Universidade Federal do ABC

Graduação em Engenharia de Informação

Fernando Teodoro de Lima

URNA ELETRÔNICA DE 3ª GERAÇÃO

Santo André – SP

2016

Fernando Teodoro de Lima

URNA ELETRÔNICA DE 3ª GERAÇÃO

Trabalho de graduação apresentado ao Curso de Graduação Universidade Federal do ABC, como requisito parcial para obtenção do grau de Engenheiro de Informação.

Orientador: Prof. Dr. Mario Alexandre Gazziro

Santo André – SP

2016

Ficha Catalográfica

Lima, Fernando Teodoro de.
Urna Eletrônica de 3ª. Geração /
Fernando Teodoro de Lima –
Santo André, SP: UFABC, 2016.
75 p.

Fernando Teodoro de Lima

URNA ELETRÔNICA DE 3ª GERAÇÃO

Esse trabalho de graduação foi julgado e aprovado para a obtenção do grau de Engenheiro de Informação no curso de Graduação em Engenharia de Informação da Universidade Federal do ABC.

Santo André – SP, 17 de agosto de 2016

_____

Prof. Dr. Murilo Bellezoni Loiola

Coordenador do Curso

BANCA EXAMINADORA

_____

Prof. Dr. Mario Alexandre Gazziro

Orientador

_____

Prof. Dr. João Henrique Kleinschmidt

UFABC

_____

Prof. Dr. Carlos Kamienski

UFABC

_____

Prof. Dr. Diego de Freitas Aranha

UFSCar

_____

Dr. Paulo Matias

UFSCar

AGRADECIMENTOS

À Universidade Federal do ABC.

Aos meus pais, por todo esforço para me oferecer a melhor educação possível e por sempre estarem ao meu lado, me apoiando nos sucessos e fracassos.

À toda minha família e amigos pelo apoio oferecido.

Ao orientador Prof. Dr. Mario Alexandre Gazziro por todo suporte e empenho durante todo trabalho.

Aos professores do Curso de Graduação.

RESUMO

Este trabalhou buscou descrever diferentes modelos de máquinas de votação utilizados nos dias de hoje, divididos em gerações, nas quais a geração mais atual corrige um problema da geração anterior. Além disso, foi feita uma breve análise de um sistema de votação online e suas dificuldades nos quesitos segurança e confiabilidade. Finalmente, o trabalho descreve uma urna eletrônica de terceira geração, VVPAT (Documento de Auditoria em Papel Conferível pelo Eleitor), construída na Universidade Federal da UFABC e utilizada em uma eleição oficial para representantes discentes de graduação e de pós-graduação e representantes técnico-administrativos, bem como seus suplentes, para composição do Conselho do CMCC da UFABC.

Palavras-chave: urna eletrônica; votação; terceira geração; votação online

ABSTRACT

This study aimed to describe different voting machine models in use nowadays, dividing it in generations in which the most recent one fixes a problem in the predecessor model. Furthermore, there is a brief analysis of an online voting system and its difficulties regarding security and reliability. Finally, this study describes a third generation, Voter Verifiable Paper Audit Trail, voting system built at Universidade Federal do ABC and used in an official election for student and technician representatives, as well as their surrogates, to compose the CMCC board at UFABC.

Keyword: voting system; election; third generation; online voting

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS

Qtde. – Quantidade

LISTA DE SIGLAS

CMCC – Centro de Matemática, Computação e Cognição

CPU – Central Processing Unit ou Unidade Central de Processamento

DRE – Direct Record Electronic voting machine ou Máquina de Gravação Eletrônica Direta do Voto

E2E – *End to End* ou Fim a Fim

GUI – *Graphical User Interface* ou Interface Gráfica do Utilizador

IVVR – *Independent Voter Verifiable Record* ou Registro Independente Conferível pelo Eleitor

MIT – *Massachusetts Institute of Technology* ou Instituto de Tecnologia de Massachusetts

NTI – Núcleo de Tecnologia da Informação

QR – *Quick Response* ou Resposta Rápida

RFID – *Radio-Frequency Identification* ou Identificação por Radiofrequência

SGBD – Sistema de Gerenciamento de Banco de Dados

SQL – *Structured Query Language* ou Linguagem de Consulta Estruturada

TSE – Tribunal Superior Eleitoral

VVPAT – *Voter Verifiable Paper Audit Trail* ou Documento de Auditoria em Papel Conferível pelo Eleitor

VVSG – *Voluntary Voting System Guidelines* ou Diretrizes do Sistema de Votação Voluntárias

SUMÁRIO

1. INTRODUÇÃO

O sistema de eleição atual se baseia em três características fundamentais: votação, através da qual os membros da população reconhecidos como eleitores podem expressar, anonimamente, sua vontade; apuração, que permite a contabilização dos votos emitidos por esses membros da população; e fiscalização, que visa garantir a idoneidade do processo, de modo a assegurar que o resultado da apuração dos votos seja realmente a expressão da vontade da grande maioria da população.

Um sistema eletrônico de eleição deveria ser tal que assegurasse essas três características fundamentais, de preferência melhorando cada um de seus aspectos e sem nunca ser menos seguro e confiável do que um sistema não eletrônico.

Na marca dos 142 milhões de brasileiros que votam no Brasil e dos 350 mil eleitores que votam no exterior segundo dados apontados pelo Tribunal Superior Eleitoral (TSE) em 2014, a segurança do voto se torna cada vez mais algo que gera preocupação. A privacidade de cada informação prestada pelo eleitor deve ser garantida, de forma a garantir o máximo do sigilo de cada voto com o mesmo intuito de inibir as fraudes que antes existiam antes da criação da máquina eleitoral, a urna eletrônica.

Para ajudar a aperfeiçoar o modelo de votação existente é necessário observar algumas complicações.

A princípio, o próprio TSE admite que a urna eletrônica não é totalmente confiável, embora a imagem passada em propagandas na televisão mostra o contrário, o que reafirma a opinião de muitos especialistas.

Os eleitores após digitarem seu voto na urna eletrônica e depositarem com esperança a mudança para um país melhor, saem da cabina eleitoral sem nenhuma garantia de que o seu voto está de fato fazendo a diferença para tal.

1.1 Objetivos

Estudar a evolução do sistema brasileiro de votação e apresentar uma urna eletrônica de terceira geração, que tem por objetivo suprir as deficiências na segurança da urna eletrônica eleitoral utilizada atualmente, bem como mostrar um estudo de caso do uso desta urna em uma eleição na Universidade Federal do ABC.

2. REVISÃO DE LITERATURA

2.1 A Urna Eletrônica

O primeiro sistema informatizado de votação foi iniciado assim que se completou o cadastro único e automatizado de eleitores, que começou em 1985 e foi finalizado em 1986, quando o Brasil contava com cerca de 70 milhões de eleitores. Não havia um registro nacional até então, o que abria espaço para fraudes no cadastro.

Em 1994, sob a Presidência do ministro Sepúlveda Pertence, o TSE realizou pela primeira vez o processamento eletrônico do resultado das eleições gerais daquele ano com recursos computacionais da própria Justiça Eleitoral.

A partir de 1995 começou uma grande revolução no sistema de votação: a criação do voto eletrônico com o objetivo de eliminar a fraude no processo eleitoral. Dessa forma seria possível votar e apurar os votos de forma bastante rápida.

O objetivo passou a ser a construção de um equipamento baseado em computador, com tela, teclado e CPU num mesmo bloco, e com vários requisitos de segurança já implementados.

Outras condições fundamentais eram que a máquina fosse de fácil interação com o cidadão e totalmente fechada, impedindo o acesso a suas memórias internas, algo que o computador na época não oferecia.

Em 1996, os votos de mais de 32 milhões de brasileiros, um terço do eleitorado da época, foram coletados e totalizados por meio das mais de 70 mil urnas eletrônicas produzidas para aquelas eleições. Participaram 57 cidades com mais de 200 mil eleitores, entre elas, 26 capitais (o Distrito Federal não participou por não eleger prefeito).

Embora o Brasil tenha sido pioneiro no uso da urna eletrônica, adotada pela primeira vez em 1996, o TSE sempre usou o mesmo tipo de equipamento, chamado de primeira geração.

2.2 Gerações

Criado em 1991, o equipamento usado no Brasil desde 1996 é do modelo DRE (*Direct Record Electronic voting machine* ou máquina de gravação eletrônica direta do voto). Nesse modelo, cada voto é mostrado na tela para confirmação do eleitor e depois o voto é gravado diretamente em algum arquivo na memória digital. No final da votação, o equipamento faz a apuração dos votos eletronicamente que depois devem ser transmitidos, por alguma via digital, para a central de totalização.

A dependência da confiabilidade do software nos modelos DRE encontrou muita resistência e a partir de 2004, na Venezuela, começou o fim do ciclo de vida desse modelo, que começou a ser substituído por outros modelos independentes de software.

Entre 2006 e 2012, a Holanda, a Alemanha, os EUA, o Canada, a Rússia, a Bélgica, a Argentina, o México e o Paraguai abandonaram o modelo DRE. Finalmente, em 2014, chegou a vez da Índia e do Equador adotarem modelos mais avançados e, com isso, o Brasil é o único país a usar esse modelo.

Em 2012, um grupo de especialistas brasileiros – na Universidade de Brasília - conseguiu colocar os votos em ordem cronológica[1], de forma o sigilo do voto foi comprometido, já que podia ser quebrado por quem anota a ordem dos eleitores. Segundo o TSE, o sigilo do voto não foi quebrado, já que o dono do voto não foi identificado.

A maioria dos países que usam urna eletrônica adota um modelo que emite comprovante de papel, conhecido como 2ª geração. Esse modelo ficou conhecido como IVVR (*Independent Voter Verifiable Record* ou Registro Independente Conferível pelo Eleitor) ou VVPAT (*Voter Verifiable Paper Audit Trail* ou Documento de Auditoria em Papel Conferível pelo Eleitor).

Esse novo modelo permite gravar o voto em meio independente, de forma que este não pode ser alterado pelo equipamento de votação e deve permitir ao eleitor checar os candidatos escolhidos antes de confirmar o voto. O papel fica na seção eleitoral.

[1] G1. UnB diz que descobriu fragilidade na segurança da urna eletrônica. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/03/unb-diz-que-descobriu-fragilidade-naseguranca-da-urna-eletronica.html>. Acesso em: 20 de novembro de 2014.

A principal característica de equipamentos VVPAT é que os votos passam a ser independentes do software. O Registro Digital de Votos e a sua apuração eletrônica podem ser conferidas por ações contábeis de auditoria, independentes do desenvolvedor do software e do administrador do sistema.

Assim, em 2006, desenvolveu-se o Princípio da Independência do Software em Sistemas Eleitorais que, aos poucos, passou a ser exigido em todos os países que usam voto eletrônico, fora o Brasil.

A partir de 2008, várias iniciativas começaram a apresentar sistemas eleitorais independentes do software que aprimoravam e/ou facilitavam os procedimentos de auditoria, tanto do registro do voto, como de sua apuração e totalização.

Na Argentina foi apresentada a ideia de uma cédula eleitoral com um chip de radiofrequência (RFID) embutido[2], onde, num só documento, estão presentes o registro digital e o registro impresso do voto. Um leitor óptico verifica se o dado gravado no chip coincide com o do voto impresso. Em caso positivo, o eleitor insere a cédula em uma urna comum.

Em 2009, foi testado o sistema *Scantegrity* II[3], nos EUA, onde o voto criptografado é impresso e entregue ao eleitor, que pode verificar posteriormente o seu processamento, sem, no entanto, revelar o conteúdo do seu voto.

Os sistemas de 3ª geração são designados como "*End-to-End Verifiability*" ou E2E, que pode ser interpretado como verificabilidade de fim a fim ou verificabilidade de ponta a ponta. Todos esses sistemas de 3ª geração têm como característica comum a independência do software e a grande facilidade de auditoria independente, de fim a fim, no processamento digital do voto.

Na Figura 1, pode-se ver a distribuição, fevereiro de 2014, dos modelos usados no mundo. Em cinza, estão os países que não adotam o voto eletrônico em eleições oficiais. Em vermelho, os países que ainda usam sistemas DRE de 1ª geração (dependentes de software). Em laranja, países que testaram e abandonaram sistemas de

[2] Digital Rights. Argentina: O Sistema de Votação em Debate. Disponível em: http://www.digitalrightslac.net/pt/argentina-el-sistema-de-votacion-en-debate/. Acesso em: 24/08/2016.

[3] CHAUM, David et al. Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. EVT, v. 8, p. 1-13, 2008.

1ª geração por falta de transparência ou falta de confiabilidade e não estão usando votação eletrônica. Em azul, países que abandonaram sistemas de 1ª geração e passaram a usar sistemas VVPAT de 2ª geração (independentes de software). Em verde, países que adotaram ou estão testando sistemas E2E de 3ª geração (independentes de software, com auditoria facilitada).

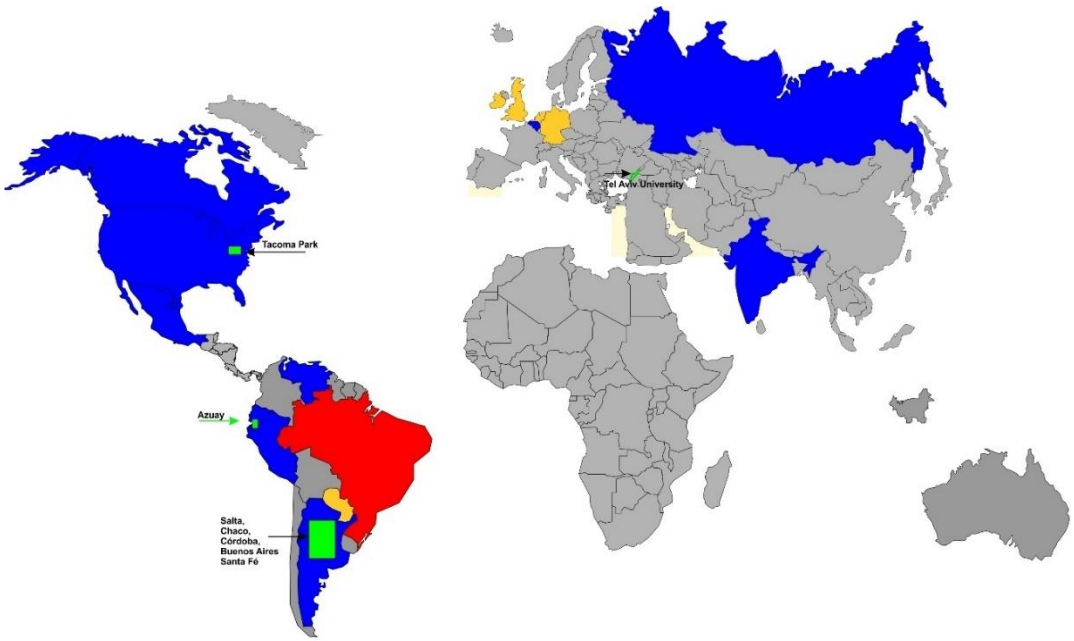


Figura 1: Distribuição dos modelos usados no mundo.
Fonte: www.brunazo.eng.br/voto-e/textos/modelosUE.htm (Atualizado em fevereiro de 2014. Acesso em agosto de 2016).

2.3 Princípio da Independência de Software

O Princípio da Independência de Software em sistemas eleitorais estabelece que:

"Um sistema eleitoral é independente do software se um erro não detectado no software não puder causar um erro indetectável no resultado da apuração ou na inviolabilidade do voto."[4].

[4] FILHO, A.B.; GAZZIRO,M. Critérios para Avaliação de Sistemas Eleitorais Digitais. In: XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2014. Santo André – SP. Anais ... Santo André: UFABC, 2014. p. 599-610

Esse princípio foi criado a partir da constatação de que é muito mais difícil e caro se determinar que um software eleitoral complexo está livre de erros que afetem o seu desempenho, do que desenvolver esse próprio software.

Conforme as diretrizes Voluntary Voting System Guidelines (VVSG)[5], sistemas eleitorais devem oferecer total verificabilidade do resultado por via independente do software usado, estabelecendo as seguintes recomendações, assim traduzidas e adaptadas:

- Ao menos dois registros do voto devem ser produzidos e um deles deve ser guardado em meio que não posso ser modificado pelo sistema (eletrônico) de votação, de forma que ambos registros não estejam sob controle de um único processo digital.

- O eleitor deve estar capacitado para verificar a igualdade dos dois registros do seu voto antes de deixar o local de votação.

- O processo de verificação dos registros do voto devem ser independentes e ao menos um deles ser conferível diretamente pelo eleitor.

- Os dois registros de um voto poderão ter sua consistência verificada posteriormente por meio de identificadores únicos que permitam a correlação dos registros.

A Tabela 1 descreve a conformidade de três modelos de máquinas de votação com relação ao princípio de Independência de Software.

Os equipamentos analisados são os seguintes:

- Urnas eletrônicas brasileiras, desenvolvidas pelo TSE, em uso no Brasil desde 1996.

- Equipamentos de votação SAES 3000[6], fabricados pela empresa Smartmatic e usadas desde 2004 na Venezuela e mais recentemente na Bélgica e no Equador.

[5] http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx
[6] Digital Vote. A look at the basis of electronic voting in Venezuela: SAES Machines. Disponível em: <https://digitalvote.wordpress.com/2010/08/02/a-look-at-the-basis-of-electronic-voting-in-venezuela-saes-machines/> Acesso em: 24 de agosto de 2016.

- Equipamentos Vot-AR[7], fabricados pela empresa MAS e usado em algumas províncias da Argentina desde 2010 e mais recentemente no Equador.

Tabela 1: Conformidade de três modelos de máquinas de votação com relação ao Princípio de Independência de Software.

	UE2009 Brasil	SAES Venezuela	Vot-AR Argentina
Uma modificação ou erro não detectado no software pode causar um erro indetectável no resultado da apuração	Sim	Não	Não
Conformidade com a Norma Técnica: Voluntary Voting Suystem Guidelines	Não	Sim	Sim

2.4 RSA e Assinatura Digital

RSA é um algoritmo de criptografia de dados, que deve seu nome a três professores do Instituto de Tecnologia de Massachusetts (MIT), Rivest, Adi Shamir e Leonard Adleman, que inventaram esse algoritmo que implementa um sistema de chaves assimétricas. O RSA, uma das mais bem-sucedidas implementações de sistemas de chaves assimétricas, envolve um par de chaves, uma pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Apesar de diferentes, as duas partes desse par de chaves são matematicamente ligadas. A chave pública é usada, por exemplo, para encriptar texto puro ou para verificar uma assinatura digital; já a chave privada é usada para a operação oposta, nesses exemplos para decriptar texto cifrado ou para criar uma assinatura digital. O termo assimétrico vem do uso de diferentes chaves para realizar essas funções opostas, cada uma inversa a outra.

Fazendo-se uso da assinatura digital, o emissor da mensagem não pode negar tê-la emitido, já que ele é o único de posse da chave privada, logo, ninguém mais poderia ter criado tal assinatura. O receptor utiliza a chave pública para fazer a validação da mensagem.

[7] Vot.ar. Sobre Vot.ar. Disponível em: <http://www.votar.com.ar/> Acesso em 24 de agosto de 2016.

Para que a assinatura não aumente de tamanho com o crescimento da mensagem, opera-se o algoritmo sobre um resumo (*digest*) da mensagem, que identifica essa mensagem como única. Esse resumo pode ser feito utilizando uma função de dispersão criptográfica (ou função *hash* criptográfica), de forma que, geralmente, o resumo de uma mensagem é alterado quando um byte da mensagem é alterado. Sendo assim, qualquer alteração na mensagem no meio do caminho, alteraria o resumo e, portanto, a assinatura também seria modificada, fazendo com que a mensagem não seja validada.

Na Figura 2 podemos ver o fluxo da informação utilizando o sistema de assinatura digital de chaves assimétricas.

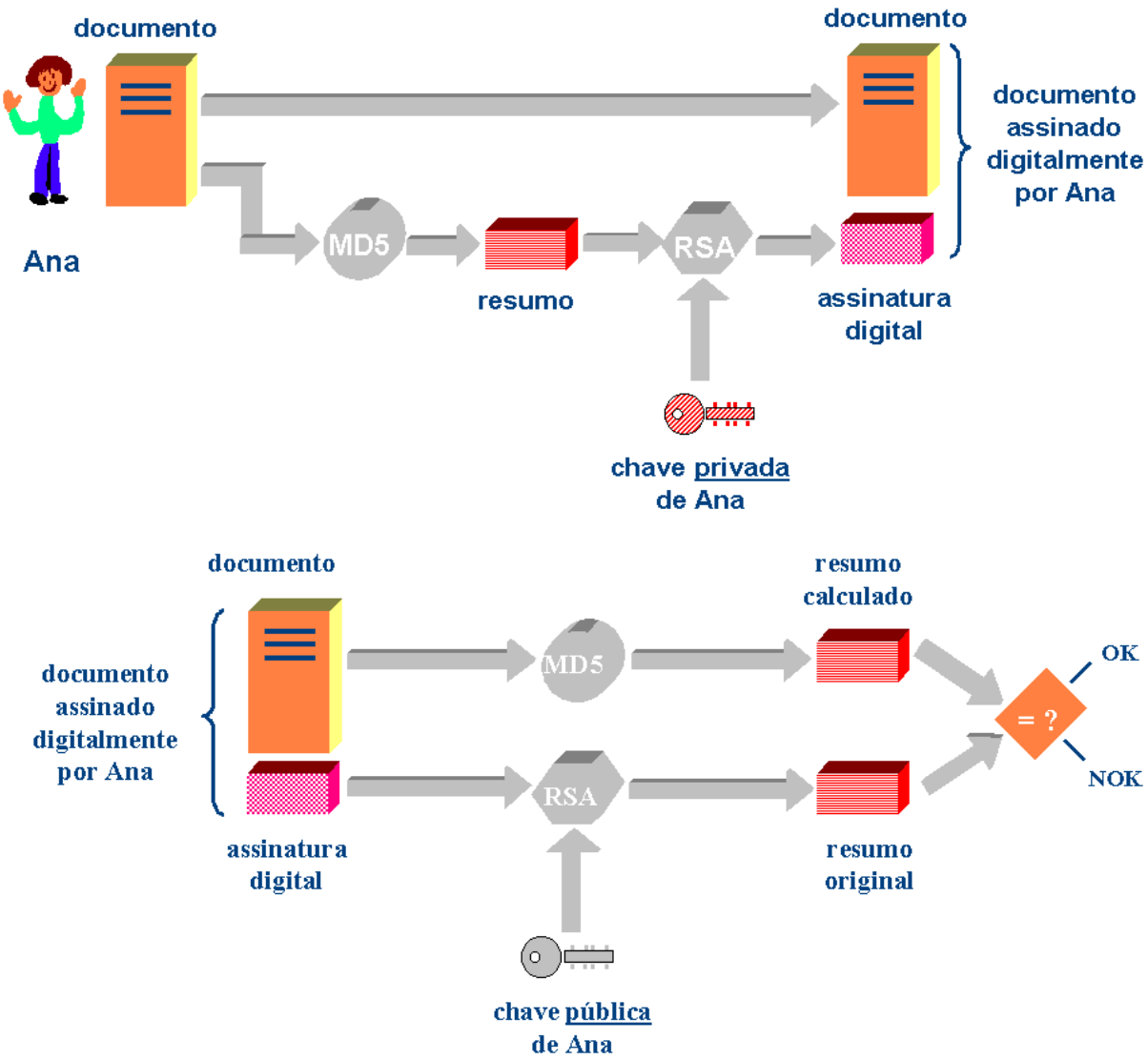


Figura 2: Fluxo da informação para assinatura e verificação utilizando chaves assimétricas.

Fonte: http://www.training.com.br/lpmaia/pub_seg_cripto.htm (2016)

2.5 Urna Eletrônica e a Internet

A Estônia foi o primeiro país a criar um sistema de votação pela internet. O governo testou o sistema nas eleições regionais de 2005[8] e, dois anos depois, o modelo foi usado nas eleições nacionais parlamentares. Em 2011, 25% dos votos para o Parlamento Europeu foram online.

Observando as Figura 3, 4 e 5, podemos ter um entendimento melhor de como funciona essa urna.

O processo de votação é mostrado na Figura 3. Neste, o eleitor precisa se conectar ao servidor de eleições utilizando o seu cartão nacional de identidade, que contém dois pares de chaves RSA, um para autenticação e um para fazer assinaturas digitais. O servidor verifica se o eleitor é elegível e manda uma lista de candidatos específicos àquele eleitor. O eleitor deve escolher os candidatos e vota, enviando os votos assinados e criptografados para o servidor, que associa uma identificação ao voto e a retorna para o cliente, que mostra um código QR para o eleitor.

Como uma forma de defesa contra coerção, os eleitores podem votar múltiplas vezes, porém somente o último voto é contabilizado.

[8] PIETERS, Wolter. Verifiability of electronic voting: between confidence and trust. In: DataProtection in a Profiled World. Springer, Dordrecht, p. 157-175. Disponível em: < http://doc.utwente.nl/72498/ > Acesso em: 09 de março de 2015.

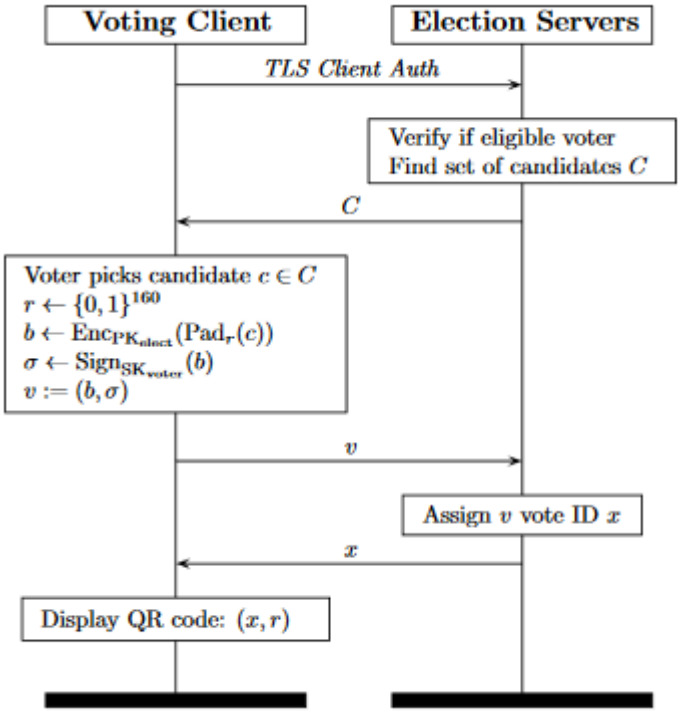


Figura 3: Processo de votação

Fonte: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf (2016)

Para o processo de verificação, mostrado na Figura 4, um aplicativo faz a leitura do código QR e envia a identificação do voto, gerada na etapa anterior, para o servidor, que retorna o voto criptografado. O aplicativo simula todos os possíveis votos e compara com o voto retornado pelo servidor e, quando os dois são iguais, o aplicativo mostra os candidatos votados.

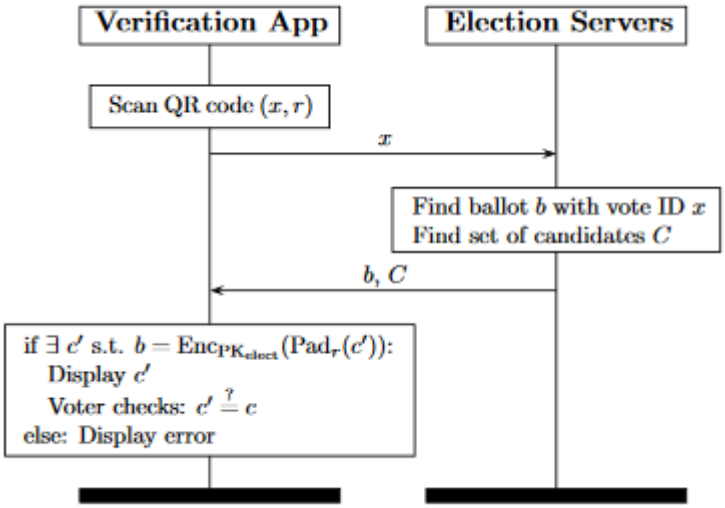


Figura 4: Processo se verificação

Fonte: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf (2016)

Já na Figura 5, temos o processo de apuração dos votos. Após o fim das eleições, o servidor processa os votos criptografados para revalidar as assinaturas e remove votos que foram revogados ou que são inválidos. Os votos criptografados são gravados em DVD e movidos para o servidor de contagem, aonde os votos são decriptados e somados. Os resultados são então gravados em DVD e junto com os resultados das votações "físicas", ou em pessoa, são publicados.

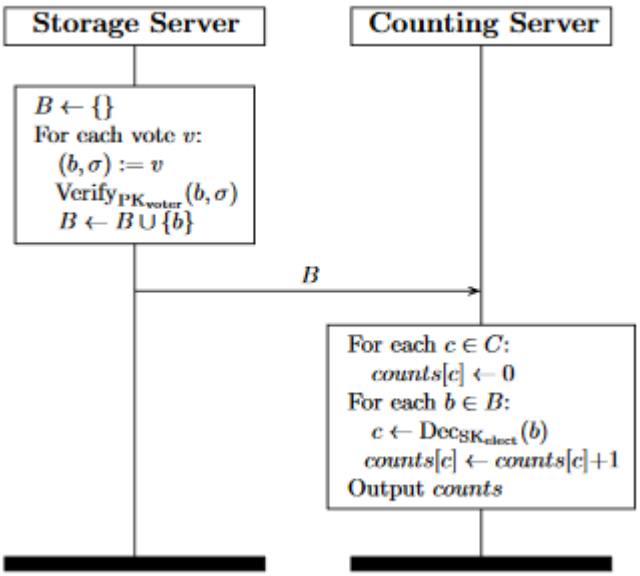


Figura 5: Processo de apuração.

Fonte: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf (2016)

Apesar de muitos Estonianos terem orgulho de seu sistema de votação, críticos questionam a segurança e a confiabilidade do sistema.

Primeiramente, o sistema utilizado na Estônia não é verificável E2E. Ele utiliza um conceito mais simples ao custo de ter que confiar que os computadores e os oficiais das eleições são confiáveis.

Segundo, devido ao fato de o sistema contar com várias etapas durante a votação, controles de processos inadequados, falta de segurança durante as operações executadas podem ocorrer com bastante frequência.

Além disso, apesar de o código ser publicado abertamente, partes essenciais a segurança do mesmo não são, o que não permite que pessoas externas façam revisões a avaliações para assegurar que o código é, de fato, seguro e, mesmo nas partes do código que foram publicadas, algumas falhas foram encontradas. O sistema de votação pode sofrer um ataque de negação de serviço enviando requisições HTTP contendo cabeçalhos inesperados para o servidor, que guarda os logs dos cabeçalhos em disco. Um atacante poderia utilizar todo o espaço em disco, fazendo com que o servidor não recebesse mais votos.

3. METODOLOGIA

Visando atingir os objetivos propostos, foi desenvolvido um software para eleições que estivesse de acordo com o Princípio de Independência do Software e com as diretrizes do VVSG.

3.1 Bibliotecas utilizadas

Pré-requisitos necessários para fazer uso do software:

- Computador com sistema operacional Ubuntu 14.

- Uma webcam instalada.

- Uma impressora simples.

Foram utilizadas as seguintes biblioteca para o desenvolvimento da urna eletrônica de terceira geração:

3.1.1 python-2.7

Descrição: Plataforma de desenvolvimento da linguagem Python.
Versão: 2.7.6.

3.1.2 pip

Descrição: Sistema Gerenciador de pacotes para o Python.
Versão: 8.1.12

3.1.3 PySide

Descrição: PySide é uma biblioteca Python que possui um conjunto de ferramentas de binding[9] para interface gráfica de usuário (GUI) Qt. É uma das alternativas para a programação de janelas em Python. A biblioteca PySide é software livre.
Essa biblioteca foi lançada sob a licença LGPL em agosto de 2009 pela Nokia.
Versão: 1.2.1.

[9] Um *binding* é literalmente a ligação ou ponte entre dois sistemas. No caso de *bindings* para Python, chama-se de *extensão* a ligação entre bibliotecas desenvolvidas em C ou C++ para o uso direto no interpretador Python.

3.1.4 NumPy

Descrição: A biblioteca NumPy (Numerical para Python) possui ferramentas para o processamento de matriz para números, sequencias, registros e objetos. Seu uso geral foi projetado para manipular de forma eficiente matrizes de registros arbitrários grandes e multi-dimensionais sem comprometer o desempenho de arrays pequenas.

A biblioteca NumPy foi construída sobre a base do código numérico e adiciona funcionalidades introduzidas por numarray, além de possuir a capacidade de criar matrizes de tipo arbitrário que fazem da biblioteca adequada para interface com aplicações de base de dados de uso geral.

Existem também instalações para a transformada de Fourier discreta, álgebra linear básica e geração de números aleatórios.

Versão: 1.8.2.

3.1.5 SciPy

Descrição: A biblioteca SciPy é uma biblioteca desenvolvida para cientistas, matemáticos e engenheiros. O nome dessa biblioteca vem da abreviação da palavra ciência em inglês (Science).

A biblioteca central é a NumPy que fornece uma manipulação conveniente e rápida de um array N-dimensional. A biblioteca SciPy foi desenvolvida para trabalhar com arrays NumPy e fornece rotinas amigáveis e bem eficientes para rotinas de integração numérica.

Versão: 0.13.3.

3.1.6 PyQRCode

Descrição: A biblioteca PyQRCode é um gerador de código QR[10] escrito em linguagem Python. Esse pacote automatiza a maior parte do processo da construção de códigos QR.

Os códigos QR podem ser salvos como SVG, PNG (utilizando a biblioteca pypng), e texto simples. Em ambientes Linux, o código QR pode ser exibido diretamente na maioria dos emuladores no terminal do Linux.

[10] **Código QR** (sigla do inglês *Quick Response*) é um código de barras bidimensional que pode ser facilmente esquadrinhado usando a maioria dos telefones celulares equipados com câmera. Esse código é convertido em texto (interativo), um endereço URL, um número de telefone, uma localização geográfica, um e-mail, um contato ou uma mensagem de texto.

Versão: 1.1.

3.1.7 Pillow

Descrição: A biblioteca PIL (Python Imaging Library) é uma biblioteca voltada para a manipulação de imagens com suporte para os formatos PNG, TIFF, BMP, EPS, e GIF. Mais tarde a biblioteca sofreu atualizações e passou a ser chamada Pillow.

Versão: 1.1.7.

3.1.8 zbar

Descrição: A biblioteca ZBar é um pacote que possui a finalidade de digitalização e decodificação de código de barras dimensionais a partir de várias fontes, tais como transmissões de vídeo, arquivos de imagem, além de suportar vários tipos de código como o EAN – 13/ UPC – A, UPC – E, e principalmente o QR Code.

Em outras palavras seu funcionamento é parecido com um scanner de código de barras e decodificador desse código.

Versão: 0.10.

3.1.9 PyPng

Descrição: A biblioteca PyPNG é um pacote para codificação e decodificação de imagens em formato PNG, dessa forma as imagens geradas por essa biblioteca podem ser lidas e escritas em Python.

Versão: 0.0.18.

3.1.10 PyCrypto

Descrição: A biblioteca PyCrypto é uma coleção de funções hash (como SHA256 e RIPEMD160), e vários algoritmos de criptografia (AES, DES, RSA, EIGamal, etc.).

Versão: 2.1.6.

3.1.11 SQLAlchemy

Descrição: SQL Alchemy é uma biblioteca de mapeamento objeto-relacional SQL em código aberto para a linguagem de programação Python e sobre a licença MIT.

Versão: 1.0.14.

3.2 Módulos

Este software foi concebido de forma a dividir as tarefas executadas durante uma eleição. Dessa forma, foram construídos diferentes módulos. O módulo para Configuração de Eleição, onde podem ser cadastrados Partidos, Cargos e Candidatos; o módulo para Configuração de Urna, onde são geradas as chaves pública e privada; o módulo para Votação, onde o eleitor vota; o módulo para Verificação, onde o eleitor pode verificar se o voto impresso é realmente o que foi escolhido e módulo de Apuração, onde é feita a contagem de votos e impresso o boletim de urna.

O fluxo de votação e contabilização dos votos de uma seção é uma das partes mais importantes do processo de eleições. Algumas pessoas estão envolvidas nesse processo e são essenciais para que o mesmo possa ter sucesso, principalmente no que diz respeito à segurança na votação.

3.2.1 Setup de Eleição

Neste módulo é possível fazer o cadastro de Partidos, Cargos e Candidatos. Essas entidades cadastradas são guardadas em um banco de dados e para tanto, foi utilizada a biblioteca SQLite, que implementa um banco de dados SQL embutido. Programas que usam a biblioteca podem ter acesso ao banco de dados SQL sem executar um processo SGBD (Sistema de Gerenciamento de Banco de Dados) separado.

Vale citar, que apesar de ter sido utilizado o SQLite durante o desenvolvimento e testes, o SQLAchemy, uma biblioteca de mapeamento objeto-relacional SQL, possibilita a utilização de outros bancos de dados além do SQLite, sendo eles PostgreSQL, MySQL, FireBird, entre outras.

A Figura 6 apresenta o modelo de Entidade-Relacionamento utilizado na base de dados para fazer cadastro de partidos, cargos e candidatos. Nesse modelo, um candidato pode fazer parte de apenas um partido e pode concorrer a apenas um cargo. Por outro lado, um partido pode ter N candidatos pertencentes a ele e um cargo pode ter N candidatos concorrendo a ele.

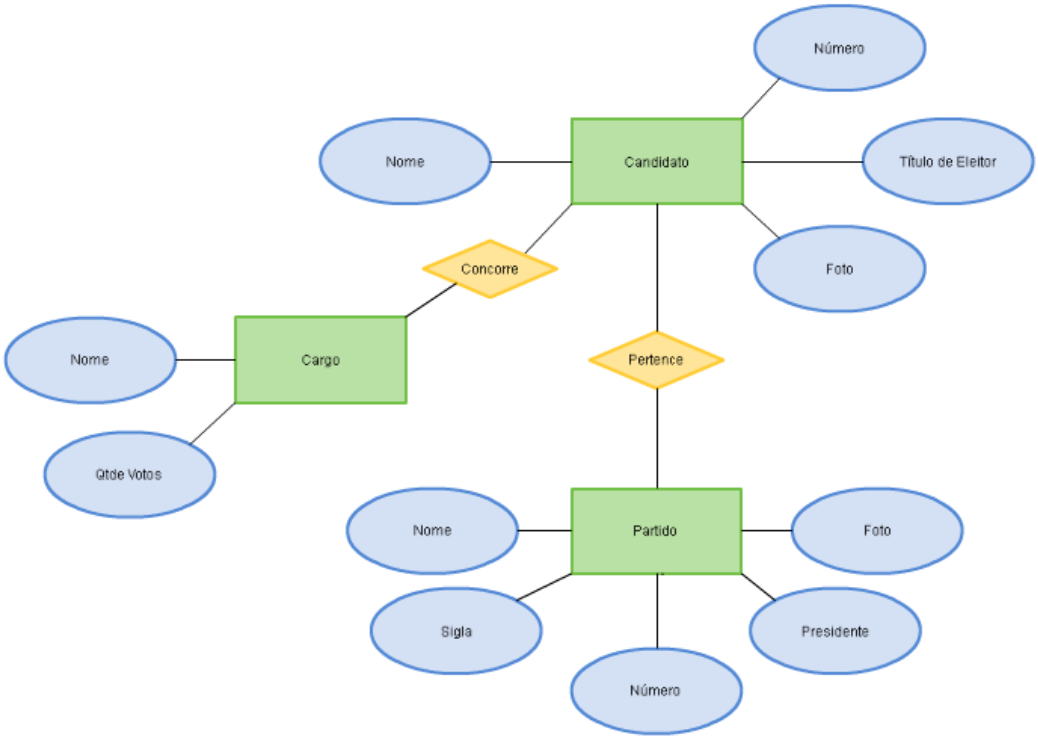


Figura 6: Modelo Entidade Relacionamento da base de dados apresentando os campos relacionados ao registro de candidatos e seu relacionamento com o cadastro de partidos e cargos.

A Figura 7 mostra a implementação da tela de Setup de Eleição, onde é possível escolher entre as opções Apagar Eleição, para apagar a base de dados de eleições anteriores, Cadastrar Partido, Cadastrar Cargo, Cadastrar Candidato e Sair.

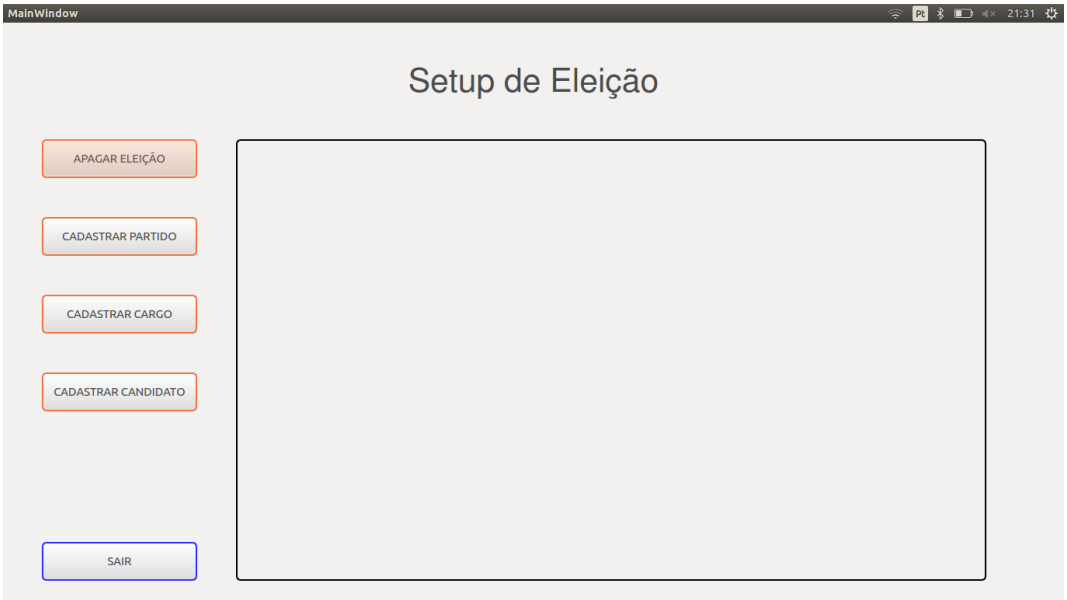


Figura 7: Tela de Setup de Eleição.

As Figuras 8 e 9 apresentam um fluxograma para cadastro de partidos e a implementação da tela Cadastro de Partido.

Ao inserir um partido, é importante lembrar que o número do partido é a chave primária da tabela de partidos no banco de dados, de forma que não é possível cadastrar dois partidos com o mesmo número.

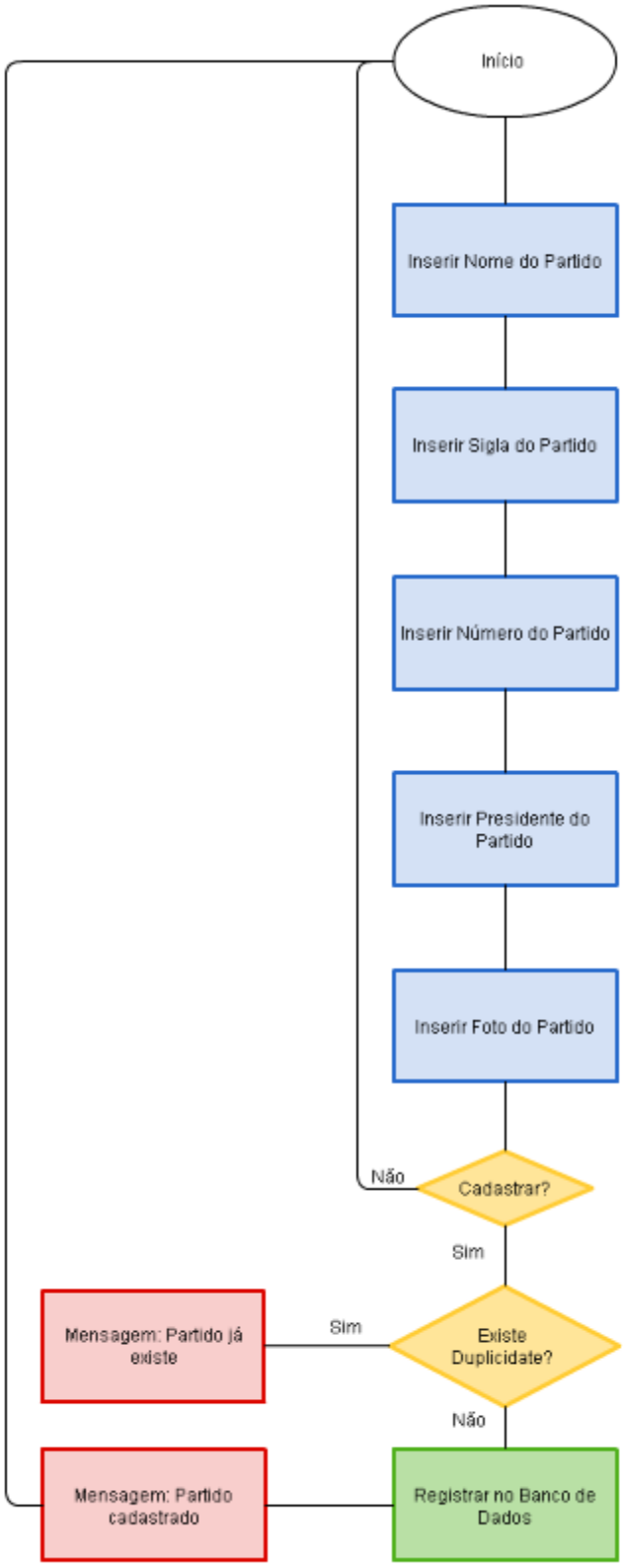


Figura 8: Diagrama de fluxo de dados para cadastro de partidos.

Figura 9: Tela de Cadastro de Partido

As Figuras 10 e 11 apresentam um fluxograma para cadastro de cargos e a implementação da tela Cadastro de Cargos.

Ao inserir um cargo, é oferecida a opção “Qtde. de vezes a ser votado”. Essa opção faz com que seja possível votar em mais de um candidato para o mesmo cargo. Esse recurso foi implementado devido a sua recorrente necessidade em eleições da UFABC, onde eleitores podem votar em mais de uma pessoa para um mesmo cargo. Vale lembrar, no entanto, que esse mesmo recurso pode ser utilizado para eleições de Deputados Federais, por exemplo, onde os eleitores podem votar em mais de um candidato.

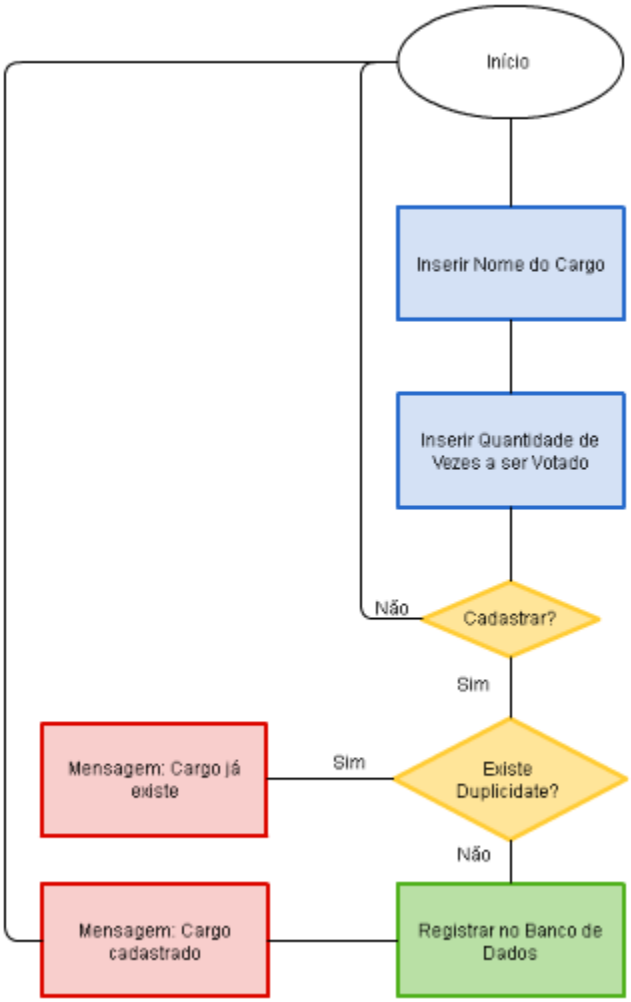


Figura 10: Diagrama de fluxo de dados para cadastro de cargos.

Figura 11: Tela Cadastro de Cargos

As Figuras 12 e 13 apresentam um fluxograma para cadastro de candidatos e a implementação da tela Cadastro de Candidato.

Ao inserir um candidato, é importante lembrar que o título do candidato e o número do candidato devem ser únicos na tabela de candidatos no banco de dados, de forma que não é possível cadastrar dois candidatos com o mesmo título ou com o mesmo número. As caixas de listagem “Cargo” e “Partido” mostram cargos e partidos cadastrados anteriormente. Caso não haja nenhum cargo e / ou partido cadastrados, não é possível inserir um candidato.

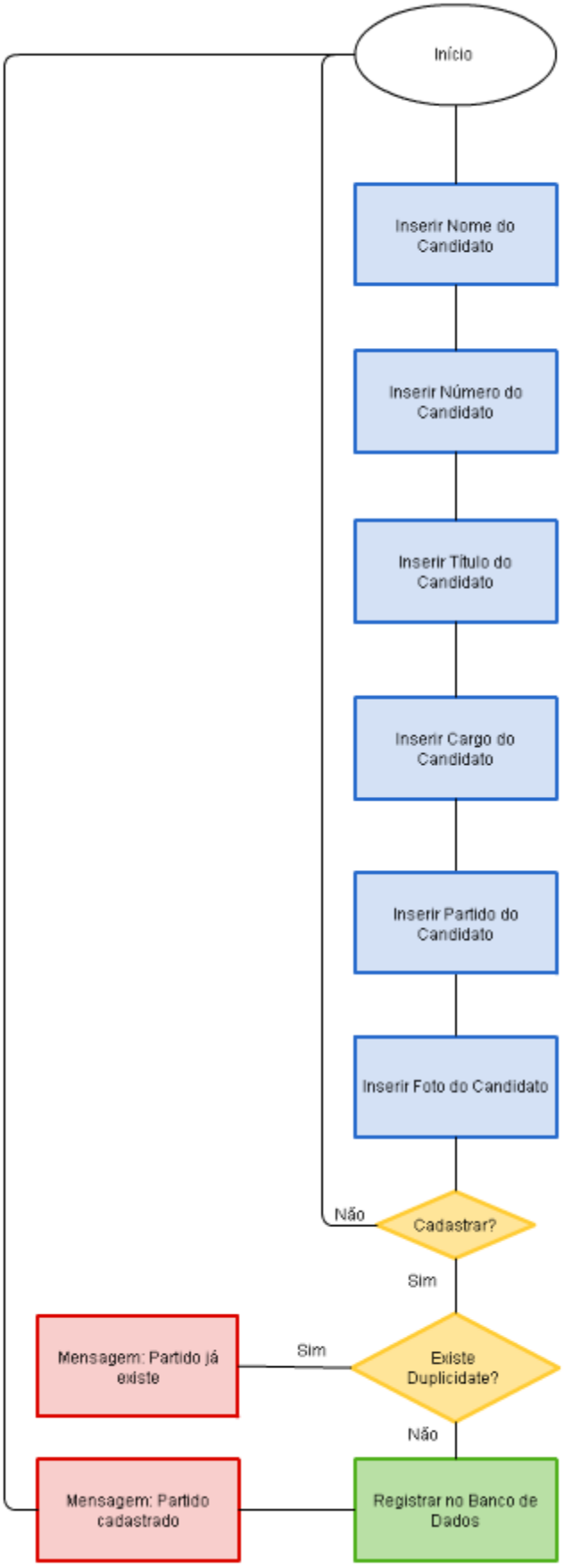

Início
Inserir Nome do Candidato
Inserir Número do Candidato
Inserir Título do Candidato
Inserir Cargo do Candidato
Inserir Partido do Candidato
Inserir Foto do Candidato
Não
Cadastrar?
Sim
Mensagem: Partido já existe
Sim
Existe Duplicidate?
Não
Mensagem: Partido cadastrado
Registrar no Banco de Dados

Figura 12: Diagrama de fluxo de dados para cadastro de candidatos.

Figura 13: Tela Cadastro de Candidato

3.2.2 Setup de Urna

A Figura 14 mostra a implementação da tela de Setup de Urna, onde são geradas as chaves pública e privada. A chave privada é utilizada pelo sistema de votação para assinar o voto, enquanto que a chave pública é utilizada tanto pelo sistema de verificação quanto pelo sistema de apuração, para validar a assinatura do voto. É importante que a chave privada fique guardada em local seguro, ou mesmo que ela não saia da urna eletrônica. Por outro lado, a chave pública pode ser divulgada, pois dessa forma, caso haja algum problema com a urna eletrônica, outro par de chaves pode ser gerado para dar continuidade à votação sem que os votos anteriores sejam perdidos.

Tipicamente, são utilizadas chaves RSA de 1024 a 4096 bits. No entanto, alguns especialistas acreditam que chaves de 1024 bits podem se tornar quebráveis em um futuro próximo, ou até mesmo já podem ter sido quebradas por algum atacante bem financiado. Logo, o par de chaves é gerado utilizando 2048 bits, de forma que o código QR gerado a partir da assinatura do voto e o voto em si ainda fique reconhecível para a webcam.

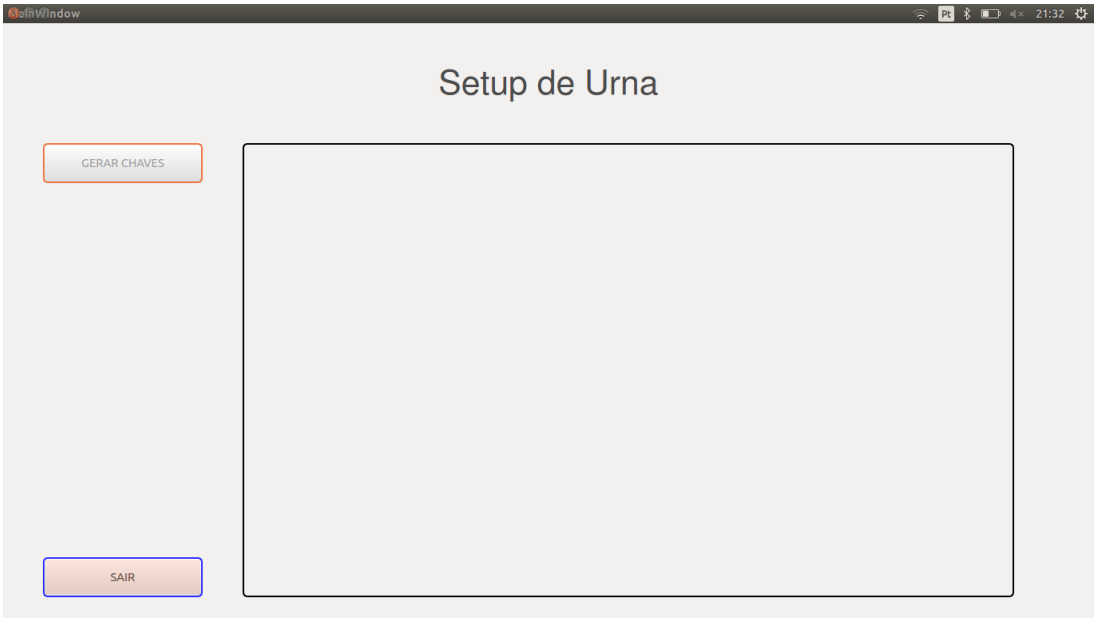


Figura 14: Tela Setup de Urna

3.2.3 Votação e Verificação

Na Figura 15, podemos ver um diagrama de fluxo de dados para a votação. Vale lembrar que o voto é impresso na cédula de duas maneiras diferentes, a primeira é legível ao eleitor e a segunda é em forma de um código QR, para possibilitar processos de verificação diferentes, aonde ao menos um deles feito pelo eleitor, de acordo com as diretrizes do VVSG.

O código QR é gerado a partir de uma *string* assinada utilizando uma chave privada, de forma a não permitir que um voto que não foi assinado possa ser contabilizado. Utilizar o voto assinado também evita que uma pessoa leve um voto feito em casa ou que uma pessoa vote em seções eleitorais diferentes, mesmo que ela tenha acesso à foto de um voto de uma seção diferente, já que cada seção eleitoral deve ter um par de chaves assimétricas diferentes. Além disso, a chave pública poderia ser disponibilizada para qualquer pessoa fazer o seu próprio sistema de verificação de votos ou até mesmo de apuração, no caso de um partido ter dúvidas com relação ao software sendo utilizado.

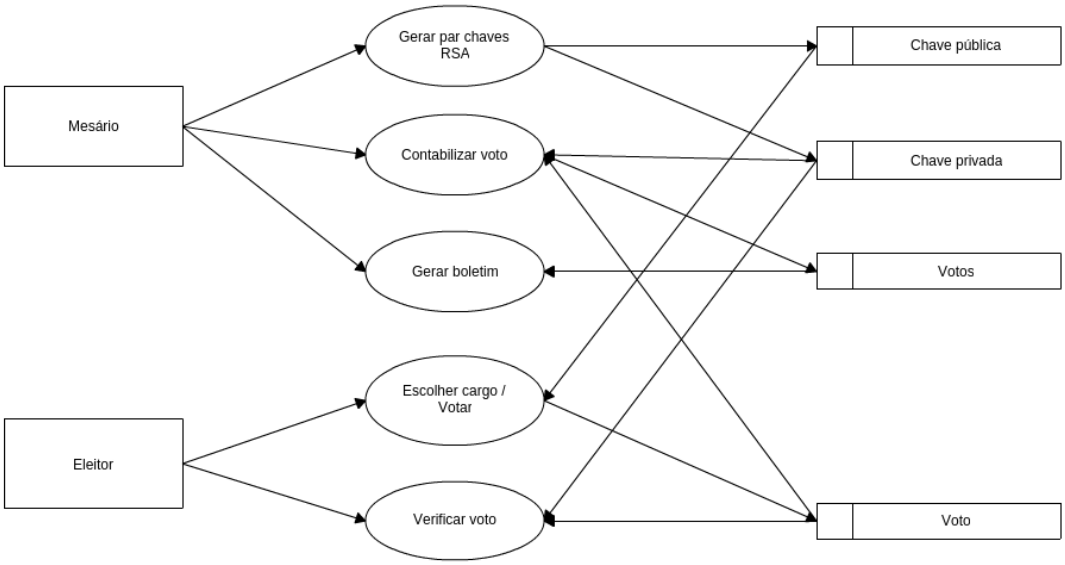


Figura 15: Diagrama de fluxo de dados para a votação.

Já na figura 16, podemos ver como funciona o fluxo de votação, verificação e apuração dos votos através de um diagrama de atividades. Para que o eleitor consiga votar e verificar seu voto, é imprescindível que o mesário gere um par de chaves RSA (pública e privada). O processo de verificação do voto pode ser feito em um outro computador/urna, desde que este possua a chave pública gerada pelo mesário, de forma a conseguir ler a mensagem do código QR.

Após a verificação do voto, o eleitor pode escolher por confirmar seu voto, depositando o mesmo em uma urna, ou votar novamente. Neste caso, é necessário que o eleitor descarte o voto em local seguro e que o mesário não permita que o eleitor deposite dois votos na urna.

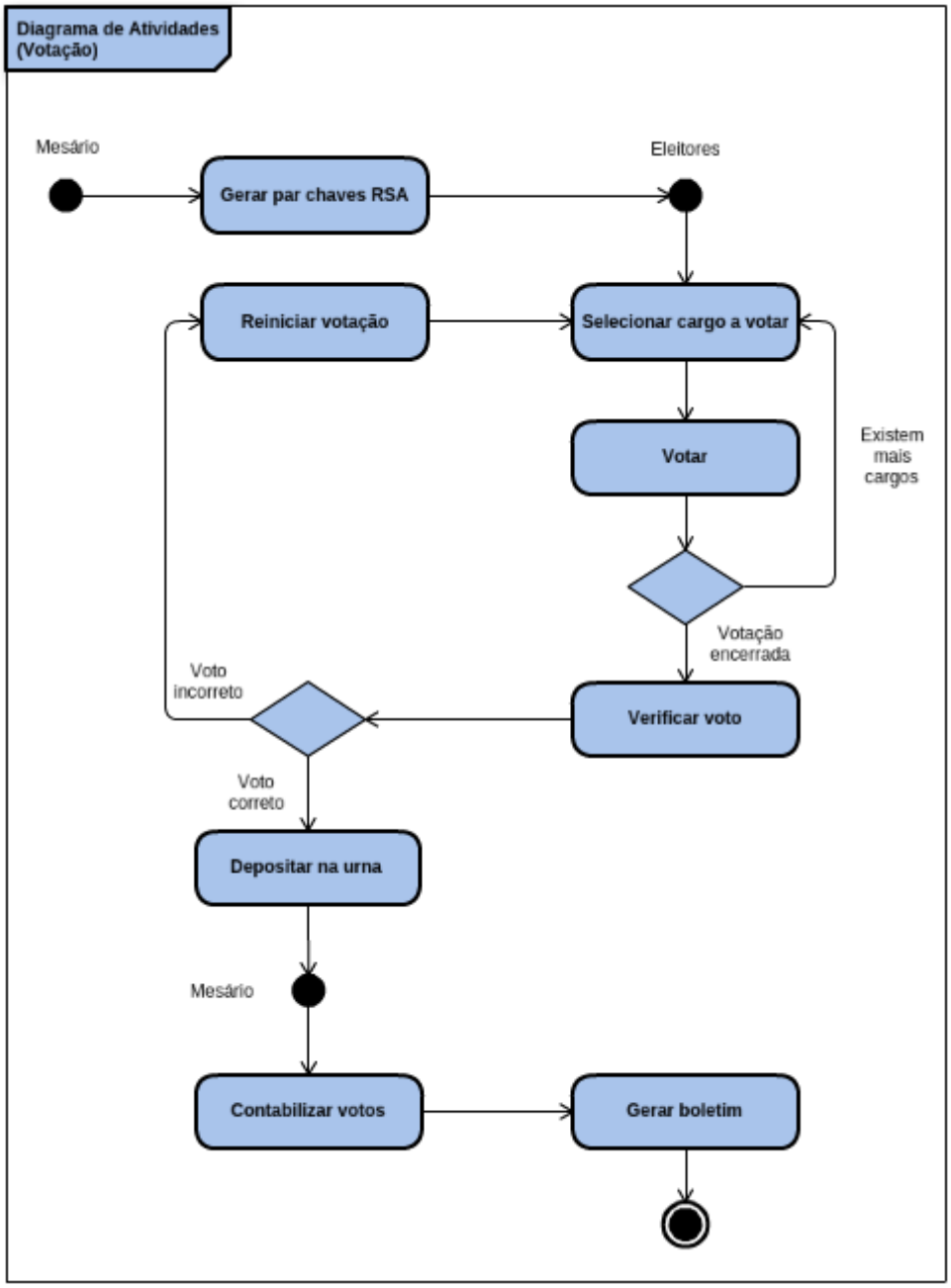


Figura 16: Diagrama de atividades para Votação, Verificação e Apuração dos votos.

As Figuras 17 e 18 mostram implementação das telas de seleção de cargos a serem votados e votação, respectivamente.

Para selecionar o cargo a ser votado, basta pressionar o número correspondente no teclado.

Quando um cargo pode receber mais de um voto, ou seja, quando é possível votar em mais de um candidato para o mesmo cargo, a tela de votação não é encerrada até que todos os votos tenham sido inseridos. É importante lembrar também, que nessa situação, não é possível votar no mesmo candidato mais de uma vez.

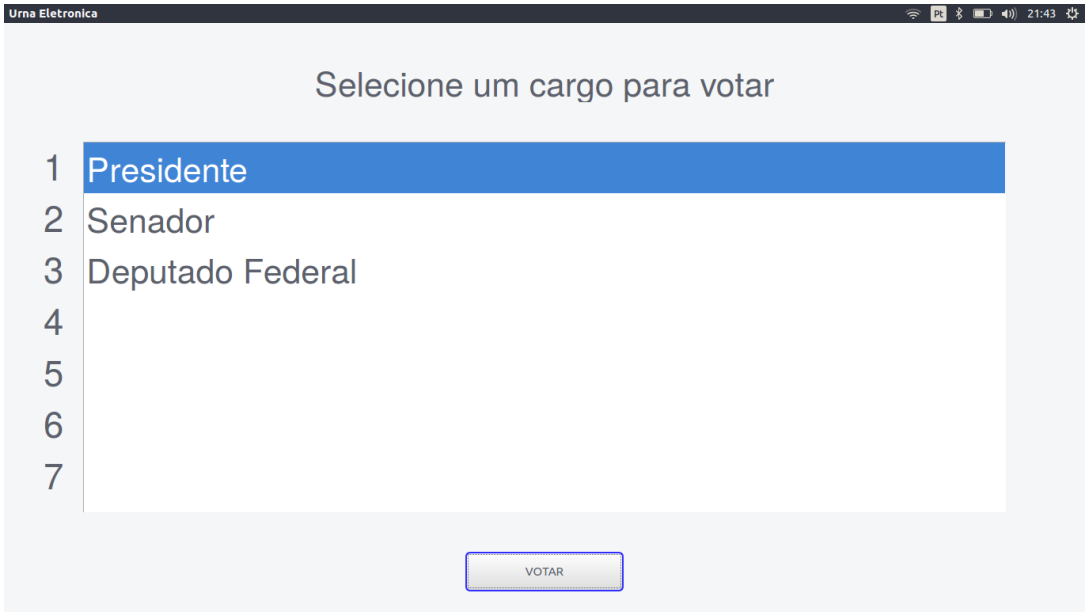


Figura 17: Tela Selecionar Cargo

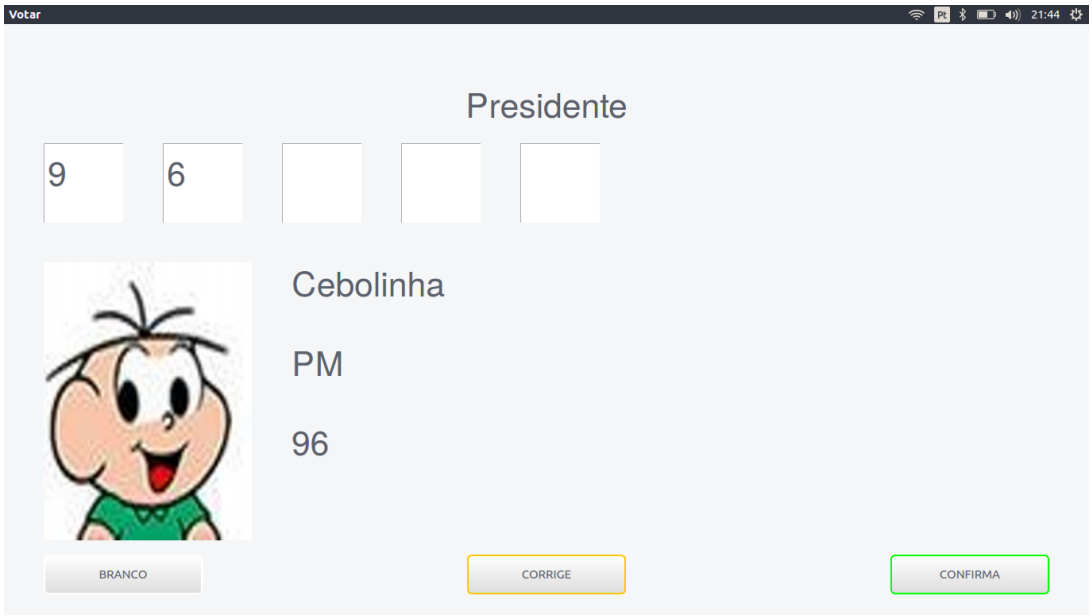


Figura 18: Tela Votação

A Figura 19 mostra um voto depois de impresso. Nesta cédula, temos o voto impresso e legível e um código QR, que contém o a assinatura do voto e o voto.

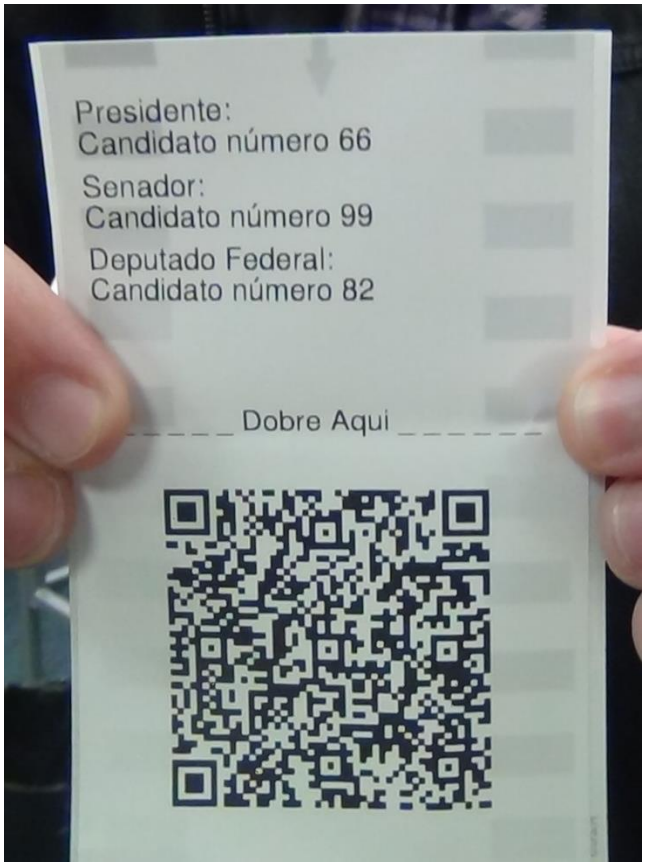


Figura 19: Voto impresso e código QR

A Figura 20 mostra a implementação da tela de Verificação. Ao clicar no botão “Verificar”, será aberta uma tela mostrando a imagem da webcam. O eleitor deve apontar o código QR para a webcam e aguardar que o seu voto seja verificado, mostrando na tela qual foi o seu voto.

Figura 20: Tela Verificação

3.2.4 Apuração

Nessa etapa, o mesário deve ficar responsável por fazer a contabilização dos votos. Novamente, é necessário que esse módulo tenha acesso a chave pública, para o sistema conseguir efetuar a leitura do código QR.

É importante lembrar também, que cada voto recebe uma identificação; inicialmente, foi gerado um número aleatório entre 0 e 1 bilhão, de forma que um voto não possa ser contabilizado duas vezes. A probabilidade de dois ou mais votos terem o mesmo número de identificação, dado que cada seção eleitoral pode ter no máximo 400 pessoas nas capitais - segundo artigo 20 da lei número 1.164, de 24 de julho de 1950 - é de 0.00004%, que é um número estatisticamente relevante, se considerarmos que o Brasil possui cerca de 147 milhões de eleitores[11]. Dessa forma, foi utilizada a função *os.urandom*, gerando uma string de 16 bytes aleatórios, o que resulta em uma probabilidade de $1{,}2 \times 10^{-34}$%. Esses resultados foram obtidos através de um script escrito para o Matlab. O mesmo encontra-se no anexo H.

[11] Valor consultado no site do TSE: <http://www.tse.jus.br/eleitor/estatisticas-de-eleitorado/consulta-quantitativo>

A Figura 21 mostra a implementação da tela de Apuração. Ao clicar no botão “Ler Código”, será aberta uma tela mostrando a imagem da webcam. O responsável pela apuração deve apontar o código QR para a webcam e aguardar que o voto seja computado.

Figura 21: Tela apuração

4. ESTUDO DE CASO

Nos dias 25 e 26 de julho de 2016 ocorreram as eleições para representantes discentes de graduação e de pós-graduação e representantes técnico-administrativos, bem como seus suplentes, para composição do Conselho do CMCC. As eleições ocorreram nos *campi* de Santo André e de São Bernardo do Campo. Mais informações sobre as eleições podem ser vistas nos Anexos.

Nestas eleições, foram utilizados kits de *netbooks* fornecido pelo NTI. O software da urna eletrônica foi disponibilizado no GitHub[12], um serviço de hospedagem para compartilhamento de projetos utilizando versionamento na web, baixado nos *netbooks* e instalados, bem como suas bibliotecas e dependências.

Na Figura 22, podemos ver a estrutura montado para as eleições. Foram utilizados um teclado numérico e um monitor para o eleitor, de forma que ele não tivesse acesso a qualquer outro teclado de computador.

Durante as eleições, o mesário ficou responsável por recolher a assinatura do eleitor antes do voto e por garantir que o voto do mesmo fosse depositado na urna. Após as eleições, coube ao professor Dr. Mario Alexandre Gazziro, presidente da comissão eleitoral, fazer a apuração dos votos e disponibilizar o boletim de urna. O número total de votantes foi de 84, sendo que foram contabilizadas apenas 83 assinaturas. Devido ao fato de que esta discrepância não altera os resultados da eleição, como pode ser verificado no Anexo F, o presidente da comissão eleitoral considerou os dados válidos.

[12] Software pode ser encontrado em <https://github.com/ferfolima/UrnaEletronica3G>

Figura 22: Estrutura da urna eletrônica para as eleições do CMCC na UFABC.

5. CONCLUSÃO

A segurança e confiabilidade de um sistema de votação, incluindo o software, as máquinas, as pessoas envolvidas antes, durante e depois da votação, é muito frágil caso processos bem definidos não estejam estabelecidos com bastante clareza antes das eleições. Nestes processos deve-se definir inclusive o que fazer quando um problema não esperado ocorre. Isso ficou bastante claro nas eleições da UFABC que utilizaram uma urna de terceira geração, e também na análise feita do sistema de votação online utilizado pela Estônia.

Além disso, é possível perceber que a segurança de um sistema de votação, de maneira nenhuma, depende do quão secreto o software é, já que as falhas estarão presentes no software sendo este aberto a público ou não. Mais ainda, quando um código é aberto, muitas pessoas podem analisá-lo e apontar deficiências e melhorias no mesmo.

Por último, fica claro que um software e um sistema simplificados podem ser capazes de prover uma eleição mais confiável e segura do que se ambos fossem extremamente complexos e extensos, como acontece em grande parte dos sistemas de votação utilizados atualmente.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ARTIGOS EM BIBLIOTECAS DIGITAIS

GAZZIRO, M. **Documento de Requisitos da Urna Eletronica de 3o. Geração desenvolvida na UFABC.** Santo André, p. 1-9, out. 2014.

PIETERS, Wolter. **Verifiability of electronic voting: between confidence and trust.** In: DataProtection in a Profiled World. Springer, Dordrecht, p. 157-175. Disponível em: < http://doc.utwente.nl/72498/ > Acesso em: 09 de março de 2015.

SPRINGALL, D.; FINKENAUER, T.; DURUMERIC, Z.; KITCAT, J.; HURSTI, H.; MACALPINE, M.; HALDERMAN, J.A. **Security Analysis of the Estonian Internet Voting System.** Scottsdale, Arizona, EUA, p. 1-11, nov. 2014.

ARTIGOS NA INTERNET

AcceptMidia. Disponível em: <http://acceptmidia.com.br/>. Acesso em: 10 de abril de 2015.

G1. **UnB diz que descobriu fragilidade na segurança da urna eletrônica.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/03/unb-diz-que-descobriu-fragilidade-na-seguranca-da-urna-eletronica.html>. Acesso em: 20 de novembro de 2014.

G1. **A quantidade de urnas utilizadas em 2014.** Disponível em: <http://g1.globo.com/jornal-da-globo/noticia/2014/10/cerca-de-530-mil-urnas-eletronicas-serao-usadas-no-1-turno-das-eleicoes.html>. Acesso em 06 de dezembro de 2014.

Gnome. **Biblioteca GTK para a linguagem Python.** Disponível em: <http://ftp.gnome.org/pub/GNOME/binaries/win32/pygtk/2.24/>. Acesso em: 17 de maio de 2015.

HDF. **The HDF Group.** Disponível em: <https://www.hdfgroup.org/products/java/release/download.html>. Acesso em: 23 de maio de 2015.

Info Escola. **A urna eletrônica.** Disponível em: <http://www.infoescola.com/politica/urna-eletronica/>. Acesso em: 19 de novembro de 2014.

Instituto de Pesquisas Tecnológicas. **Proteção para as urnas.** Disponível em: <http://www.ipt.br/noticias_interna.php?id_noticia=590>. Acesso em: 06 de abril de 2015.

IstoÉ Independente. **As urnas são seguras mesmo?.** Disponível em: <http://www.istoe.com.br/reportagens/243315_AS+URNAS+SAO+SEGURAS+MESMO+>. Acesso em: 12 de março 2014.

MPF. **Campanha por uma disputa justa.** Disponível em: <http://eleitoral.mpf.mp.br/campanha-mpf-por-uma-disputa-justa/cartilha-eleitoral/cartilha_eleicoes_2014_web.pdf>. Acesso em: 26 de novembro de 2014.

O Globo. **Novos municípios do Brasil.** Disponível em: <http://oglobo.globo.com/brasil/com-5-novos-municipios-brasil-agora-tem-5570-cidades-7235803>. Acesso em: 26 de novembro de 2014.

PDT. **Urna eletrônica segura é desenvolvida na Universidade do ABC.** Disponível em: <http://www.pdt.org.br/noticias/urna-eletronica-segura-e-desenvolvida-na-universidade-do-abc>. Acesso em: 27 de fevereiro de 2015.

Portal PUC Rio Digital. **O dia do voto.** Disponível em: <http://puc-riodigital.com.puc-rio.br/Fotojornalismo/O-dia-do-voto-7986.html?gtag=0154#.VSxGd9zF9e8>. Acesso em: 13 de abril de 2015.

Python. **Download da plataforma Python versão 2.7.9.** Disponível em: <https://www.python.org/ftp/python/2.7.9/python-2.7.9.msi>. Acesso em: 17 de maio de 2015.

Python. **Pacotes para linguagem Python.** Disponível em: <https://pypi.python.org/pypi>. Acesso em: 17 de maio de 2015.

Qt. **The Qt Company.** Disponível em: <https://www.qt.io/download-open-source/>. Acesso em: 24 de maio de 2015.

QR Code Generator. **The QR Code Generator.** Disponível em: <https://www.the-qrcode-generator.com/scan>. Acesso em: 09 de junho de 2015.

SQLAlchemy. **The Python SQL Toolkit and Object Relational Mapper.** Disponível em: <http://www.sqlalchemy.org/>. Acesso em: 20 de julho de 2016.

SQLite. **About SQLite.** Disponível em: <https://www.sqlite.org/about.html>. Acesso em 20 de julho de 2016.

Spyratus Digital. **20 vantagens para se utilizar o novo código de barras "QR Code".** Disponível em: <https://spyratus.wordpress.com/2012/08/11/20-vantagens-para-se-utilizar-o-novo-codigo-de-barras-qr-code/>. Acesso em: 28 de fevereiro de 2015.

TechMundo. **Os sinais de Haptics.** Disponível em: <http://www.tecmundo.com.br/touchscreen/9111-haptics-a-resposta-na-ponta-dos-seus-dedos.htm>. Acesso em: 19 de abril de 2015.

Terra. **O sigilo do voto.** Disponível em: <http://tecnologia.terra.com.br/urna-eletronica-brasileira-nao-assegura-sigilo-de voto,a70829b92696b310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 23 de novembro de 2014.

TSE. **A história da urna eletrônica.** Disponível em: <http://www.tse.jus.br/noticias-tse/2014/Junho/conheca-a-historia-da-urna-eletronica-brasileira-que-completa-18-anos>. Acesso em: 21 de novembro de 2014.

TSE. **Estatísticas eleitorais.** Disponível em: <http://www.tse.jus.br/eleicoes/estatisticas/estatisticas-eleitorais-2014-eleitorado>. Acesso em: 26 de novembro de 2014.

TSE. **Galeria de Fotos.** Disponível em: <http://www.tse.jus.br/noticias-tse/galerias/serie-urna-eletronica>. Acesso em: 20 de janeiro de 2015.

UNB. **UnB quebra sigilo de urna eletrônica em testes organizados pelo TSE.** Disponível em: <http://www.unb.br/noticias/unbagencia/unbagencia.php?id=6375>. Acesso em: 09 de abril de 2015.

UOL. **O aumento do número de eleitores.** Disponível em: <http://eleicoes.uol.com.br/2014/noticias/2014/07/18/numero-de-eleitores-cresceu-5-desde-a-ultima-eleicao-para-presidente.htm> Acesso em: 21 de novembro de 2014.

Veja. **Entre todos os países que adotaram o voto eletrônico, o Brasil é o único que ainda utiliza urnas que podem ser manipuladas.** Disponível em: <http://veja.abril.com.br/blog/augusto-nunes/opiniao-2/entre-todos-os-paises-que-adotaram-o-voto-eletronico-o-brasil-e-o-unico-que-ainda-utiliza-urnas-que-podem-ser-manipuladas/>. Acesso em: 09 de abril de 2015.

Veja. **Sistemas biométricos não são seguros como imaginamos, diz especialista.** Disponível em: <http://veja.abril.com.br/noticia/vida-digital/leitores-de-impressoes-digitais-sao-muito-faceis-de-enganar-diz-pesquisador/>. Acesso em: 11 de abril de 2015.

Wiki. **RSA.** Disponível em: <https://pt.wikipedia.org/wiki/RSA/>. Acesso em: 16 de dezembro de 2015.

FILHO, A.B. **Modelos e Gerações dos equipamentos de votação eletrônica.** Disponível em: <http://www.brunazo.eng.br/voto-e/textos/modelosUE.htm>. Acesso em: 22 de julho de 2016.

TSE. **Conheça a história da urna eletrônica brasileira, que completa 18 anos.** Disponível em: <http://www.tse.jus.br/imprensa/noticias-tse/2014/Junho/conheca-a-historia-da-urna-eletronica-brasileira-que-completa-18-anos>. Acesso em 22 de julho de 2016.

LIVROS

CASTELLS, Manoel. **Sociedade em rede.** Tradução de Roneide Venancio Majer e Klauss Brandini Gerhardt. São Paulo: Paz e Terra, 1999.

REZENDE, Denis A.; ABREU, Aline F. de. **Tecnologia da Informação: Aplicadas a Sistemas de Informação Empresariais.** São Paulo: Atlas, 2000.

PERIÓDIOCOS NA INTERNET

Revista Eletronica Total. Brasília. Departamento de Ciencia da Computação. Universidade de Brasília. 2006. Disponível em: <http://www.cic.unb.br/~rezende/trabs/entrevistaET.html>. Acesso em: 16 de janeiro de 2015.

Semana Academica. **O processo da evolução tecnológica.** Disponível em: <http://semanaacademica.org.br/o-processo-da-evolucao-tecnologica>. Acesso em: 08 de janeiro de 2015.

SIMPÓSIOS

FILHO, A.B.; GAZZIRO,M. **Critérios para Avaliação de Sistemas Eleitorais Digitais**. In: XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2014. Santo André – SP. **Anais** ... Santo André: UFABC, 2014. p. 599-610.

ANEXO A – BOLETIM DE SERVIÇO

FUNDAÇÃO UNIVERSIDADE FEDERAL DO ABC

BOLETIM DE SERVIÇO

Nº 565 - 24 de junho de 2016

ANEXO B – COMUNICAÇÃO INTERNA No. 123/2016/CMCC

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Direção do CMCC
Avenida dos Estados, 5001 - Bairro Bangu - Santo André - SP
CEP 09210-580 - Fone: (11) 4996-7953
direcao.cmcc@ufabc.edu.br

Comunicação Interna nº 123/2016/CMCC

Santo André, 05 de julho de 2016.

Ao Núcleo de Tecnologia da Informação

Assunto: **Solicitação de kit de urna eletrônica**

Prezados,

Solicitamos a disponibilização de quatro kits de urna eletrônica para a eleição da representação discente no Conselho de Centro do CMCC.

Data da eleição: 20 de julho de 2016

Regra da eleição: os eleitores poderão votar em no máximo duas chapas, sendo que eleitores discentes de graduação só podem votar nos representantes discentes de graduação e eleitores discentes de pós-graduação só poderão votar nos representantes discentes de pós-graduação.

Quantidade de KITs, correspondente ao número de seções: 2 kits na seção do campus de São Bernardo do Campo e 2 kits na seção do campus de Santo André, sendo 1 kit para cada categoria.

Quantidade e nome dos candidatos: informaremos assim que forem homologadas as inscrições.

Identificação do responsável pela interface com o NTI e nome dos membros da comissão eleitoral: a interface será a secretária executiva Patrícia Dias dos Santos e os membros da Comissão: Mario Alexandre Gazziro, matrícula SIAPE nº 1061139; a servidora técnica-administrativa Acsa Pereira de Almeida, matrícula SIAPE nº 1941784 e a aluna de graduação Maria Fernanda Pinho, matrícula nº 21003414, sob a presidência do primeiro.

Data e horário limite para a disponibilização das urnas e do inicio do escrutínio: 20 de julho de 2016 e o horário limite para montagem das urnas é às 9h, pois a eleição será realizada das 10h ás 19h.

Universidade Federal do ABC

Os locais de instalação das seções (unidade, bloco, sala, andar, torre): piso térreo do Bloco A e piso térreo do Bloco Alpha1.

Atenciosamente,

Prof. Edson Pinheiro Pimentel
Diretor do CMCC

ANEXO C – PORTARIA DO CMCC No. 24 DE 23 DE JUNHO DE 2016

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Centro de Matemática, Computação e Cognição
Av. dos Estados, 5001 - Bairro Bangu - Santo André - SP
CEP 09210-580 - Fone: (11) 4996.7952
secretariacmcc@ufabc.edu.br

PORTARIA DO CMCC Nº 24 DE 23 DE JUNHO DE 2016.

Nomeia, no âmbito do CMCC da Fundação Universidade Federal do ABC, comissão eleitoral para organizar a eleição pra representação discente e técnico-administrativa no ConCMCC.

O DIRETOR DO CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO, nomeado pela portaria nº 834, publicada no Diário Oficial da União, Seção 2, de 29 de novembro de 2013, no uso de suas atribuições legais e estatutárias e considerando:

- o disposto na Resolução do CONSUNI nº 23, publicada no boletim de serviço nº 64 de 17 de junho de 2009, que estabelece a composição mínima dos Conselhos de Centro;

RESOLVE:

Art. 1º. Regulamentar a eleição dos representantes discentes de graduação e de pós-graduação e representantes técnico-administrativos, bem como de seus suplentes, para composição do Conselho do CMCC.

Art. 2º. Designar o professor Mario Alexandre Gazziro, matrícula SIAPE nº 1061139; a servidora técnica-administrativa Acsa Pereira de Almeida, matrícula SIAPE nº 1941784 e a aluna de graduação Maria Fernanda Pinho, matrícula nº 21003414 para comporem a comissão eleitoral responsável pela condução do processo, sob a presidência do primeiro.

Art. 3º Esta Portaria entra em vigor a partir da data de sua publicação.

Edson Pinheiro Pimentel
Diretor

ANEXO D – PORTARIA DO CMCC No. 25 DE 23 DE JUNHO DE 2016

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Centro de Matemática, Computação e Cognição
Av. dos Estados, 5001 - Bairro Bangu - Santo André - SP
CEP 09210-580 - Fone: (11) 4996.7953
direcao.cmcc@ufabc.edu.br

PORTARIA DO CMCC Nº 25 DE 23 DE JUNHO DE 2016.

Regulamenta, no âmbito do CMCC da Fundação Universidade Federal do ABC, a eleição dos representantes discentes de graduação e de pós-graduação e técnico-administrativos bem como de seus suplentes, para composição do Conselho do CMCC.

O DIRETOR DO CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO, nomeado pela portaria nº 834, publicada no Diário Oficial da União, Seção 2, de 29 de novembro de 2013, no uso de suas atribuições legais e estatutárias e considerando:

- o disposto na Resolução do CONSUNI nº 23, publicada no boletim de serviço nº 64 de 17 de junho de 2009, que estabelece a composição mínima dos Conselhos de Centro;

RESOLVE:

Art. 1º. Regulamentar a eleição dos representantes discentes de graduação e de pós-graduação e dos servidores técnico-administrativos, bem como de seus suplentes, para composição do Conselho do CMCC, nos termos do anexo I.

Art. 2º Esta portaria entra em vigor na data de sua publicação.

Edson Pinheiro Pimentel
Diretor

Universidade Federal do ABC

ANEXO I

1. Das vagas:

Representante	Vagas titulares	Vagas suplentes	Mandato
Discente de graduação	2	2	1 ano (até 31/07/2017)
Discente de pós-graduação	2	2	1 ano (até 31/07/2017)
Técnicos-Administrativos	2	2	1 ano (até 31/07/2017)

2. Do cronograma das eleições:

De 04/07/2016 a 11/07/2016	Inscrição dos candidatos
12/07/2016	Análise das inscrições
13/07/2016	Divulgação dos candidatos inscritos
De 14/07/2016 a 22/07/2016	Campanha eleitoral
25/07/2016 e 26/07/2016	Votação
27/07/2016	Apuração
28/07/2016	Divulgação dos resultados
29/07/2016	Conclusão das atividades da comissão eleitoral, mediante apresentação de relatório final à Direção do CMCC

3. Das inscrições

3.1. As inscrições serão efetuadas a partir do dia 04/07/2016 e até as 23h59m do dia 11/07/2016, através de formulário eletrônico disponível nos links:
- discentes: https://docs.google.com/forms/d/1JqbpT-JEaYQbhzAZM8cBnShaZtkxlewB6u8BYbIZPIos
- TAs: https://docs.google.com/forms/d/1jAaIf18Xqj4ymFvRdrXtorx6yWj5Hxh7d3I2Q-dkq1A

3.2. As inscrições ocorrerão mediante chapas, a serem compostas por um titular e um suplente;

3.3. Não serão aceitas as inscrições:

3.4.1. Cujos formulários estiverem preenchidos de forma incorreta;
3.4.2. Realizadas fora do prazo estabelecido;
3.4.3. Que constem apenas titulares, sem suplentes.

3.5. As inscrições serão avaliadas e deferidas exclusivamente pela Comissão Eleitoral responsável pelo processo.

3.6. Findo o período de inscrições, a Comissão Eleitoral divulgará a lista das inscrições deferidas no site http://cmcc.ufabc.edu.br/.

3.7. Recursos de qualquer natureza serão analisados pela Comissão Eleitoral, desde que protocolados no local de inscrição no prazo de 24 (vinte e quatro) horas, a contar da data da divulgação da lista de inscrições deferidas.

4. Da campanha eleitoral

4.1. Os candidatos poderão distribuir panfletos, utilizar cartazes, faixas e outros meios de divulgação na UFABC, inclusive eletrônicos, sem danificar bens da Universidade e atentando-se às normas de ética estabelecidas.

4.2. É vetada a propaganda sonora dentro do campus da UFABC, bem como qualquer outra que perturbe as atividades didáticas e administrativas.

5. Da votação

5.1. A votação será por meio de sistema eletrônico on-line que será disponibilizado no dia previsto no cronograma, das 00h00 as 23h59 através de um link disponível no site http://cmcc.ufabc.edu.br/.

5.2. Na impossibilidade de realização da votação pelo sistema online na data prevista, esta será reagendada dentro do prazo de cinco dias úteis.

5.3. Na inviabilidade da votação ocorrer pelo sistema online esta ocorrerá através de urnas eletrônicas ou votações em papel, em locais e horários a serem amplamente divulgados.

Parágrafo único – Caso a votação seja realizada por meio de urna eletrônica ou cédulas de papel, o votante deverá se apresentar ao local indicado em divulgação, na data e horário estabelecidos, portando documento com foto.

5.4. Os eleitores votarão apenas nos candidatos de sua respectiva categoria, ou seja, somente discentes e técnico-administrativos (lotados no CMCC) poderão votar.

5.5. Os eleitores poderão votar em no máximo duas das chapas inscritas.

5.6. Os eleitores somente poderão utilizar para votação máquinas pertencentes à rede da UFABC.

5.7. A votação não será realizada no caso de haver número menor ou igual de candidatos inscritos, em relação ao número de vagas, hipótese em que os inscritos serão eleitos automaticamente.

6. Do direito a voto

6.1. Somente poderão votar discentes que estejam em situação regular na UFABC, de acordo com lista de votantes publicada antecipadamente no site http://cmcc.ufabc.edu.br/.

6.2. Somente poderão votar os discentes matriculados em cursos de graduação e de pós-graduação da UFABC.

6.3. Somente poderão votar os técnicos-administrativos lotados no CMCC.

6.4. O discente cujo nome não constar na lista de votantes deverá protocolar na Diretoria do CMCC, até o dia 20/07/2016, solicitação de inclusão do nome na lista direcionada ao Presidente da Comissão Eleitoral juntamente com documento comprobatório da situação regular na UFABC (para discentes, comprovante de matrícula na UFABC).

7. Da apuração dos votos e da divulgação dos resultados

7.1. A apuração dos votos será realizada em sala e horário a serem definidos pela Comissão Eleitoral.

7.2. A divulgação dos resultados será realizada por meio do site http://cmcc.ufabc.edu.br/.

7.3. Recursos de qualquer natureza serão analisados pela Comissão Eleitoral, desde que protocolados no local de inscrição no prazo de 24 (vinte e quatro) horas a contar da data da divulgação dos resultados.

7.4. Concluídos a apuração, a contabilização dos votos e o julgamento de possíveis pedidos de impugnações, a Comissão Eleitoral deverá encaminhar à Direção do CMCC ata circunstanciada da sessão de apuração dos votos, contendo os nomes dos eleitos e o total dos votos brancos e nulos.

7.5. Em caso de empate no resultado da votação das categorias discente de graduação e discente de pós-graduação, será considerada a seguinte ordem de desempate:
1°- titular com maior tempo de matrícula na UFABC;
2°- titular de idade mais avançada;
3°- suplente com maior tempo de matrícula na UFABC;
4°- suplente de idade mais avançada.

7.6. Em caso de empate no resultado da votação da categoria técnico-administrativa, será considerada a seguinte ordem de desempate:
1°- titular com maior tempo de exercício na UFABC;
2°- titular de idade mais avançada;
3°- suplente com maior tempo de exercício na UFABC;

4°- suplente de idade mais avançada.

8. Disposições Finais

8.1. Os membros da Comissão Eleitoral são inelegíveis. Para se candidatarem, faz-se necessário requerer dispensa das atividades da Comissão.

8.2. Se o número de candidatos for igual ou menor ao número de vagas, estes automaticamente estarão eleitos sem a necessidade de votação.

8.4. Todas as divulgações serão realizadas em meio eletrônico oficial da UFABC.

8.3. Os casos omissos serão decididos pela Comissão Eleitoral.

ANEXO E – ERRATA DA PORTARIA No. 25 DE 23 DE JUNHO DE 2016

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Centro de Matemática, Computação e Cognição
Av. dos Estados, 5001 - Bairro Bangu - Santo André - SP
CEP 09210-580 - Fone: (11) 4996.7953
direcao.cmcc@ufabc.edu.br

ERRATA DA PORTARIA Nº 25 DE 23 DE JUNHO DE 2016 PUBLICADA NO BOLETIM DE SERVIÇO Nº 565 DE24 DE JUNHO DE 2016

Errata da Portaria CMCC nº 25 de 23 de junho de 2016.

O DIRETOR DO CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO, nomeado pela portaria nº 834, publicada no Diário Oficial da União, Seção 2, de 29 de novembro de 2013, no uso de suas atribuições legais e estatutárias e considerando:

- No item "2. Do cronograma das eleições", onde se lê:

De 04/07/2016 a 11/07/2016	Inscrição dos candidatos
12/07/2016	Análise das inscrições
13/07/2016	Divulgação dos candidatos inscritos
De 14/07/2016 a 22/07/2016	Campanha eleitoral
25/07/2016 e 26/07/2016	Votação
27/07/2016	Apuração
28/07/2016	Divulgação dos resultados
29/07/2016	Conclusão das atividades da comissão eleitoral, mediante apresentação de relatório final à Direção do CMCC

- Leia-se:

De 04/07/2016 a 11/07/2016	Inscrição dos candidatos
12/07/2016	Análise das inscrições
13/07/2016	Divulgação dos candidatos inscritos
De 14/07/2016 a 19/07/2016	Campanha eleitoral
20/07/2016	Votação
21/07/2016	Apuração
22/07/2016	Divulgação dos resultados
01/08/2016	Conclusão das atividades da comissão eleitoral, mediante apresentação de relatório final à Direção do CMCC

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Centro de Matemática, Computação e Cognição
Av. dos Estados, 5001 - Bairro Bangu - Santo André - SP
CEP 09210-580 - Fone: (11) 4996.7953
direcao.cmcc@ufabc.edu.br

- No item 5.1., onde se lê:

5.1. A votação será por meio de sistema eletrônico on-line que será disponibilizado no dia previsto no cronograma, das 00h00 as 23h59 através de um link disponível no site http://cmcc.ufabc.edu.br/.

- Leia-se:

5.1. A votação será por meio de um sistema de urnas eletrônicas a ser disponibilizado pelo Núcleo de Tecnologia da Informação no dia previsto no cronograma, das 10h00 às 13h00 e das 15h00 às 19h00 em locais a serem informados no site http://cmcc.ufabc.edu.br/ no prazo máximo de 24 horas antes da realização da eleição.

- No item 5.2., onde se lê:

5.2. Na impossibilidade de realização da votação pelo sistema online na data prevista, esta será reagendada dentro do prazo de cinco dias úteis.

- Leia-se:

5.2. Na impossibilidade de realização da votação pelo sistema de urnas eletrônicas na data prevista, esta será reagendada dentro do prazo de cinco dias úteis.

- No item 5.3., onde se lê:

5.3. Na inviabilidade da votação ocorrer pelo sistema online esta ocorrerá através de urnas eletrônicas ou votações em papel, em locais e horários a serem amplamente divulgados.

- Leia-se:

5.3. Na inviabilidade da votação ocorrer pelo sistema de urnas eletrônicas esta ocorrerá através de urnas convencionais e cédulas em papel, em locais e horários a serem amplamente divulgados.

Edson Pinheiro Pimentel

Diretor do CMCC

ANEXO F – ATA No. 02/2016

CENTRO DE MATEMÁTICA, COMPUTAÇÃO E COGNIÇÃO
(CMCC)

Comissão Eleitoral para o Conselho de Centro do CMCC

ATA Nº 02/2016

Aos vinte e um dias do mês de julho do ano de dois mil e dezesseis, no horário das treze horas e vinte minutos, na sala de reuniões 502-2, localizada no quinto andar da torre dois do Bloco A da Universidade Federal do ABC - UFABC, situada à Avenida dos Estados, cinco mil e um, Bairro Bangu, Santo André, São Paulo, realizou-se a reunião da Comissão Eleitoral para a eleição da representação discente do Conselho de Centro do CMCC, previamente convocada e presidida pelo presidente o professor Mario Alexandre Gazziro. Ausência justificada da técnica-administrativa Acsa Pereira de Almeida e da discente de graduação Maria Fernanda Pinho. Segue abaixo a tabela com a contabilização dos votos:

Chapas	Número de votos
Vanessa Carneiro Morita (titular) e Esaú Sirius Ventura Pupo (suplente)	82
Luiz Henrique Fonseca (titular) e Jeferson Guimarães de Souza (suplente)	76
João Antonio Machado Cardoso Filho (titular) e Paulo Leal Taveira (suplente)	0
Brancos	8
Nulos	2
Total de votos	168

O número total de votantes foi de oitenta e quatro discentes, porém ao conferirmos a folha de assinaturas, foi constatado que havia apenas oitenta e três assinaturas. O Presidente da Comissão Eleitoral optou então por considerar todos os dados válidos uma vez que essa diferença entre um voto e uma assinatura não alteraria o resultado. Foram eleitas as seguintes chapas: Vanessa Carneiro Morita (titular) e

1

Esaú Sirius Ventura Pupo (suplente) e Luiz Henrique Fonseca (titular) e Jeferson Guimarães de Souza (suplente). Nada mais havendo a tratar, o professor Mario Alexandre Gazziro agradeceu a presença de todos e encerrou a sessão às treze horas e quarenta e sete minutos, da qual, para constar, eu, Patrícia Dias dos Santos, secretária executiva deste Centro, lavrei a presente Ata.

Mario Alexandre Gazziro
Presidente da Comissão Eleitoral

Patrícia Dias dos Santos
Secretária Executiva

Fernando Marcate Garcia dos Anjos
Testemunha

ANEXO G – CONGRESSO UFABC DE EMPREENDEDORISMO

PROTÓTIPO DE URNA ELETRÔNICA DE TERCEIRA GERAÇÃO

THIRD GENERATION ELETRONIC VOTING MACHINE PROTOTYPE

Eixo temático: Inovação

M. Gazziro[1], F. Lima[1], E. Martinez[1], R. Pereira[1] (mario.gazziro@ufabc.edu.br)
1.Universidade Federal do ABC, Santo André, Brasil

RESUMO

Foi construído nesse trabalho uma uma eletrônica de terceira geração, com capacidade de elaboração de voto impresso, dentre outras inovações importantes. São apresentados aqui detalhes de seu projeto, como modelagem da base de dados, assim como detalhes técnicos dos componentes de hardware e software envolvidos. Por fim, um teste simulado foi realizado com o sistema, sendo apresentada a cédula devotação impressa gerada pela urna.

1. INTRODUÇÃO

O Brasil atualmente é o único país no mundo ainda a utilizar as chamadas urnas eletrônicas de primeira geração, as quais registram o voto apenas digitalmente, sem deixar rastro em papel para auxiliar no processo de fiscalização partidária ou para uma eventual conferência por recontagem manual, seja de seção eleitoral em particular ou mesmo de toda uma eleição. Embora pareca exagerada a ideia de uma recontagem manual após uma apuração eletrônica, ja aconteceu antes, na Venezuela, onde mesmo tendo utilizado urnas eletrônicas foi necessária uma contagem manual das cédulas impressas pelas urnas devido a suspeitas de fraude eleitoral.

As chamadas urnas de segunda geração, registram o voto tanto digitalmente quanto em forma impressa, e trata-se do modelo mais utilizado hoje no mundo. Porém, eventuais discrepâncias entre o total registrado digitalmente e o total registrado em papel ainda causam discórdia no processo de apuração.

Já as urnas de terceira geração - utilizadas em poucas regiões do mundo - não mantem um registro digital isoladamente, e nem um registro impresso isoladamente, e sim um registro conjunto, digital e em impresso. Isso é possível de ser realizado por diversas maneiras, sendo que podemos citar dois exemplos: utilizar cédulas de votação com chips de RFid embutidos - solução tecnológica adotada pelas urnas argentinas atuais; utilizar cédulas de votação com impressão de códigos de barras - solução adotada no presente trabalho.

Dentre as diversas vantagens de urnas de terceira geração, destaca-se principalmente a possibilidade de fiscalização e conferência, assim como o atendimento ao critério de independência do software. Tal critério estabelece que uma falha ou fraude no sistema eletrônico da urna (hardware ou software) não pode afetar o resultado da eleição.

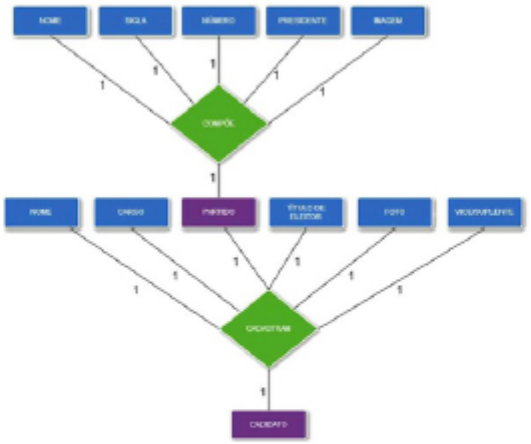
Maiores detalhes sobre os critérios para uma votação eletrônica podem ser encontrados no paper "Critérios para Avaliação de Sistemas Eleitorias Digitais", de [Brunazo], sendo que sua leitura é recomendada para o melhor entendimento desse trabalho.

2. METODOLOGIA

Foi utilizada linguagem de programação Python versão 2.7, com a adição de bibliotecas de terceiros - todas licenciadas como softwares livres: PySide, que fornece acesso a API do framework QT para criação da interface gráfica com o usuário; a biblioteca H5PY, para acesso a API do gerenciador de base de dados HDF5, desenvolvido pelo JPL/NASA - sendo esse último o padrão de base de dados adotado no projeto, adotado por se tratar de um sistema de base de dados tolerante a falhas; e por fim, foi utilizada a biblioteca PyQRTools, para criar e decodificar os símbolos gerados para os padrões de código de barras - no caso foi utilizado o padrão QR, de duas dimensões, por possibilitar um maior volume de dados em menor área do que o padrão convencional de código de barras com uma dimensão.

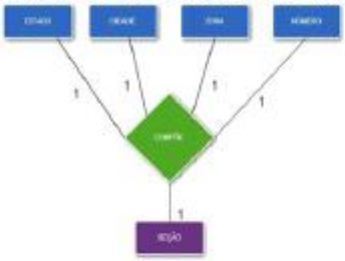
As Figuras 01 e 02 apresentam os modelos de Entidade-Relacionamento utilizados na base de dados, respectivamente para os cadastros de candidatos e partidos, assim como para seções eleitorais.

Figura 01 - Modelo Entidade-Relacionamento da base de dados apresentando os campos relacionados ao registro dos candidatos e seu relacionamento com o cadastro de partidos. Todas as cardinalidades são um-para-um.



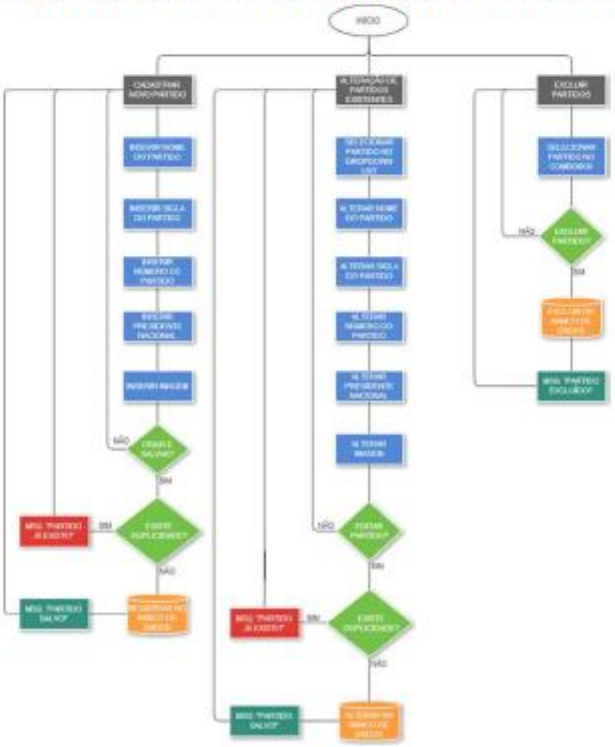
Vale destacar que na Figura 2, a seção eleitoral é definida como sendo uma chave-composta pela união de seus campos, para evitar repetições, visto que o conjunto cidade, estado, zona e número da seção são únicos.

Figura 02 - Modelo Entidade-Relacionamento da base de dados apresentando o cadastro de seção eleitoral, sendo esta uma chave-composta gerada pela união de todos os seus campos.



A Figura 03 a seguir apresenta fluxograma para cadastro, alteração e exclusão de partidos na base de dados. O cadastro, alteração e exclusão de candidatos e seções eleitorais utilizam fluxogramas similares, e, dado a sua simplicidade, foram omitidas desse documento por questões de economia de espaço.

Figura 03. Diagrama de fluxo de dados para cadastro, alteração e exclusão de partidos. Demais itens na base de dados, como candidatos e seção utilizam fluxogramas similares.



3. PROTÓTIPO DESENVOLVIDO

O protótipo desenvolvido consta simplesmente de: 01 computador, 01 impressora térmica e 01 webcam de alta resolução, conforme apresentado na Figura 04 a seguir.

Figura 04. Protótipo de urna de 3o. geração desenvolvido, com destaque para (A) impressora de cédula de votação e (B) webcam de alta-resolução para conferência do código de barras padrão QR impresso na cédula de votação.

O computador deve ser de arquitetura Intel x86 ou compatível, sem qualquer requisito específico de recursos como memória ou velocidade de processamento, sendo que modelos comerciais de prateleira atendem perfeitamente ao projeto.

A impressora térmica pode ser genérica, mas recomendamos o uso de impressoras da marca Brother, por possuir drivers para o sistema operacional Linux constantemente atualizados.

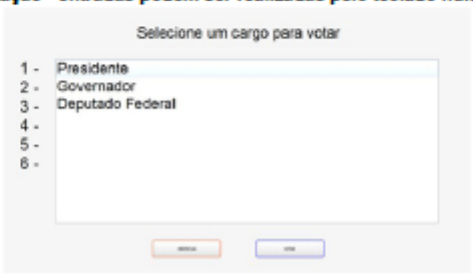
Por fim, a webcam deve obrigatoriamente ser de alta resolução, pois a leitura de códigos de barra de duas dimensões padrão QR-Code demanda esse requisito.

Qualquer modelo atual do mercado que atenda o requisito de filmar com qualidade HD - High Definition 1920x1080 pixels - pode ser utilizada.

Toda a interface gráfica com o usuário foi desenvolvida no ambiente de janelas QT, e recursos de programação gráfica para projeto de interfaces, como ListBox e CanvasBox.

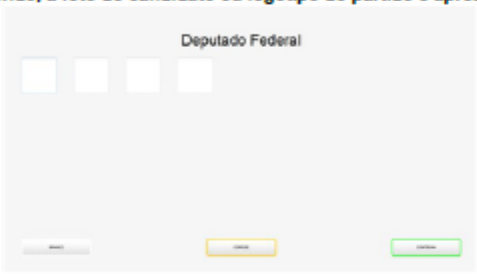
Vale a pena destacar que em nosso protótipo, o eleitor pode escolher a ordem de votação, através da seleção do cargo desejado a se votar, conforme apresentado na Figura 05. A seleção do eleitor pode ser realizada pelo teclado numérico (teclado do próprio computador ou externo numérico, padrão usb, como foi adotado em nosso protótipo).

Figura 05. Tela inicial do software de votação desenvolvida, possibilitando escolha da ordem de votação - entradas podem ser realizadas pelo teclado numérico.



A Figura 06 apresenta a tela de escolha do candidato ou partido, que também é realizada via teclado numérico ou touchscreen. Uma vez selecionado um candidato ou partido válido e constante na base de dados, a foto do candidato ou logotipo do partido é então apresentado ao eleitor, o qual deve ainda confirmar ou corrigir seu voto.

Figura 06. Exemplo de interface para escolha de candidato. Após o número do candidato ou partido ser inserido, a foto do candidato ou logotipo do partido é apresentado na tela.



Após entrar com todas as suas escolhas, o eleitor deve confirmar o conteúdo apresentado na tela e apertar o botão de confirmação (no caso, o número do teclado numérico que representa a confirmação). Em caso de retificação, o software vai guiá-lo para a nova votação do cargo o qual se deseja retificar. Após a confirmação final, é realizada a impressão do voto, sendo exibido nesse momento a mensagem apresentada na Figura 07.

Destacamos aqui que NENHUM registro digital do voto fica armazenado na base de dados da urna, a qual aliás nem tem um campo específico para tal. Toda informação sobre o voto fica única e exclusivamente registrada na cédula de votação impressa, de duas formas: legível e em código de barras.

Figura 07. Mensagem exibida durante impressão da cédula do voto.

Após a impressão da cédula do voto, a qual é apresentada na Figura 08, o eleitor pode conferir os dados na cédula de 3 formas distintas.

- Primeira: ler os nomes dos candidatos e partidos impressos de forma legível na própria cédula de votação.

- Segunda: aproximar a cédula de votação até a câmera da mesma urna em que votou, a qual vai automaticamente detectar código de barras e realizar a sua leitura, apresentando os candidatos e partidos constantes no código de barras da cédula.

- Terceira: aproximar a cédula de votação em qualquer outra urna disponível na seção de votação, para ter plena certeza de que os candidatos e partidos escolhidos estão sendo exibidos por um sistema o qual não tinha conhecimento a priori das suas escolhas.

Figura 08. Exemplo de cédula impressa gerada pela urna após uma votação simulada. Dados da cédula podem ser conferidos visualmente e/ou através da verificação do conteúdo do código de barras QR.

Mesmo após a impressão da cédula ter sido realizada, o eleitor ainda tem o direito de refutar seu voto e votar novamente. Nesse caso, a cédula é destruida e uma nova cédula será gerada após o eleitor selecionar novamente seus candidatos. Só após o eleitor depositar seu voto impresso na urna, seu voto será computado - na fase posterior, de apuração.

Ao término do período de votação, uma apuração local deve ser realizada na própria seção de votação, ocasião na qual o software da urna a converte em um equipamento de apuração. Os resultados das apurações locais devem então seguir para uma central de totalização, também em forma impressa, através da geração de um boletim de urna impresso, com informações também em forma legível e em código de barras.

Para evitar que um mesmo voto seja computado mais de uma vez pelo sistema de apuração, utilizamos um artifício muito simples: adicionamos ao código de barras da cédula de votação um número aleatório muito grande, gerado no momento da impressão do voto. Tal número é armazenado durante a apuração, e se for encontrado novamente, caracteriza que o mesmo voto foi apresentado ao sistema de apuração, e dessa maneira, não computando o mesmo.

Esse número aleatório, por sua vez, não precisa ser grande o suficiente para garantir a separabilidade de todos os eleitores do país inteiro, apenas precisa garantir a separabilidade dos eleitores de uma mesma seção, sendo que números inteiros de 32 bits são estatisticamente suficientes, e não comprometem sua representação em código de barras QR, que podem armazenar até 3.000 bytes na versão 40 com 177 módulos [QRCode Information Capacity].

4. CONCLUSÕES

Foi construído, com sucesso, uma urna eletrônica de terceira geração, a qual atende a todos os critérios estabelecidos para um sistema dessa geração, a destacar sendo mais importante, o princípio da independência do software, ou seja, uma falha ou fraude no sistema eletrônico da urna não consegue comprometer o resultado da eleição.

5. REFERÊNCIAS

Brunazzo F., A. et al - Critérios para Avaliação de Sistemas Eleitorais Digitais. In: Anais do XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2014. pp. 599-610. 2014

QRCode Information Capacity, http://www.qrcode.com/en/about/version.html, acessado em 29/08/2015.

Neumann, P.G. - Security Criteria for Electronic Voting - 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993. - http://www.csl.sri.com/users/neumann/ncs93.html. Acessado em 07/09/14.

CT, Computer Technologists' Statement on Internet Voting – disponível em: http://www.verifiedvoting.org/wp-uploads/2012/09/InternetVotingStatement.pdf 2012

Pieters, W. - Verifiability of electronic voting: between confidence and trust. In: Data Protection in a Profiled World. Springer, Dordrecht, pp. 157-175. ISBN 9789048188642, 2010. - http://doc.utwente.nl/72498/

Três, C.A.- A Soberania do Povo na Fiscalização do Exercício de sua Soberania. In: Seminário do Voto Eletrônico, Câmara dos Deputados, 29 de maio de 2002. - http://www.brunazo.eng.br/voto-e/textos/tres2.htm

TCFA, Decisão original do Tribunal Constitucional Federal da Alemanha, www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html

CMind, Comitê Multidisciplinar Independente. Relatório sobre o Sistema Brasileiro de Votação Eletrônica. Brasília: Edição dos Autores, 2010. Os temas referidos se encontram nas Seções 4.1.1 e 4.1.2, 2010

Aranha, D. et al. - Vulnerabilidades no software da urna eletrônica brasileira. UnB, 2012. 36 pp. - disponível em http://sites.google.com/site/dfaranha/projects/relatoriourna.pdf, 2014

Rivest R.R. , Wack, J.P. - On the notion of "software independence" in voting systems : USA, NIST/MIT, 28/07/2006 - http://people.csail.mit.edu/rivest/pubs/RW06.pdf

Stallman – A Opinião de Richar Stallman - http://www.vialibre.org.ar/2008/11/12/votodigital-la-opinion-de-richard-stallman/

NIST, Voluntary Voting System Guidelines - NIST/US-EAC (2009). - Definição de Independent Verification Systems na Seção 7.8 - http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf

Rezende, P. D. - Votação Eletrônica, 3a Geração. CMind, 2010 – apresentado em cerimônia pública no TSE - http://www.cic.unb.br/docentes/pedro/trabs/TSE3G.pdf

ANEXO H – SCRIPT MATLAB PARA CALCULAR A PROBABILIDADE DE REPETIÇÃO DE VOTO

```
clear all;
clc;
x = 0:400;
bytes = 16
bits = bytes*8;
n = 400;
p = 1/(2^bits);
%Calculo da função densidade de probabilidade
%   somente para plotar gráfico
pdf = binopdf(x,n,p);
stem(x(1:end-300), pdf(1:end-300));
hold on;
%Calculo da função de distribuição cumulativa
%   somente para plotar gráfico
cdf = binocdf(x,n,p);
plot(x(1:end-300), cdf(1:end-300));
hold on;
%Calculo da probabilidade da identificação do voto ser repetida
p_repeticao = binopdf(1,n,p);
plot(0,p_repeticao,'*')
ylim([0,.2e-35])
```