votes) {
            private void checkVote(vote vote) {
                // Check server signature
                var serverSigh = verifyServerSignature(serverPublicKeys[vote.ServerInstanceId], vote.OnsSignature, vote.ServerSignature);
                // serverPublicKeys.Any(xk => verifyServerSignature(xk.Value, vote.OnsSignature, vote.ServerSignature));
                if (!serverSigh) {
                    throw new Exception("Vote on pool {vote.PoolId} slot {vote.Slot} has an invalid server signature");
                }
                var certInfo = CertHosting.Income(vote.CertSignature);
                var expectedMessageDigestValue = HashAlgorithm.Create(certInfo.MessageDigest.AlgorithmName).ComputeHash(vote.EncodeValue);
                if (!certInfo.MessageDigest.Value.Equals(certInfo.ExpectedMessageDigestValue)) {
                    throw new Exception("Message digest mismatch");
                }
                // Check signing certificate
                var expectedCertDigestValue = HashAlgorithm.Create(certInfo.SigningCertificateDigest.AlgorithmName).ComputeHash(certInfo.SigningCertificate.RawData);
                if (!certInfo.SigningCertificateDigest.Value.Equals(certInfo.ExpectedCertDigestValue)) {
                    throw new Exception("Signing certificate mismatch");
                }
                // Check signature of signed attributes
                if (!signatureCertificatePublicKey.VerifyHash(certInfo.SignedAttributesDigestValue, certInfo.Signature, certInfo.SignedAttributesDigest)) {
                    throw new Exception("Signature mismatch");
                }
                // Check PoolId and Slot integrity
                if (vote.PoolId != vote.Value.PoolId || vote.Slot != vote.Value.Slot) {
                    throw new Exception("Vote address corruption");
                }
            }
            private bool verifyServerSignature(BSA serverPublicKey, byte[] data, byte[] signature) {
                return serverPublicKey.VerifyData(data, signature, HashAlgorithmName.SHA256, RSASignaturePadding.Pkcs1);
            }
            private void countVote(IEnumerable<ResultCollection results, DescriptionFolde choiceDescriptions, Vote vote) {
                foreach (var choice in vote.Value.Choices) {
                    var decryptedChoice = Encoding.UTF8.GetString(choiceDecryptions.GetDecryption(choice.DecryptedChoice));
                }
            }
        }
    }
}
    
```

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": "3bf8a83df2ecd489457b5fa72fe83d046a105e449b7e9f3ed8ffa3b2ff4b4b",
  "Hash": "0f342fe2c8bd86439ce650655b5dc0fa299089d28a2083c19c45d795273699e",
  "Files": {
    "/appsettings.Azure.json": "42ac4cb097875ae57559e15fcb29e6ba42642e3a2f35a99912091c4a783440ef",
    "/appsettings.json": "2e38d7bd295c2b550f5331383a7b741a4879dc71e0c55eabcac669546a14078",
    "/AspNetCore.ReCaptcha.dll": "13a904c039201e1bf7cd6db02aa92659072f380feds98a57acac0392a77907",
    "/AspNetCore.RateLimit.dll": "6ce12d50bc1dd37c47291b7fb45139a274f41867e8c6550c42ea52478c584501",
    "/Azure.Core.dll": "774ac8e8354566e390567174579493968d52eb7ca46e031f0c476c188ca90ace",
    "/Azure.Identity.dll": "cab12c36c6ff7eaeedc29efcd766d2823656b21592242553ec8b8da64413e8ad",
    "/Azure.Security.KeyVault.Keys.dll": "83e1824cc04b9a4c996cdf2315a37c74b89811da577893c2f25a38fcbbf041d",
    "/Azure.Storage.Blobs.dll": "d72429c1c9de6d9a740fa8b3bc90c60ff61ca7125191c687394318f9558c14",
    "/Azure.Storage.Common.dll": "f34fe3f8ff62f1b10c1afc7e2661fe9edd732d6a3fbdfbfc4f0486764b3b7f",
    "/Azure.Storage.Queues.dll": "1e69b3e136fe7fc498f5105d5d5f0eade73dc757e33f55894d934186a55d7cf",
    "/BouncyCastle.Crypto.dll": "70dbb0b78785dbcc69ea459b4f033541984962219d63fe896153c789c33457b3",
    "/ClientApp/dist/3rdpartylicenses.txt": "cf8569576d050838e257e0ebc13fdcc227c85a7f03809e18aed347f776f90a",
    "/ClientApp/dist/assets/camera-allow.svg": "eb2d18604b6eb5214dbff152bfe427fa41617fc4f8c372525b96c7eb731b7cd5",
    "/ClientApp/dist/assets/colégio-eleitoral.svg": "e065429049bd11f7d8a82b92b302883c20240e8828c5d97d3dd61815fb6a34d5",
    "/ClientApp/dist/assets/desktop-ok.svg": "e645852dd1e8dad26c8a91b173370f0f07c8db8e556355647bc7942c2586fad3",
    "/ClientApp/dist/assets/face-dont.svg": "a5cc618db8bd81f0523e575abb4c998031619406c6a467768d272d7c271483",
    "/ClientApp/dist/assets/face-ok.svg": "a74ddb42c2d747458bf48e0d84eb1f96e0c85105a84da8aa9b94c18bfe2e7b3",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.eot": "d90056c11bba2549a885b24eb2f386ce694d957d075579eb19b787362caa85",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.ttf": "c6b161a38fb2fec8b2a52225d03c907355cd91bcc28e19dfdda5f335abef058",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff": "35ad6e8e517c07069adc22f026792d94e466aa0d00512c08dd8de54e2e9f14",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff2": "4750fa97c834fa926c373e0cc1c143dd74178ba2853e382e187817d6c0e31f1f",
    "/ClientApp/dist/assets/img/loading.gif": "b1f4b2b5014d5a60523c88dbd44c2a453c56009c7ce7e6ef37ae6380c8157ff",
    "/ClientApp/dist/assets/key-blank.png": "1c9eabebc1a7d7815c001cef55f87f2d0438d5a611f9ba31f7c19f811c0359e",
    "/ClientApp/dist/assets/manual-auth.svg": "20361b209857d947bb223c1e6123984a84617d8e0d194296f4dda86e785bda",
    "/ClientApp/dist/assets/mobile-ok.svg": "2fe5ab264b44bc34c622c50ff3d09b9939b30f40d47f054ecce4e9691c2dade",
    "/ClientApp/dist/assets/models-v2/Face_expression_model-shard1.bin": "9a940f2c1f14c7eab95f197512569345c00d2426744600b92af30e0300f3d",
    "/ClientApp/dist/assets/models-v2/Face_expression_model-weights_manifest.json": "a123309117124d36d9e60056437591c8943f759f0c0015493d80ec13751e",
    "a123309117124d36d9e60056437591c8943f759f0c0015493d80ec13751e"
  }
}
    
```

Servidor 1 de um total de 4.

```

{
  "ProductName": "Election",
  "ProductVersion": "11.0.0 Beta 3",
  "Location": "840e9decf1990e96921a12ab61510682796166f08e328c475cb1e22400e99fa",
  "Hash": "0f342fe2c8bd86439ce650655b5dc0fa299089d28a2083c19c45fd795273699e",
  "Files": {
    "/appsettings.Azure.json": "42ac4cb097875ae57559e15fcb29e6ba42642e3a2f35a99921091c4a783440ef",
    "/appsettings.json": "2e38d7bd295c2b50f5331383a7b741a4879dc71e8ce56eabc669546a14078",
    "/AspNetCore.ReCaptcha.dll": "13a9b4c039201e1bf7cd6db02aa992659072f380fed598a57aca20392a77907",
    "/AspNetCoreRateLimit.dll": "6ce12d50bc1dd37c47291b7fb45139a274f41867e8c6550c42ea52478c584501",
    "/Azure.Core.dll": "774ec8e8354566e390567174579493968d52eb7ca46e031f0c476c188ca90ece",
    "/Azure.Identity.dll": "cab12c36c6fff7eaedcd29efcd766d2823656b21592242553ce8b8da64413e8ad",
    "/Azure.Security.KeyVault.Keys.dll": "83e1824cc04b9a4c996cdf2315a37c74b89811da577893c2f25a38fcbbf041d",
    "/Azure.Storage.Blobs.dll": "d72429c1c9de6d9a740fa8b3ceb30c60ff61ca77125191c687394318f9558c14",
    "/Azure.Storage.Common.dll": "f34efe3f8ff62f1b10c1afc7e2661fe9edd732d6a3fbd6fbcf40486764b3b7f",
    "/Azure.Storage.Queues.dll": "1e69b3e136f6e7fc498f5105d5d5f0eede73dc757e33f5589d4934186a55d7cf",
    "/BouncyCastle.Crypto.dll": "70dbb0b78785dbcc69ea459b4f033541984962219d63fe896153c789c33457b3",
    "/ClientApp/dist/3rdpartylicenses.txt": "cf8569576d050838e257e0ebc13fdc2275c85a75f03809e18aed347f776f90a",
    "/ClientApp/dist/assets/camera-allow.svg": "eb2d186046eb5214dbff152bfe427fa41617fc4f8c372525b96c7eb731b7cd5",
    "/ClientApp/dist/assets/desktop-ok.svg": "e645852dd1e8dab26c8a91b173370f0f07c8d8e556355647bc7942c2586fad3",
    "/ClientApp/dist/assets/face-dont.svg": "a5cc618db8bd81f0523e575abbc4cb998031519406c6a467768d272d7c271483",
    "/ClientApp/dist/assets/face-ok.svg": "a74ddb42c2d74758bf48e0d84eb1f96e0c85105a84da8a9ba94c18bf7e2b73",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.eot": "d90056c111baa2549a885b24ed2f386ce694d957d075579eb19b787362caa85",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.ttf": "c6b161a38bf2fec8b2a52252d03c907355c491bc28e19dfdda5f335abe0f058",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff": "35ad6e8e517c07069adc22f0267972d94e466aa0d00512c08dd8de54e2e9f14",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff2": "4750fa97c834fa926c37e0cc1c143dd74178ba2853e382e1871d6c0e31f1f",
    "/ClientApp/dist/assets/img/loading.gif": "b1f4b25014d5a60523c88dbdd44c2a453c56009c7ce7e6ef37ae6380c8157ff",
    "/ClientApp/dist/assets/key-blank.png": "1c9eabebc1a7d7a815c001cef55f87f2d0438d5a611f9ba31f7c19f811c0359e",
    "/ClientApp/dist/assets/key-null.png": "20361b209857d947bbd223c1e6123984a84617d8e0d194296f4dda86e785bda",
    "/ClientApp/dist/assets/manual-auth.svg": "2fe5ab264b44bc34c622c50ff3d09b93930f40d47f054ecce4e9691c2dadec",
    "/ClientApp/dist/assets/mobile-ok.svg": "7e25dd029665d166e242ca256d44e7656d2f537c69fa251a51c252e924f4f1d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-shard1.bin": "9a9840f2cf1f4c7eab95f197512569345c00d24267544600892af30e0300f3d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-weights_manifest.json": "a123300117124d36d3ef0056437591c28943f759ff0e00154493d80ec137511e"
  }
}

```

Servidor 2 de um total de 4.

```

{
  "ProductName": "Election",
  "ProductVersion": "11.0.0 Beta 3",
  "Location": "759b695c9e025f5d43c17084cb5d238f40c4aace069a4e391d2bf6a299e63ae",
  "Hash": "0f342fe2c8bd86439ce650655b5dc0fa299089d28a2083c19c45fd795273699e",
  "Files": {
    "/appsettings.Azure.json": "42ac4cb097875ae57559e15fcb29e6ba42642e3a2f35a99921091c4a783440ef",
    "/appsettings.json": "2e38d7bd295c2b50f5331383a7b741a4879dc71e8ce56eabc669546a14078",
    "/AspNetCore.ReCaptcha.dll": "13a9b4c039201e1bf7cd6db02aa992659072f380fed598a57aca20392a77907",
    "/AspNetCoreRateLimit.dll": "6ce12d50bc1dd37c47291b7fb45139a274f41867e8c6550c42ea52478c584501",
    "/Azure.Core.dll": "774ec8e8354566e390567174579493968d52eb7ca46e031f0c476c188ca90ece",
    "/Azure.Identity.dll": "cab12c36c6fff7eaedcd29efcd766d2823656b21592242553ce8b8da64413e8ad",
    "/Azure.Security.KeyVault.Keys.dll": "83e1824cc04b9a4c996cdf2315a37c74b89811da577893c2f25a38fcbbf041d",
    "/Azure.Storage.Blobs.dll": "d72429c1c9de6d9a740fa8b3ceb30c60ff61ca77125191c687394318f9558c14",
    "/Azure.Storage.Common.dll": "f34efe3f8ff62f1b10c1afc7e2661fe9edd732d6a3fbd6fbcf40486764b3b7f",
    "/Azure.Storage.Queues.dll": "1e69b3e136f6e7fc498f5105d5d5f0eede73dc757e33f5589d4934186a55d7cf",
    "/BouncyCastle.Crypto.dll": "70dbb0b78785dbcc69ea459b4f033541984962219d63fe896153c789c33457b3",
    "/ClientApp/dist/3rdpartylicenses.txt": "cf8569576d050838e257e0ebc13fdc2275c85a75f03809e18aed347f776f90a",
    "/ClientApp/dist/assets/camera-allow.svg": "eb2d186046eb5214dbff152bfe427fa41617fc4f8c372525b96c7eb731b7cd5",
    "/ClientApp/dist/assets/colegio-eleitoral.svg": "e645852dd1e8dab26c8a91b173370f0f07c8d8e556355647bc7942c2586fad3",
    "/ClientApp/dist/assets/desktop-ok.svg": "a5cc618db8bd81f0523e575abbc4cb998031519406c6a467768d272d7c271483",
    "/ClientApp/dist/assets/face-dont.svg": "a74ddb42c2d74758bf48e0d84eb1f96e0c85105a84da8a9ba94c18bf7e2b73",
    "/ClientApp/dist/assets/face-ok.svg": "a74ddb42c2d74758bf48e0d84eb1f96e0c85105a84da8a9ba94c18bf7e2b73",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.eot": "d90056c111baa2549a885b24ed2f386ce694d957d075579eb19b787362caa85",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.ttf": "c6b161a38bf2fec8b2a52252d03c907355c491bc28e19dfdda5f335abe0f058",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff": "35ad6e8e517c07069adc22f0267972d94e466aa0d00512c08dd8de54e2e9f14",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff2": "4750fa97c834fa926c37e0cc1c143dd74178ba2853e382e1871d6c0e31f1f",
    "/ClientApp/dist/assets/img/loading.gif": "b1f4b25014d5a60523c88dbdd44c2a453c56009c7ce7e6ef37ae6380c8157ff",
    "/ClientApp/dist/assets/key-blank.png": "1c9eabebc1a7d7a815c001cef55f87f2d0438d5a611f9ba31f7c19f811c0359e",
    "/ClientApp/dist/assets/key-null.png": "20361b209857d947bbd223c1e6123984a84617d8e0d194296f4dda86e785bda",
    "/ClientApp/dist/assets/manual-auth.svg": "2fe5ab264b44bc34c622c50ff3d09b93930f40d47f054ecce4e9691c2dadec",
    "/ClientApp/dist/assets/mobile-ok.svg": "7e25dd029665d166e242ca256d44e7656d2f537c69fa251a51c252e924f4f1d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-shard1.bin": "9a9840f2cf1f4c7eab95f197512569345c00d24267544600892af30e0300f3d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-weights_manifest.json": "a123300117124d36d3ef0056437591c28943f759ff0e00154493d80ec137511e"
  }
}

```

Servidor 3 de um total de 4.

```

{
  "ProductName": "Election",
  "ProductVersion": "11.0.0 Beta 3",
  "Location": "8f164566240bab0706908843860a7b8537284d6ccb1d416978516b3aa5f36547",
  "Hash": "0f342fe2c8bd86439ce550655b5dc0fa299089d28a2083c19c45fd795273699e",
  "Files": {
    "/appsettings.Azure.json": "42ac4cb097875ae57559e15fcb29e6ba42642e3a2f35a99921091c4a783440ef",
    "/appsettings.json": "2e38d7bd295c2b550f531383a7b741a4879dc71e8ce56eabcac669546a14078",
    "/AspNetCore.ReCaptcha.dll": "13a9b4c039201e1bf7cd6dbc02aa992659072f380fed598a57aca20392a77907",
    "/AspNetCoreRateLimit.dll": "6ce12d50bc1dd37c47291b7fb45139a274f41867e8c6550c42ea52478c584501",
    "/Azure.Core.dll": "774ec8e8354566e390567174579493968d52eb7ca4e031f0c476c188ca90ece",
    "/Azure.Identity.dll": "cab12c36c6ff7eaeedc29efcd766d2823656b2159224253ec8b8da64413e8ad",
    "/Azure.Security.KeyVault.Keys.dll": "83e1824cc04b9a4c996cdf2315a37c74b89811da577893c2f25a38fcbf041d",
    "/Azure.Storage.Blobs.dll": "d72429c1c9de6d9a740fa8b3ceb30c60ff61ca77125191c687394318f9558c14",
    "/Azure.Storage.Common.dll": "f34ef3f8ff62f1b10c1a7c7e2661fe9edd732d6a3f0de7bc4f0486764b3b7f",
    "/Azure.Storage.Queues.dll": "1e69b3e136f6e7fc498f5105d5d5f0eeder73dc757a33f589d4934186a55d7cf",
    "/BouncyCastle.Crypto.dll": "70db0b78785dbcc69ea459b4f033541984962219d63fe896153c789c33457b3",
    "/ClientApp/dist/3rdpartylicenses.txt": "cf8569576d058038e257e0ebc13fddc2275c85a75f03809e18aad347f7776f90a",
    "/ClientApp/dist/assets/camera-allow.svg": "eb2d18604b6eb5214dbf152bfe427fa41617fc4f8c372525b96c7eb731b7cd5",
    "/ClientApp/dist/assets/colégio-eleitoral.svg": "e065429049bd11f7d8a2b92b302883e20240e8828c5d97d3dd61815fb6a34d5",
    "/ClientApp/dist/assets/desktop-ok.svg": "e645852dd1e8dab26c8a91b173370f0f07cd8de556355647bc7942c2586fad3",
    "/ClientApp/dist/assets/desktop-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": "c6b161a38fb2fec8b2a52225d03c90735cd91bcc28e19dfdd5f335abef058",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff": "35ad6e8e517c07069ad22f0267972d94e466aa0d00512c08dd8e54e2e97f14",
    "/ClientApp/dist/assets/fonts/MaterialIcons-Regular.woff2": "4750fa97c834fa926c373e0c1c143dd74178ba2853e382e187817d6c0e31f1f",
    "/ClientApp/dist/assets/img/loading.gif": "b1f4b2b5014d5a60523c88dbdd44c2a453c56009c7ce7e6ef37ae6380c8157ff",
    "/ClientApp/dist/assets/key-blank.png": "1c9eabebc1a7d7a815c001cef55f87f2d0438d5a611f9ba31f7c19f811c0359e",
    "/ClientApp/dist/assets/key-null.png": "20361b209857d947bbd2231e6123984a84617d8e0d1942964ddda86e785bda",
    "/ClientApp/dist/assets/manual-auth.svg": "2fe5ab264b44bc34c622c50ff3d09b9939b30f40d47f054ecce4e9691c2daded",
    "/ClientApp/dist/assets/mobile-ok.svg": "7e25dd029665d166e242ca256d44e7656d2f37c69fa251a51c252ef924f4f1d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-shard1.bin": "9a9840f2cf1f4c7eab95f19751259345c00d2426754d4608b92af30e0300f3d",
    "/ClientApp/dist/assets/models-v2/face_expression_model-weights_manifest.json": "a123300117124d36d3ef0056437591c28943f759ff0e0154493d80ec137511e"
  }
}

```

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.

```

C:\Users\filipe.santos\Downloads\evidencias-poc-cofen\Resultados\Apuracao\signed-results-2023-08-14-185337.bin - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
signed-results-2023-08-14-185337.p7s signed-results-2023-08-14-185337.bin
1
2
3
4 =====
5 Conselho Regional-DF
6 =====
7
8 +-----+-----+
9 | Chapa          | Votos |
10 +-----+-----+
11 | 1. Chapa 1     | 41,842 |
12 | 2. Chapa 2     | 39,852 |
13 | Votos nulos    | 9,644  |
14 | Votos brancos  | 8,662  |
15 +-----+-----+
16
17
18 =====
19 Conselho Regional-RJ
20 =====
21
22 +-----+-----+
23 | Chapa          | Votos |
24 +-----+-----+
25 | 1. Chapa 1     | 80,426 |
26 | 2. Chapa 2     | 79,184 |
27 | Votos brancos  | 20,674 |
28 | Votos nulos    | 19,716 |
29 +-----+-----+
30
31
32
33 =====
34 Conselho Regional-SP
35 =====
36
37 +-----+-----+
38 | Chapa          | Votos |
39 +-----+-----+
40 | 2. Chapa 2     | 81,571 |
41 | 1. Chapa 1     | 78,647 |
42 | Votos brancos  | 20,115 |
43 | Votos nulos    | 19,667 |
44 +-----+-----+

```

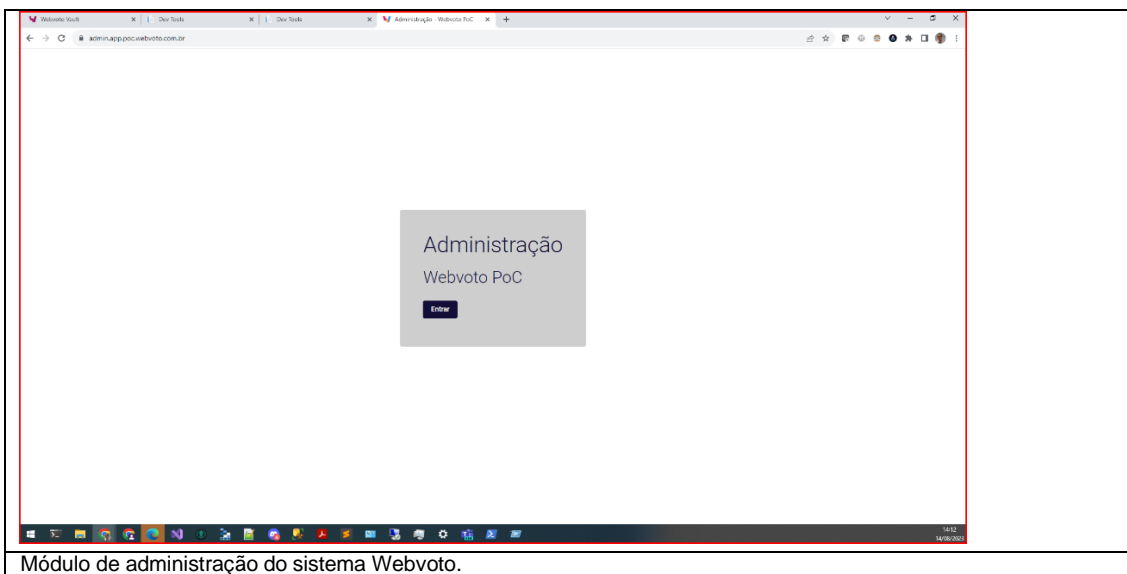
Arquivo gerado após a finalização das votações.

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.

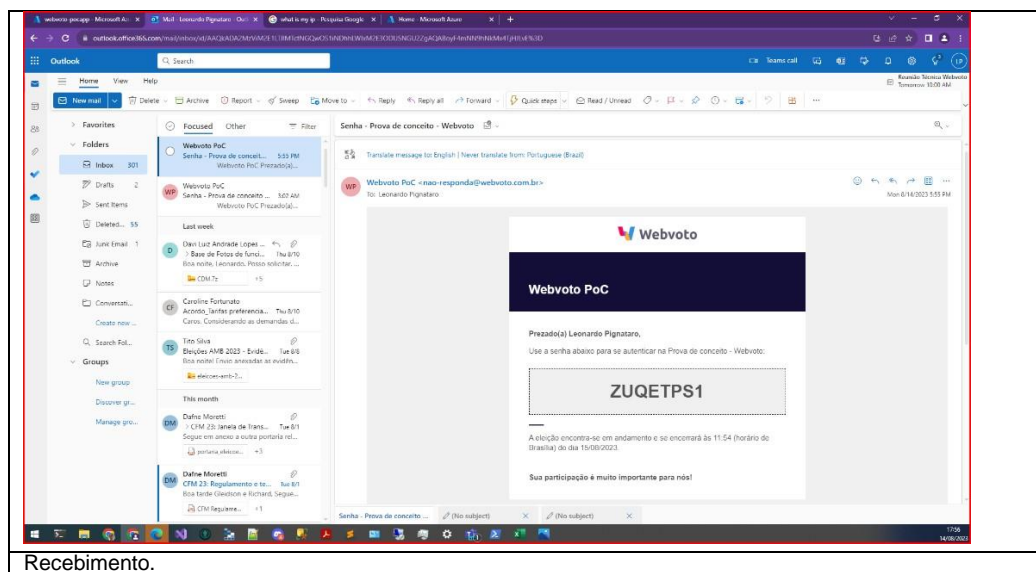
Este teste foi realizado durante a prova de conceito, porém o procedimento foi realizado no celular, onde não foi possível gerar *print screens* das evidências. Porém, existem imagens gravadas da realização da eficácia destes testes.

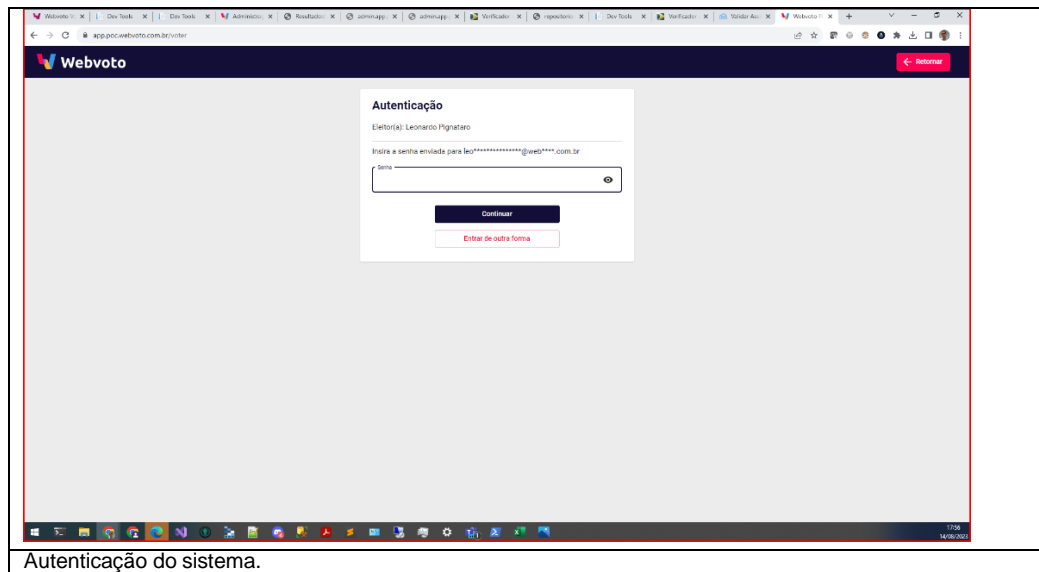
5.1.4.3. Deverá ser demonstrada a existência de um módulo de administração para importação e acompanhamento de base de dados, mediante a utilização de perfil de acesso seguro, autenticado com certificado digital, pelos responsáveis pela importação de bases de dados;



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.

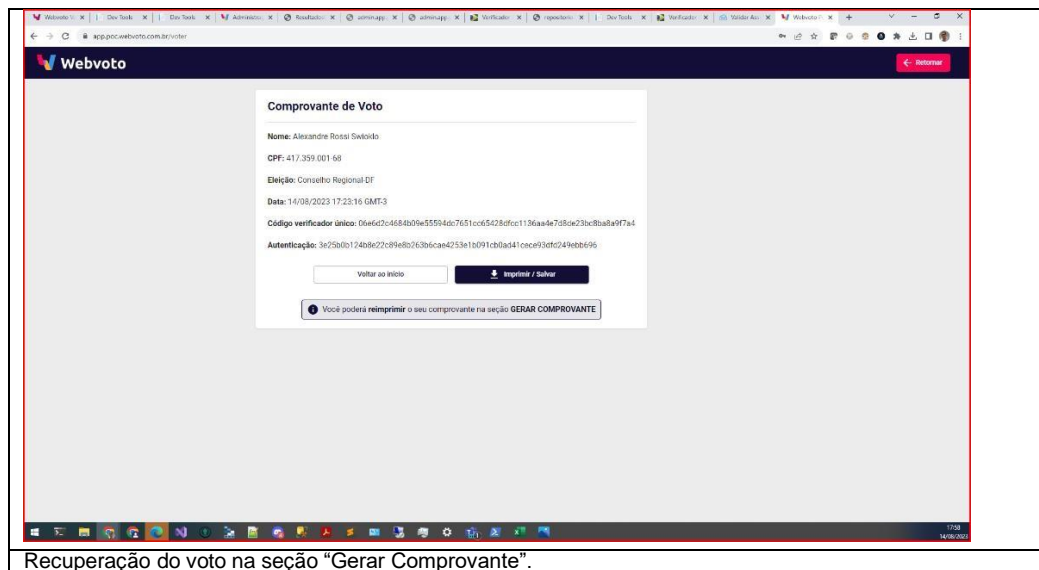




III - Autenticação do eleitor através de biometria facial. Essa funcionalidade deverá ser demonstrada para, no mínimo, 12 casos com dados reais disponibilizados pelo Cofen. A solução deverá ser capaz de validar, de forma automática, a similaridade de no mínimo 10 casos.

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.



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

Participação

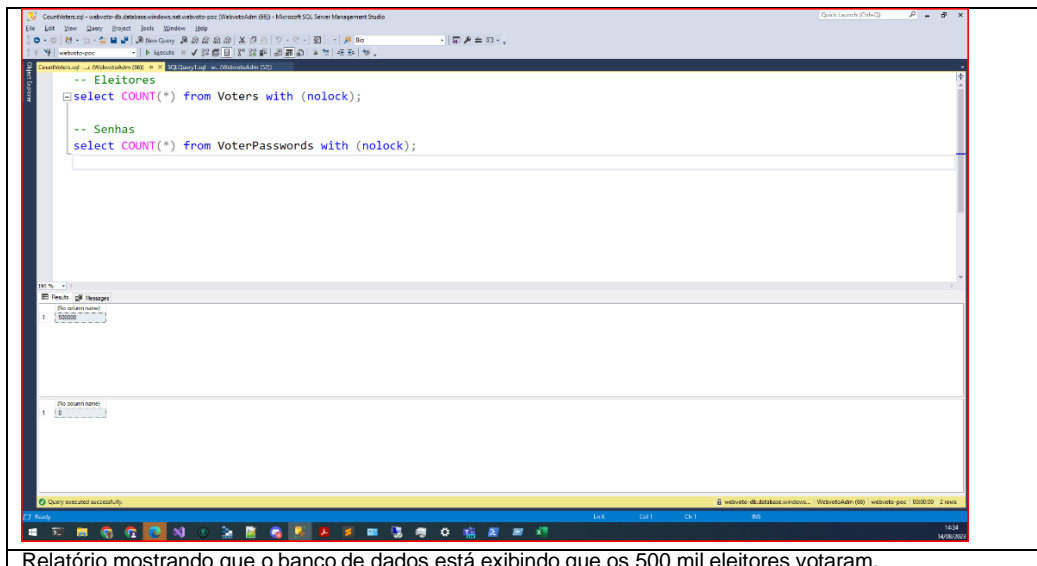
Eleitores habilitados	Eleitores votantes	Eleitores não votantes
500.000	0 (0%)	500.000 (100%)

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;



```

-- Eleitores
select COUNT(*) from Voters with (nolock);

-- Senhas
select COUNT(*) from VoterPasswords with (nolock);

```

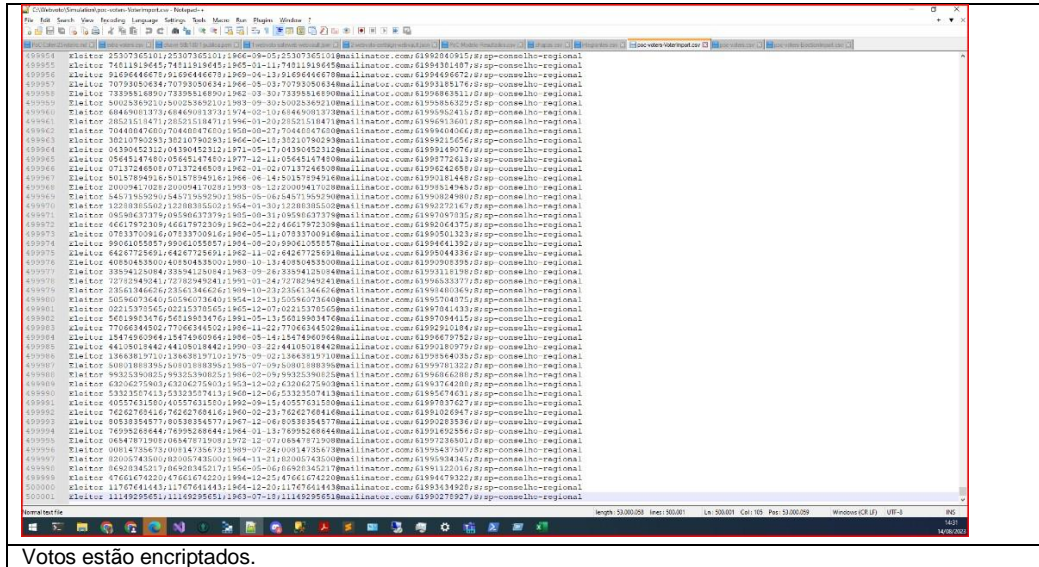
Results

(No column name)
500000

Query executed successfully.

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.



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.

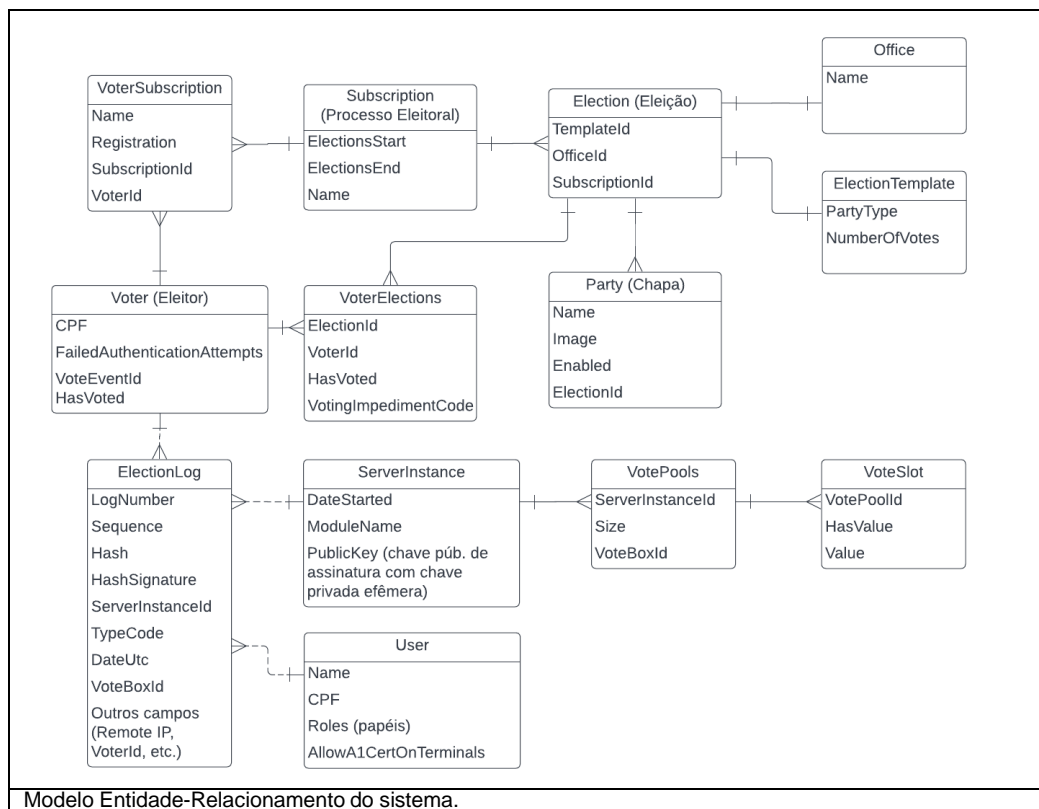
II - A apuração deverá ocorrer em equipamento separado, onde apenas a lista e votos encriptados deve ser obtida do sistema eleitoral;

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.



6. CONCLUSÃO

Concluimos 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.