

Universidade Federal de São João Del Rei

**Sistema Eletrônico de Votação
Harpócrates**

Segurança de Sistemas de Votação Eletrônica

Carlos Magno
Lucas Geraldo
Matheus Reis

**São João Del Rei
2018**

Sumário

1. Introdução	2
1.1 Escopo do Produto	2
1.1.1 Urna	2
1.1.2 VVPAT (Voter Verifiable Paper Audit Trail)	2
1.1.3 Monitoração de Comportamento	2
1.2 O processo de Votação	2
2. Requisitos	3
2.1 Requisitos Funcionais	3
2.1.1 Eleitor	3
2.1.2 Mesário	3
2.1.3 Técnico Eleitoral	4
2.2 Requisitos Eleitorais	4
2.3 Requisitos Não Funcionais	5
2.3.1 Requisitos de Desempenho	5
2.3.2 Requisitos de Segurança	5
2.3.3 Requisitos Gerais	5
3. Viabilidade	5
3.1 Urna eletrônica	6
3.2 Interface do Mesário	6
3.3 Impressora do VVPAT	6
3.4 Urna para VVPAT	7
3.5 Câmera de fiscalização	7
3.6 Câmera scanner	7
3.7 Interface de Confirmação	7
4. Arquitetura	7
5. Módulos	11
5.1 Mecanismos de segurança	11
5.1.1 Nível de código:	11
5.1.2 Procedimentos/Protocolos:	11
5.2 Procedimentos da Eleição	11
5.2.1 Procedimentos pré-eleição:	11
5.2.2 O cadastro de candidatos:	12
5.2.3 Procedimentos durante a eleição:	12
5.2.4 Procedimentos pós-eleição:	12

1. Introdução

Esta documentação apresenta uma breve descrição de requisitos e análise de viabilidade de um ambiente de votação eletrônica.

1.1 Escopo do Produto

O Sistema de votação eletrônica harpócrates possui como âmagos um simples sistema de impressão e leitura de QR-Code com validação e monitoração do comportamento do eleitor.

1.1.1 Urna

As urnas eletrônicas não terão como função armazenar os resultados da eleição. As mesmas somente serão capazes de imprimir um cartão de confirmação de voto que será utilizado posteriormente para contabilização dos votos e auditorias.

1.1.2 VVPAT (Voter Verifiable Paper Audit Trail)

O cartão de confirmação (VVPAT) será impresso em um papel offset com os seguintes dados:

- Um código QR codificado com a escolha do eleitor.
- Um número, que representam o candidato seguido de uma identificação em braile.

1.1.3 Monitoração de Comportamento

Cada ambiente de votação contará com uma câmera que irá monitorar as ações do eleitor. Essas câmeras não serão capazes de identificar o voto de cada eleitor.

1.2 O processo de Votação

O processo de votação pode ser enumerado nos seguintes passos:

1. O eleitor se autentica por meio de documento oficial com foto e biometria junto ao mesário.
2. O mesário confirma a identificação do eleitor e libera a urna eletrônica para o voto.
2.1 Caso o eleitor possua alguma dificuldade visual, o mesmo é acompanhado por um fiscal até a urna e inicia o processo de votação através do teclado físico com impressão em braile (O eleitor tem sua privacidade respeitada durante o processo de votação).
3. Com a urna eletrônica liberada o eleitor inicia o processo de votação através do teclado físico.
4. O eleitor escolhe uma opção dentre as seguintes para procurar um candidato: a) Partido, Ordem Alfabética ou código do candidato.
5. O eleitor escolhe um candidato e confirma a sua escolha.
6. O voto é impresso e o eleitor pode verificar o mesmo.
7. O eleitor coloca o voto impresso no leitor de confirmação.
8. O leitor realiza a leitura da cédula de voto impresso e apresenta na tela da urna a escolha do candidato.
9. O eleitor confirma o sua escolha e o voto impresso é automaticamente depositado em uma urna lacrada.
10. Após a confirmação do voto a urna é bloqueada até a liberação do mesário.
11. O processo para um novo eleitor se inicia novamente.
12. Ao fim do processo eleitoral a urna é bloqueada e travada para a remoção e contagem de votos.

2. Requisitos

Nesta seção serão apresentados os requisitos funcionais, não funcionais e eleitorais cobertos pelo ambiente de votação eletrônica *Harpócrates*.

2.1 Requisitos Funcionais

Descrição dos requisitos atendidos em nível de usuário. Neste primeiro momento serão cobertos os requisitos dos usuários que interagem diretamente ou indiretamente com a urna no processo de votação.

2.1.1 Eleitor

1. Deve ser capaz de interagir com a urna eletrônica por meio de teclado físico ou por toque na tela.
2. Deve ser capaz de escolher um candidato para votar.
3. Deve ser capaz de confirmar o seu voto através do VVPAT.
4. Dever ser capaz de interromper o seu processo de votação em caso de inconsistência.
5. Deve ser capaz de anular o seu voto.
6. Deve ser capaz de votar em branco.

2.1.2 Mesário

1. O mesário deve ser capaz de autenticar o eleitor.
2. O mesário deve ser capaz de liberar a urna para votação.
3. O mesário deve ser capaz de interromper o processo de votação em caso de irregularidade.

2.1.3 Técnico Eleitoral

1. O técnico deve ser capaz de contabilizar os votos.
2. Deve ser capaz de realizar um processo de recontagem dos votos.

2.2 Requisitos Eleitorais

Os principais requisitos que este sistema visa atender integralmente ou parcialmente são apresentados na Tabela 1.

Tabela 1 - Requisitos eleitorais

Requisito	Descrição	Como será Atendido
Sigilo	O voto é secreto, garantindo segurança ao eleitor	O eleitor não será passível de identificação.
Integridade	O voto deverá refletir a vontade do usuário.	O eleitor poderá conferir o seu voto impresso.
Autenticação dos Eleitores	O eleitor deverá se autenticar para votar	A autenticação será realizada pelo mesário.
Auditabilidade	Processo de recontagem devem ser possíveis.	Poderá ocorrer um processo de recontagem através dos votos impressos.
Disponibilidade.	A urna aceitará os votos como planejado e irá gerar um resultado em tempo hábil.	O processo de contagem será realizado por meio da utilização do código QR.
Baixo Custo	O sistema deve apresentar um baixo custo.	O custo do sistema é otimizado por meio da utilização de softwares livres e equipamentos reaproveitados.

Enfranchisement	Todo eleitor autenticado poderá ter a oportunidade de votar.	Oferecendo acessibilidade a todos os eleitores.
Código Aberto	O código poderá ser auditado e verificado.	Usuários cadastrados poderão acessar e recomendar melhorias.
Verificabilidade Individual	O eleitor deve ser capaz de verificar que o seu reflete a sua vontade.	O sistema de confirmação permite verificar a integridade do código qr impresso.

2.3 Requisitos Não Funcionais

2.3.1 Requisitos de Desempenho

1. A urna deve responder a interação com eleitor em menos de 30 segundos.
2. A impressão do voto deve demorar até 1 minuto.

2.3.2 Requisitos de Segurança

1. A urna deve ser capaz de interromper o processo de votação em caso de tentativa de acesso não autorizado.
2. A urna deverá ser capaz de garantir a integridade do voto do eleitor.
3. O sistema de monitoramento do eleitor deve ser capaz de invalidar o processo de votação em caso de irregularidades.

2.3.3 Requisitos Gerais

1. O eleitor não deve ser capaz de levar o seu voto impresso.
2. O sigilo do eleitor deve ser preservado.
3. O sistema deve ser capaz de oferecer um suporte para votação para pessoas que possuem alguma necessidade especial.

3. Viabilidade

Para implementação desse sistema de votação vários componentes serão necessários. Devido a questões de custo a maior parte deles será implementada utilizando ferramentas e dispositivos alternativos com o objetivo de criar um protótipo funcional do sistema. Dessa forma será possível avaliar o funcionamento e detectar possíveis falhas no mesmo.

O sistema *Harpócrates* será construído majoritariamente utilizando softwares livres, maduros e auditados. Sendo que melhorias poderão ser recomendadas e implementadas por usuários cadastrados na comunidade de desenvolvimento.

O hardware utilizado será um sistema funcional de baixo custo aproveitando peças auditadas de antigos computadores. Todo processo de construção do software e hardware poderá ser fiscalizado por entidades públicas, privadas e pessoas físicas devidamente registradas.

Abaixo estão listados todos os componentes necessários para o desenvolvimento do projeto:

- Urna eletrônica
- interface para o mesário
- impressora do VVPAT
- urna para depositar o VVPAT
- Câmera de fiscalização
- Câmera scanner
- interface de confirmação do voto.

3.1 Urna eletrônica

A urna eletrônica a ser desenvolvida deve possuir as seguintes características:

- um display de tamanho razoável e boa resolução,
- botões grandes com impressão em alto relevo para deficientes visuais,
- não possuir outras interfaces de comunicação acessíveis ao eleitor, tais como: portas usb, SD card, hdmi , entre outras.

Para o desenvolvimento do protótipo será utilizado como urna eletrônica um notebook, o qual deverá estar com interface de comunicação com o usuário limitada apenas aos botões numéricos. Essa limitação será feita por meio do próprio software de votação.

3.2 Interface do Mesário

A interface do mesário deverá possuir as seguintes características:

- um display para confirmação do cadastro do eleitor no sistema,
- um leitor biométrico,
- um monitor para acompanhar o processo de votação,
- uma função para interromper o processo de votação em caso de irregularidades,
- uma função para liberar a urna para a votação.

Para o desenvolvimento do protótipo um notebook será utilizado como interface para o mesário.

3.3 Impressora do VVPAT

A impressora do VVPAT pode ou não estar acoplada ao corpo da própria urna eletrônica. A impressora deve ser capaz de gerar ao mesmo tempo a impressão em tinta

comum (QR Code e número do candidato), bem como impressão em alto relevo para eleitores com deficiência visual.

Para o desenvolvimento do protótipo não será utilizada uma impressora. No momento da confirmação do voto será exibido na tela da urna uma imagem do VVPAT correspondente ao candidato que o eleitor votou. Para simular o VVPAT serão utilizadas cédulas já impressas com o QR code e alto relevo correspondentes ao candidato escolhido.

3.4 Urna para VVPAT

A urna para armazenamento dos VVPATs deverá ser uma caixa lacrada. Na implementação do protótipo a urna pode ser simulada com uma caixa comum ou um cofre com cadeado.

3.5 Câmera de fiscalização

A câmera de fiscalização do eleitor deverá possuir um mínimo de qualidade necessária para que o mesário possa ver com clareza todas as ações realizadas pelo eleitor. Para que o voto do eleitor não seja revelado, a câmera deverá estar posicionada de frente para o eleitor, exatamente como uma webcam.

No protótipo a ser desenvolvido a própria câmera do notebook que estiver desempenhando o papel de urna será utilizada como fiscalizadora.

3.6 Câmera scanner

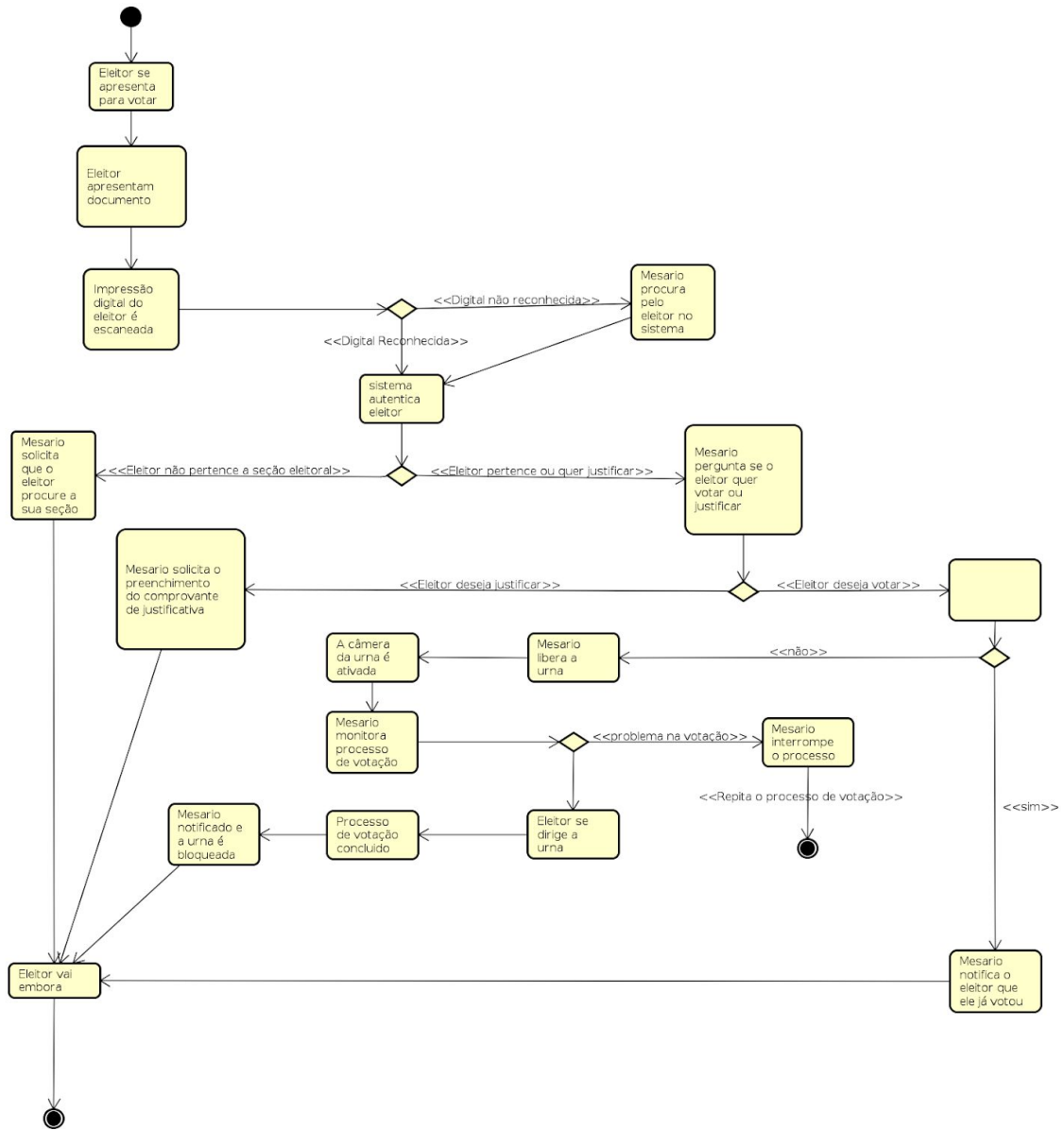
Para realizar a contagem dos votos, será utilizada uma câmera scanner ou mesmo um scanner especialista. No protótipo será utilizado a câmera de um smartphone ou a webcam de um segundo notebook.

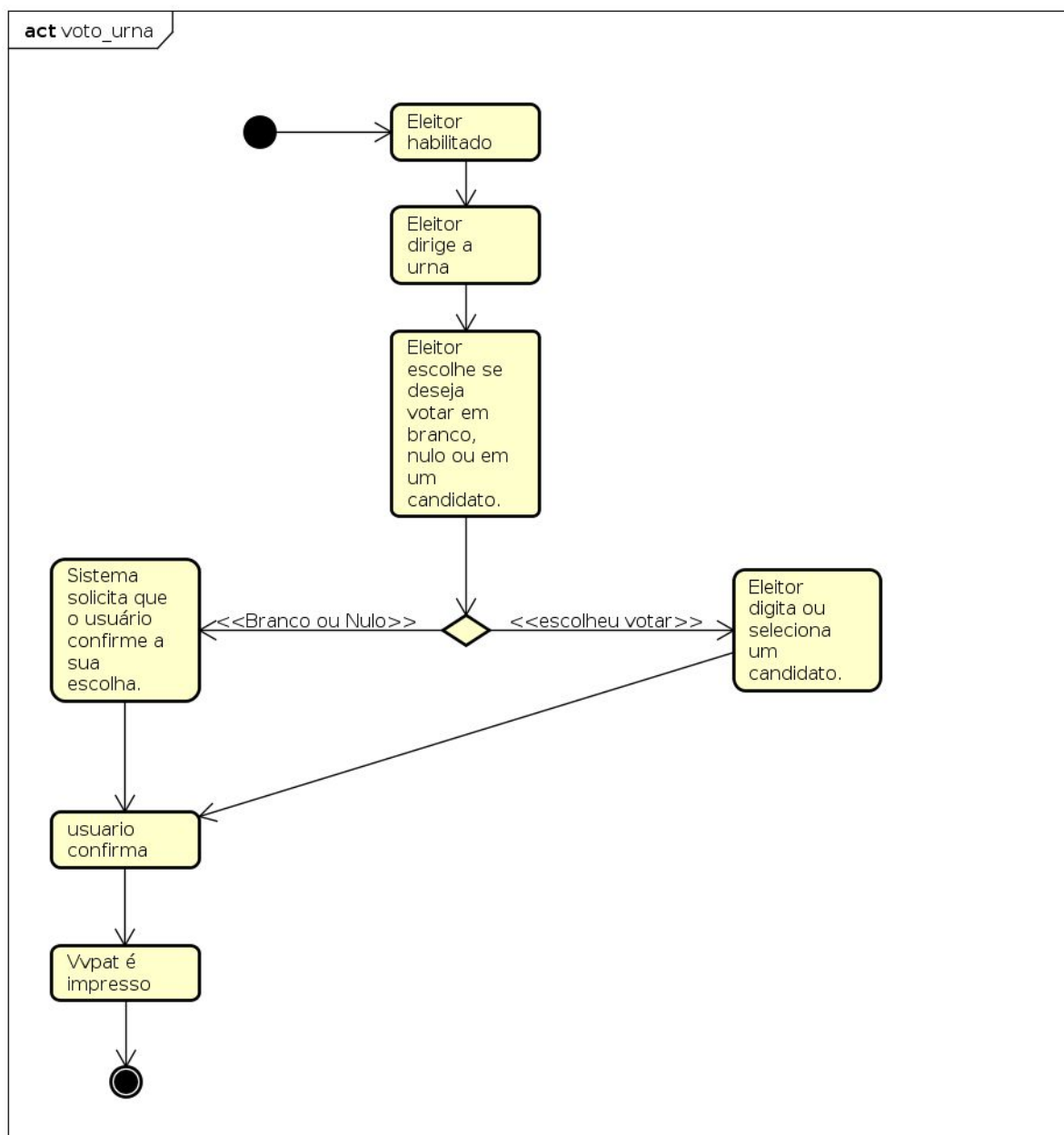
3.7 Interface de Confirmação

Para o voto do usuário ser confirmado será utilizado um scanner especialista que ficará separado da urna. Este scanner irá possuir um visor para exibir e confirmar a escolha do eleitor. No protótipo será utilizado um notebook ou tablet munido de câmera.

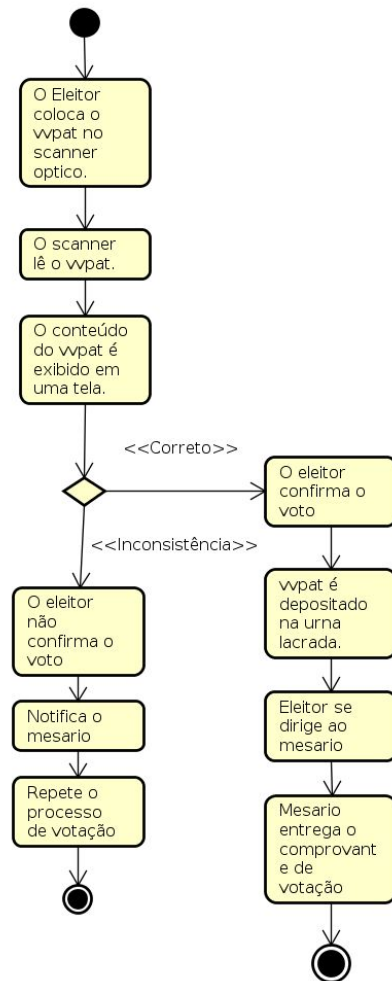
4. Arquitetura

Esta seção apresenta os diagramas de fluxo do projeto.





act confirma_voto



5. Módulos

5.1 Mecanismos de segurança

5.1.1 Nível de código:

A urna eletrônica não armazena votos como mencionado em seu projeto esquemático, porém, para contagem dos votos, onde ocorrerá a leitura dos mesmos por QR code para evitar alterações e fraudes, será utilizado uma Hash criptografada assinada digitalmente.

5.1.2 Procedimentos/Protocolos:

Para a segurança dos eleitores, o voto não será armazenado na urna eletrônica. O VVPAT após ser impresso é inserido em uma urna física pelo próprio sistema após a confirmação do eleitor. A urna é totalmente selada e só pode ser aberta quando ocorrer a contagem de votos por funcionários devidamente cadastrados e autorizados pela AE(Autoridade Eleitoral). Os funcionários serão vigiados por câmeras e a urna, caso apresente marcas de violação, será considerada inválida.

Em relação a chave privada que dará acesso a Hash, somente um funcionário da Autoridade Eleitoral terá acesso a ela.

5.2 Procedimentos da Eleição

5.2.1 Procedimentos pré-eleição:

O cadastro de eleitores deve ser feito na Justiça eleitoral de cada Estado e será feito por biometria. No cadastro eleitoral ficam armazenadas as informações cadastrais e a situação do eleitor, além de informações sobre comparecimento às urnas, justificativa eleitoral e trabalho como mesário. Também há informações sobre débitos com a Justiça Eleitoral, filiação a algum partido político, etc.

5.2.2 O cadastro de candidatos:

Para participar das eleições, os partidos políticos devem ter seu estatuto registrado na comissão eleitoral.

O software da urna eletrônica é atualizado com os respectivos candidatos após o período de confirmação do cadastramento de candidatos. O software dos mesários para reconhecimento dos eleitores também é atualizado toda época de eleição, para evitar que eleitores com débito na justiça votem e que novos eleitores que antes não eram cadastrados sejam proibidos de votar.

5.2.3 Procedimentos durante a eleição:

Durante a eleição os mesários vão ser posicionados em sua devida seção eleitoral, os eleitores vão seguir uma fila organizada e direcionados às suas respectivas seções de votos. O restante dos procedimentos são os citados na seção 1.2 deste documento e pelos diagramas da seção 4.

5.2.4 Procedimentos pós-eleição:

O encerramento da eleição será feito de acordo com as diretrizes da comissão eleitoral. Após o encerramento, os equipamentos utilizados junto com a urna lacrada, são recolhidos e enviados à unidades de armazenamento (Devidamente vigiadas por câmeras e vigias sob comando da AE).

Chegada a hora de contagem, os funcionários cadastrados abrem as urnas antes lacradas, e por meio do auxílio do leitor de QR code começam as contagens.

Terminado a contagem, é entregue aos responsáveis pela divulgação do resultado. Então finalmente o resultado é apresentado a população com os candidatos escolhidos por eles.