UNIVERSIDADE FUMEC — FUNDAÇÃO MINEIRA DE EDUCAÇÃO E CULTURA
FACULDADE DE CIÊNCIAS EMPRESARIAIS — FACE
MESTRADO EM SISTEMAS DE INFORMAÇÃO E GESTÃO DO CONHECIMENTO

SAMUEL PEREIRA DIAS

PROPOSTA DE SISTEMA DE VOTAÇÃO ELETRÔNICA AUDITÁVEL PARA INSTITUIÇÕES DE ENSINO SUPERIOR

BELO HORIZONTE
2016

SAMUEL PEREIRA DIAS

PROPOSTA DE SISTEMA DE VOTAÇÃO ELETRÔNICA AUDITÁVEL PARA INSTITUIÇÕES DE ENSINO SUPERIOR

Dissertação apresentada ao Programa de Mestrado em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC — Fundação Mineira de Educação e Cultura, como requisito parcial para a obtenção do título de Mestre em Sistemas de Informação e Gestão do Conhecimento.

Área de Concentração: Gestão de Sistemas de Informação e do Conhecimento

Linha de Pesquisa: Tecnologia e Sistemas de Informação

Orientador: Prof. Dr. Luiz Cláudio Gomes Maia

Belo Horizonte

2016

Ficha Catalográfica

D541p Dias, Samuel Pereira.
Proposta de sistema de votação eletrônica auditável para instituições de ensino superior / Samuel Pereira Dias. – Belo Horizonte, 2016.
133 f.: il. (algumas color.).

Orientador: Prof. Dr. Luiz Cláudio Gomes Maia
Dissertação (Mestrado) – Universidade FUMEC – Faculdade de Ciências Empresariais, 2016.

1. Votação eletrônica. 2. Votação auditável. 3. Segurança em votação eletrônica. 4. Institutos Federais. I. Maia, Luiz Cláudio Gomes. II. Título.

CDD 003.3

Elaborada pelo Setor de Biblioteca do IFMG — *Campus* Bambuí

UNIVERSIDADE
FUMEC
DE MINAS GERAIS PARA O MUNDO

Dissertação intitulada "**Proposta de sistema de votação eletrônica auditável para instituições de ensino superior**" de autoria de Samuel Pereira Dias, aprovada pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Luiz Cláudio Gomes Maia – Universidade FUMEC
(Orientador)

Prof. Dr. Orlando Abreu Gomes – Universidade FUMEC
(Examinador Interno)

Prof. Dr. Jeroen Antonius Maria van de Graaf – UFMG
(Examinador Externo)

Gabriel da Silva, Me. – IFMG
(Consultor *Ad Hoc*)

Prof. Dr. Fernando Silva Parreiras
Coordenador do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC

Belo Horizonte, 11 de agosto de 2016.

Rua Cobre, 200 - Cruzeiro
30310-190 - Belo Horizonte- MG
Tel. (31) 3228-3060
www.fumec.br

Nbf zrhf cnvf r snzvyvnerf, nbf zrhf nzvtbf, n gbqbf bf zrzoebf qn pbzhavqnqr pvragvsvpn dhr pbagevohvenz pbz b ninapb qn pevcgbtensvn r crezvgvenz n ernyvmnpnb qrfgr genonyub r n dhrz yre rfgnf yvaunf, qrqvpb.

Agradecimentos

A Deus, por tudo;

aos meus pais, pela dedicação e amor e por terem oferecido muito mais do que tiveram em toda a vida;

aos meus irmãos, pelo incentivo e companheirismo;

às minhas sobrinhas, por sempre receberem, com um sorriso iluminado e cheio de candura, o tio que muitas vezes teve que se fazer ausente nestes meses;

à Diretoria-Geral do IFMG — *Campus* Bambuí, pela oportunidade concedida, em especial ao Prof. Flávio Vasconcelos Godinho, pelo companheirismo e os anos de aprendizagem durante sua gestão;

aos colegas do Núcleo de Computação do Departamento de Engenharia e Computação do *Campus* Bambuí, pelas sugestões e pelo apoio para que este Mestrado pudesse se realizar;

a todos os que contribuíram com este trabalho, de forma direta ou indireta;

aos professores do Mestrado em Sistemas de Informação e Gestão do Conhecimento, por tudo o que partilharam;

e, em especial, ao Prof. Luiz Cláudio Gomes Maia, orientador deste trabalho, que acreditou na proposta e me guiou nesta jornada.

"A estrada deve ser percorrida, mas será muito difícil. E nem a força nem a sabedoria nos levarão muito longe, caminhando por ela. Essa busca deve ser empreendida pelos fracos com a mesma esperança dos fortes. Mas é sempre assim o curso dos fatos que movem as rodas do mundo: as mãos pequenas os realizam porque precisam, enquanto os olhos dos grandes estão voltados para outros lugares." (Elrond, em A Sociedade do Anel, de J. R. R. Tolkien)

Resumo

Um dos pilares da democracia é o exercício do direito ao voto. O objetivo deste trabalho foi determinar as características necessárias a um sistema eleitoral informatizado de baixo custo de implantação, auditável, com registro impresso do voto, visando à segurança e, acima de tudo, à auditabilidade pela comunidade acadêmica das instituições de ensino. Como pano de fundo, utiliza os processos de consulta à comunidade para os cargos de reitor e de diretores-gerais de *campus* dos Institutos Federais de Educação, Ciência e Tecnologia (IF). Através da revisão bibliográfica e documental, esta última na forma da legislação vigente, foi elaborado um protocolo eleitoral como artefato de *Design Science Research*. Foi também realizada uma revisão sistemática de literatura com o objetivo de estabelecer a tendência das tecnologias de votação eletrônica. Como contribuição primária do trabalho, apresenta-se um protocolo eleitoral que abrange todas as fases dos processos de consulta à comunidade e que atende de forma satisfatória os requisitos legais e de segurança. Apresenta-se ainda os requisitos funcionais e não funcionais necessários à implementação desse sistema, incorporando tanto o processo gerencial quanto a votação propriamente dita, com foco sempre voltado à segurança, à auditabilidade e à regulamentação interna, necessárias à aplicação do protocolo proposto.

Palavras-chaves: Votação eletrônica. Votação auditável. Segurança em votação eletrônica. Institutos Federais.

Abstract

One of the pillars of democracy is the exercise of the right to vote. The aim of this work is to determine the necessary features of an electoral system with low cost of deployment, auditable by voter using printed paper trail of ballots, seeking security of data and, above all, the auditability by the academic community of educational institutions. As background, uses the electoral process for the positions of dean and *campus*' principals of the Brazilian's Federal Institutes of Education, Science and Technology (IF). Through bibliographical and documentary review, the latter in the form of legislation, a election protocol was designed as artifact of Design Science Research. We also performed a systematic literature review with the aim of establishing the trend of electronic voting technologies. As primary contribution of this work, we present an electoral protocol covering all phases of the refered process that meets satisfactorily the requirements from legal and security perspective. We also presents the functional and nonfunctional requirements for implementation of this system, incorporating both the management process as well as the voting itself, focusing always on the security and the auditability. We finally presents internal rules for the application of proposed protocol.

Keywords: Eletronic Voting. Verifiable elections. Security in eletronic voting systems. Federal Institutes.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ABIN	Agência Brasileira de Inteligência
ADSL	*Asymmetric Digital Subscriber Line* (Linha Assimétrica Digital de Assinante)
AES	*Advanced Encryption Standard* (Padrão de Criptografia Avançado) — um algoritmo criptográfico
BAS	*Ballot Authentication Server* (Servidor de Autenticação de Cédulas)
CD	Cargo de Direção ou *Compact Disc*, conforme contexto
CEFET	Centro(s) Federal(is) de Educação Tecnológica
CGU	Controladoria-Geral da União
CPF	Cadastro de Pessoa Física
CS	Conselho Superior
CSV	*Comma-separated values* (valores separados por vírgulas)
DMZ	Zona Desmilitarizada
DRE	*Direct Recording Eletronic* (Registro Direto Eletrônico)
DSR	*Design Science Research*
DVVSBS	*Distributed Voter-Verifiable Secret Ballot System*
EAC	*U. S. Election Assistance Comission*
EAF	Escola(s) Agrotécnica(s) Federal(is)
EPT	[Rede Federal de] Educação Profissional e Tecnológica
ETF	Escola Técnica Federal
EUA	Estados Unidos da América
FCC	Função de Coordenação de Curso
FG	Função Gratificada
FIC	Formação Inicial e Continuada

FUMEC	Fundação Mineira de Educação e Cultura
GRE	*Generic Routing Encapsulation* (Encapsulamento de Roteamento Genérico)
HAVA	*Help America Vote Act*
HDSL	*High-Bit-Rate Digital Subscriber Line* (Linha Digital de Assinante de Alta Taxa de Bits)
HMAC	*Hash-based Message Authentication Code* (Código de Autenticação de Mensagens Baseado em Hash)
HOTP	*HMAC-based One-Time Password* (Senha de Utilização Única Baseada em HMAC)
IF	Instituto(s) Federal(is)
IP	*Internet Protocol* (Protocolo de *Internet*)
IPsec	*IP Security Protocol*
ISDN	*Integrated Services Digital Network* (Rede Digital de Serviços Integrados)
ISP	*Internet Service Providers* (Provedor de Serviços de *Internet*)
JSON	*JavaScript Object Notation* (Notação de Objeto JavaScript)
L2TP	*Layer 2 Tunnelling Protocol*
LAI	Lei de Acesso à Informação
LAN	*Local Area Network* (Rede Local)
LP	Linha Privativa
MEC	Ministério da Educação
MPLS	*Multiprotocol Label Switching* (Comutação de Rótulos Multiprotocolo)
NIST	*National Institute of Standards and Technology*
PC	*Personal Computer* (Computador Pessoal)
PCOS	*Precinct Count Optical Scan*
RAM	*Random Access Memory* (Memória de Acesso Aleatório)
RDV	Registro Digital de Voto
RFID	*Radio-Frequency Identification* (Identificação por Radiofrequência)

RNP	Rede Nacional de Ensino e Pesquisa
ROM	*Read Only Memory* (Memória Somente-Leitura)
RSA	Algoritmo de criptografia nomeado com as iniciais dos sobrenomes de seus criadores (Ronald Rivest, Adi Shamir e Leonard Adleman)
RSL	Revisão Sistemática de Literatura
SBSEG	Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais
SD	*Secure Digital* [Card] (Cartão Digital Seguro)
SEI	Sistema Eletrônico de Informações
SES	*Smart E-Voting System*
SETEC	Secretaria de Educação Profissional e Tecnológica
SGBD	Sistema Gerenciador de Banco de Dados
SGE	Sistema de Gerenciamento Eleitoral
SI	Sistemas de Informação
SIAPE	Sistema Integrado de Administração de Recursos Humanos
SIC	Serviço de Informação ao Cidadão
s. p.	*sine pagina* (sem página)
SRI	Sistemas de Recuperação da Informação
TAE	Técnico(s) Administrativo(s) em Educação
TCB	*Trusted Code Base*
TGDC	*Technical Guidelines Development Committee*
TI	Tecnologia da Informação
TPM	*Trusted Platform Module*
TRE	Tribunal Regional Eleitoral
TRF	Tribunal Regional Federal
TSE	Tribunal Superior Eleitoral
UE	Urna(s) Eletrônica(s)

UML	*Unified Modeling Language*
UNED	Unidade de Ensino Descentralizada
UTFPR	Universidade Tecnológica Federal do Paraná
VC	*Voter Client*
VLAN	*Virtual Local Area Network* (Rede Local Virtual)
VPN	*Virtual Private Network* (Rede Privada Virtual)
VTS	Vote Tally Server (Servidor de Apuração de Votos)
VVPAT	*Voter-Verified Paper Audit Trail* (Trilha de Auditoria em Papel Verificada pelo Eleitor)
ZKP	*Zero-Knowledge Proof* (Prova de Conhecimento Nulo)

Lista de símbolos

$\mathcal{A}_E$	Comissão Pré-Eleitoral
$\mathcal{A}_C$	Comissão Eleitoral Central
$\mathcal{A}_L$	Comissão Eleitoral Local
$\mathcal{BU}$	boletim de urna
$\mathcal{BB}$	*bulletin board* (quadro de avisos)
$\mathcal{C}$	lista de candidatos
c_i	i-ésimo candidato de $\mathcal{C}$
$\mathcal{E}$	rol de eleitores
e_i	i-ésimo eleitor de $\mathcal{E}$
$\mathcal{F}$	rol de fiscais
f_i	i-ésimo fiscal de $\mathcal{F}$
GB	Gigabyte
$\mathcal{M}$	conjunto de mesários da seção eleitoral (mesa receptora de votos)
m_p	presidente da mesa receptora de votos ($\mathcal{M}$)
m_{vp}	vice-presidente da mesa receptora de votos ($\mathcal{M}$)
m_s	secretário da mesa receptora de votos ($\mathcal{M}$)
MHz	Megahertz

Sumário

1 Introdução

No mundo ocidental, dentre os regimes políticos, a democracia encontra-se entre os mais utilizados. Desde suas raízes nas antigas cidades-estado gregas, notadamente Atenas, o exercício do poder através da vontade do povo é um dos pilares desta cultura. No Brasil, desde o fim da ditadura militar e a restauração do voto direto para governantes, este regime ocupa lugar de destaque na cultura, nas estruturas de governo e em diversas instituições.

Embora imperfeito, como qualquer regime político, a democracia fundamenta-se no princípio do poder emanado do povo, por ele exercido e em seu benefício. A forma mais direta de exercício do poder por parte do povo é através do sufrágio universal. Por meio do voto, garantido a todos os cidadãos aptos, governantes são elevados ao poder, decisões são tomadas de acordo com manifestação em referendo popular, instituições públicas e privadas definem diretrizes, etc. O exercício do voto está presente em vários segmentos da sociedade como manifestação legítima do poder popular. O voto é condição *sine qua non* para o pleno exercício da democracia.

Entretanto, a democracia não está livre de ameaças. Ela ainda é muito jovem no Brasil, semeada com o término da monarquia e ceifada durante os longos anos de ditadura militar. Mesmo entre estes dois eventos, não se configura em sua forma pura, sendo alvo de fraudes e ações deletérias de grupos interessados na manutenção do poder. Observando-se a história do Brasil, encontram-se narrativas dos conflitos de interesse no período denominado República do Café com Leite, onde pequenos grupos lançavam mão dos mais diversos ardis para se consolidarem no poder.

Com o propósito de reduzir as fraudes eleitorais, ao longo do tempo, observa-se o uso de sistemas de informação, implementados tanto em *hardware* quanto em *software*, nos processos eleitorais, mitigando os riscos provenientes de fatores humanos. Além do processamento mais rápido que os métodos manuais, podem produzir um vasto registro de eventos importantes, permitindo uma análise mais acurada dos fatos. No desenvolvimento, devem ser utilizadas técnicas que minimizem a possibilidade de introdução de novos tipos de fraudes ou vulnerabilidades, sendo necessário um constante processo de pesquisa e desenvolvimento.

1.1 Motivação e Justificativa

Fraudes sempre estiveram lado a lado com o direito de votar e ser votado. Mesmo com o término do período ditatorial, a democracia continua infante, sendo construída aos poucos, defendendo-se a duras penas de toda forma de ameaça.

Um dos baluartes da defesa da democracia encontra-se nas instituições de ensino superior do Brasil. Embora existam movimentos iniciados no âmbito universitário em resposta às ameaças

ao estado democrático registrados na história brasileira, o presente texto não se aterá a eles. Nelas encontram-se a escolha de dirigentes e de representantes de classe em órgãos colegiados, a prática da audiência pública para tomadas de decisões críticas, dentre outras circunstâncias que envolvem a participação da comunidade acadêmica nos processos de gestão e, portanto, do exercício do governo. Constituem um ambiente em que a democracia, permeada no processo educacional, consolida-se nos educandos, permitindo seu fortalecimento no contexto macro, extrapolando os limites físicos das instituições de ensino.

Mesmo em tais redutos, crer na completa isenção e ausência de interesses contrários ao regime democrático é mera utopia. Como fração da sociedade, pode apresentar as mesmas mazelas observadas na totalidade do conjunto. Na Seção 4.2, são apresentados alguns dos problemas que podem ser encontrados nos processos eleitorais, informatizados ou não, aos quais nenhuma organização está imune.

Por esta razão, são necessários mecanismos, técnicas ou protocolos que visem assegurar tanto o direito ao voto quanto o seu correto registro enquanto vontade do eleitor. São características que asseguram que esta última seja respeitada: auditabilidade, integridade, sigilo e ausência de coerção, conforme pode-se observar nos trabalhos apresentados no Capítulo 4.

Votação eletrônica não é uma prática estranha ao contexto da educação superior. Diversos trabalhos abordam o uso de sistemas eleitorais eletrônicos para eleições em universidades, como Budurushi; Jöris e Volkamer (33), Onshus (80) e Saad; Roseli e Zullkeply (95). No Brasil, há o relato do uso do sistema *Helios* para eleições do Conselho Universitário do Instituto Federal de Santa Catarina (39), totalmente baseado em *internet*. Entretanto, a literatura aponta que o emprego do *Helios* é mais adequado para ambientes de baixa coerção (18, 85). Em Jefferson *et al.* (61), são apresentadas vulnerabilidades inerentes à própria *internet* e aos sistemas baseados na arquitetura PC (*personal computer* — computador pessoal), levando estes autores à conclusão de que a votação via *internet*, em geral, não tem condições de segurança em futuro próximo.

Observa-se que algumas soluções domésticas, i. e., desenvolvidas no âmbito das instituições de ensino, embora sejam capazes de prover um ambiente de votação, não endereçam a segurança e o sigilo do voto de forma satisfatória (95). Mesmo o uso da urna eletrônica brasileira encontra obstáculos, explorados na Seção 4.3, e possui várias críticas na literatura, também exploradas na mesma seção. Soluções domésticas tendem, ainda, a ser simples, no aspecto de não incluir técnicas avançadas de criptografia. Embora a simplicidade seja um fator desejável em qualquer sistema, permitindo até mesmo a sua compreensão, a ausência de mecanismos de segurança mais elaborados pode tornar o comprometimento dos resultados ainda mais fácil, conforme apontado em relação à urna eletrônica usada na Índia (113).

Dentro deste contexto, tendo como pano de fundo os processos de consulta à comunidade na escolha de dirigentes dos Institutos Federais de Educação, Ciência e Tecnologia (apresentados na Seção 3.2), o presente trabalho encontra-se inserido. Em diversos casos, são instituições novas, construídas pela agregação de antigas autarquias, que trouxeram no bojo tanto episódios

de luta pelos ideais democráticos quanto casos sinistros do poder oligárquico. Exatamente por possuírem histórico tão recente quanto sua criação, torna-se necessária a proteção dos processos eleitorais para que não venham macular-se com práticas obscuras e antidemocráticas.

Além disso, a formação de cidadãos com consciência e responsabilidade social é uma premissa destas instituições. Proteger os processos democráticos nestes redutos é uma forma de estabelecer parâmetros válidos para a avaliação de processos externos, visando que esta democracia, ainda jovem, possa amadurecer de forma saudável para futuras gerações.

Uma medida utilizada em escala nacional, para reduzir as fraudes eleitorais, é a adoção de recursos de informática na coleta, apuração e totalização dos votos. Um exemplo típico é a urna eletrônica brasileira, empregada gradativamente pelo Tribunal Superior Eleitoral (TSE) desde a metade da década de 1990 em eleições majoritárias e proporcionais para os governos municipais, estaduais e federal, que se encontra desde 2010 com 100% de implantação (27). No entanto, recebe várias críticas, apresentadas de forma não exaustiva na Seção 4.3. Além das questões de natureza técnica, existem dificuldades para sua adoção, analisadas na seção supracitada.

Desta forma, o problema de pesquisa constitui-se do planejamento de um sistema eleitoral, informatizado e de código aberto, que possa ser adotado em processos eleitorais de instituições de ensino, minimizando os riscos encontrados na literatura, por meio da independência de *software*, ou seja, que os resultados possam ser auditados e validados mesmo que o *software* subjacente apresente qualquer nível de comprometimento, com base em práticas recomendadas pela literatura. Este problema pode ser sumarizado na forma da seguinte questão de pesquisa: "**Quais os requisitos e os componentes de um sistema eleitoral informatizado que seja capaz de manter a independência de *software* e um baixo custo de implantação?**"

A literatura mostra que a impressão do voto, conferido pelo eleitor antes de ser depositado em uma urna lacrada, é uma forma eficaz para a realização de eleições seguras. Cunha *et al.* (43) defendem que sistemas DRE (*Direct Recording Eletronic* — Registro Direto Eletrônico) devem ser substituídos por sistemas VVPAT (*Voter-Verified Paper Audit Trail* — Trilha de Auditoria em Papel Verificada pelo Eleitor), que são simplesmente sistemas em que o voto é materializado de forma impressa, podendo ser verificado independentemente do *software*. Em consonância com este argumento, Dill e Castro (45) vão além e afirmam que sistemas de votação sem papel deveriam ser banidos dos Estados Unidos. Em outros sistemas encontrados na literatura, em vez de registrar eletronicamente o voto em um sistema DRE, o eleitor assinala uma cédula e a submete a um *scanner* para digitalização e apuração eletrônica (PCOS — *Precinct Count Optical Scan*). Por meio da Revisão Sistemática de Literatura (Seção 2.1), pretendeu-se verificar o estado da arte em sistemas eleitorais não remotos, ou seja, aqueles que são empregados em seções eleitorais, submetidos a um controle e a uma logística diferentes da votação via *internet*. A Seção 4.5.2 apresenta algumas considerações sobre o equilíbrio entre o registro de eventos para auditoria e a manutenção do sigilo do voto.

No entanto, esta abordagem também possui seus pontos controversos. Por exemplo, havendo divergência entre o registro eletrônico e a contagem dos votos impressos, estes, verificados e confirmados pelo eleitor, assumiriam a prioridade na definição do resultado. Por outro lado, a tentativa de fraudar o conteúdo dos votos impressos poderia surgir. Os votos poderiam ser trocados, mantendo o mesmo número de cédulas que o de eleitores presentes. Pode-se reduzir a dúvida aplicando-se técnicas de assinatura digital, com chaves geradas de forma segura dentro das urnas, permitindo a detecção de votos forjados externamente. Métodos construtivos podem ser utilizados para garantir que, uma vez lacrados dentro da urna eletrônica, estes receptáculos não possam ter seu conteúdo alterado sem detecção (e. g., através de lacres de segurança), aliados a métodos de fiscalização antes da fixação e após a retirada dos lacres.

Embora a temática não seja recente, sendo discutida há algumas décadas, no Brasil só tem recebido destaque acadêmico mais recentemente, com poucos eventos e raras publicações acadêmicas em português. A partir da XIV edição, ocorrida em novembro de 2014, o Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais (SBSEG) passou a incluir como evento-satélite o *Workshop* de Tecnologia Eleitoral, que no presente ano completa três edições realizadas.

1.2 Objetivos

O objetivo geral deste trabalho é determinar as características necessárias a um sistema eleitoral de baixo custo de implantação, auditável, com registro impresso do voto, visando à segurança e, acima de tudo, à auditabilidade pela comunidade acadêmica das instituições de ensino.

Para alcançar este objetivo, delinearam-se os seguintes objetivos específicos:

- Estudar os processos eleitorais existentes em uma instituição de ensino (Instituto Federal de Educação, Ciência e Tecnologia) e suas características e regulamentações;
- Identificar o protocolo, seus diversos estágios, atores, técnicas criptográficas e estruturas de dados para representação e intercâmbio de dados, ao longo do processo eleitoral;
- Propor um sistema de informação que ofereça suporte ao protocolo eleitoral proposto, redução de custos e que permita a impressão e confirmação do voto pelo usuário antes de lançá-lo em urna lacrada.

1.3 Linha de Pesquisa

O Programa de Mestrado em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC, de natureza multidisciplinar, encontra-se estruturado em uma única

área de concentração: Gestão de Sistemas de Informação e do Conhecimento. Nesta área de concentração, encontram-se duas linhas de pesquisa: a primeira, Gestão da Informação e do Conhecimento, e a segunda, Tecnologia e Sistemas de Informação.

Em Araújo (10, s. p.), a autora conceitua sistemas de informação como "sistemas sociais, ou seja, sistemas artificiais construídos pelo homem com o objetivo de organizar e disseminar a massa crescente de informações". Nota-se que este conceito independe do suporte informacional. Pode ser manual, como realizado por séculos desde a invenção da escrita, ou ter suporte da tecnologia da informação, automatizando esse processo de organização e disseminação com o uso destas tecnologias a partir do séc. XX.

Em 1981, Pawlak definiu que o componente básico de um sistema de informação é um conjunto finito de objetos (X), classificados por um conjunto finito de atributos (A), que assumem valores de um conjunto não vazio (V). Define também ρ como uma função de $X \times A$ em V, de tal forma que um sistema de informação seja dado pela quádrupla apresentada na Equação 1.1. Se ρ for total, o sistema é denominado completo, e o autor considerou, àquela época, apenas sistemas completos (84).

$$S = \langle X, A, V, \rho \rangle \tag{1.1}$$

Portanto, segundo Pawlak (84), S é simplesmente um conjunto de descritores correspondendo a todos os atributos no sistema. Assim, a função ρ define uma tabela de atributos de objetos, em que cada linha estabelece um objeto do conjunto X, e as colunas, seus respectivos atributos. Este modelo matemático de Pawlak conduz a um método novo, simples e eficiente de recuperação de informações. O modelo apresentado, sem dúvida, permanece vigente até os dias atuais, com tabelas de dados sendo ainda um dos meios mais comuns para representação de informações nos sistemas informatizados, compondo o modelo relacional de banco de dados. O suporte da tecnologia da informação consolidou aquilo que Araújo (10, s. p.) conceituou como "sistemas de informação são aqueles que objetivam a realização de processos de comunicação".

Araújo (10), ao fazer uma análise da abordagem sistêmica, também destacou que sistemas de (recuperação da) informação (SI ou SRI) não são, dentro daquela abordagem, nem abertos nem fechados. São estruturas complexas, muitas vezes compostas por subsistemas ao mesmo tempo em que compõem sistemas maiores.

Esta visão permite uma concepção de sistema de informação que não se limita apenas à implementação (manual ou automatizada), mas que se expande ao englobar seus atores, a informação comunicada e os sistemas com que interagem em suas fronteiras. Sistemas analógicos são implementados digitalmente, simulando os processos que serviram de modelo. Na literatura consultada, discutida no Capítulo 4, observa-se, com considerável frequência, a ênfase na acurácia e segurança do sistema eleitoral proposto. Este, muitas vezes, analisado sob a perspectiva de diretivas criptográficas para registro e computação dos votos, ao mesmo tempo em que busca

garantir o sigilo do voto e a privacidade do eleitor. Neste texto, foi empregada uma abordagem mais sistêmica, analisando os atores, as ameaças e os mecanismos que permitam a implementação de um sistema de informação (eleitoral) seguro, pela adaptação digital dos procedimentos analógicos existentes.

Posiciona-se o presente trabalho na linha de pesquisa **Tecnologia e Sistemas de Informação**, por visar ao desenvolvimento de tecnologias e sistemas de informação que, aliados às práticas de segurança, solucionem um problema presente em instituições de ensino superior. Nesta linha de pesquisa, é possível enxergar o processo eleitoral não apenas como um *hardware* de votação e/ou um *software*, embarcado ou não, que o gerencie, expandindo os limites destes dois componentes para a visualização do cenário em sua completude. Nesta concepção, a ênfase recai sobre a comunicação da comunidade acadêmica acerca de sua escolha de dirigentes, representada na forma do voto eletrônico.

Segundo Moreira e Maia (75, s. p.), "a informação é recurso estratégico e não apenas operacional e cabe aos cidadãos ou aos seus representantes gerenciá-la no benefício do bem comum". Deve ser dada a máxima transparência em um processo eleitoral, especialmente no setor público, para que a comunidade certifique-se de que sua escolha foi respeitada. Um sistema de informação eleitoral deve garantir que o eleitor possa verificar todos os procedimentos realizados pela autoridade eleitoral. Esta, em última análise, é responsável pela condução do processo de escolha, não por determiná-la. Quanto maior for a transparência do sistema, maior controle a comunidade pode exercer para o bem comum.

As principais temáticas referenciadas no trabalho relacionam-se aos sistemas de votação eletrônica, à segurança da informação e aos sistemas embarcados. Este arcabouço tecnológico permite avaliar e propor um protocolo eleitoral capaz de incorporar as melhores práticas em termos de tecnologia e de sistemas de informação.

1.4 Estrutura do Texto

Para melhor organização deste trabalho, seu conteúdo foi dividido em seis capítulos. No Capítulo 1 são apresentados a motivação e os objetivos geral e específicos do trabalho. A metodologia e o protocolo de revisão sistemática de literatura encontram-se no Capítulo 2.

O Capítulo 3 apresenta as instituições de ensino superior cujos processos eleitorais são objetos de estudo. Além de uma visão geral da estrutura organizacional dos Institutos Federais de Educação, Ciência e Tecnologia (IF) e da fundamentação legal dos processos eleitorais, são abordados os pontos que podem fragilizar os processos democráticos destas instituições, e, por fim, sua infraestrutura de TI, que impacta diretamente a proposta apresentada.

O Capítulo 4 mostra uma análise geral dos sistemas de votação eletrônica na literatura e as características de segurança desejáveis. Explora, brevemente, a urna eletrônica brasileira e sua inadequação para o uso proposto em instituições de ensino.

Os resultados alcançados são apresentados e discutidos no Capítulo 5, e o Capítulo 6 conclui o trabalho. As referências bibliográficas utilizadas na composição do presente texto são apresentadas ao término do documento.

2 Metodologia

No presente trabalho, tornou-se necessária uma revisão da literatura capaz de elencar os elementos de um sistema eleitoral eletrônico que sejam capazes de controlar a incerteza da validade do resultado às partes interessadas, bem como permitir sua auditabilidade para garanti-lo. Para a condução de uma revisão sem viés, que seja reproduzível e que sumarize o estado da arte, foi realizada uma revisão sistemática de literatura (79), cujo protocolo encontra-se na Seção 2.1.

Além da revisão bibliográfica e documental, a metodologia do trabalho também pode ser classificada como pesquisa aplicada e qualitativa. Quanto aos seus objetivos, trata-se de uma pesquisa exploratória, que visa tornar explícitas as características do problema. Quanto aos procedimentos técnicos, foi adotada a metodologia *Design Science Research* (DSR), proposta inicialmente por Simon (100). Como processo deste método, foi utilizada a abordagem de Peffers *et al.* (86), composta por seis atividades em sequência nominal:

1. **Identificação do Problema e Motivação:** definição do problema específico de pesquisa e justificativa do valor da solução;
2. **Objetivos da Solução:** inferir os objetivos da solução a partir da definição do problema;
3. **Projeto e Desenvolvimento:** criar os artefatos da solução;
4. **Demonstração:** demonstrar a eficácia do artefato na solução do problema;
5. **Avaliação:** observar e mensurar quão bem o artefato suporta a solução do problema;
6. **Comunicação:** comunicar o problema e sua importância, o artefato e sua utilidade, o rigor do projeto e sua efetividade a pesquisadores e outras audiências que sejam relevantes.

A primeira atividade constituiu-se da observação dos processos quadrienais de consulta à comunidade em um IF, assim como os demais processos eleitorais para conselhos, comissões e outras representatividades, em decorrência da experiência do autor presidindo duas comissões eleitorais, aliada a dois processos em que este atuou junto a candidatos, observando externamente a sua condução. A ausência de automação dos métodos, levando a apurações que se estendem noite adentro, quando todos os escrutinadores estão cansados e mais suscetíveis a erros, levantou o questionamento da possibilidade de automatizá-los.

Embora processos eleitorais de maior impacto sempre utilizem urnas de lona cedidas pelo cartório eleitoral, muitos daqueles tidos como menos relevantes utilizaram caixas de papelão revestidas com papel *kraft* (papel pardo utilizado para confecção de diversos produtos cartonados

e envelopes, geralmente obtido na forma de bobinas ou folhas grandes e com maior gramatura), com uma abertura para inserção das cédulas, sem qualquer segurança contra adulterações antes ou após a votação. As cédulas, por sua vez, eram confeccionadas em papel A4, fracionado visando aproveitar o máximo de espaço possível, sem atenção a mecanismos de autenticação delas ou preservação do sigilo do voto.

As dificuldades em obter acesso às urnas eletrônicas do TSE, coadunadas com as críticas que esses equipamentos recebem, concomitantemente aos processos conduzidos da forma descrita no parágrafo anterior, levaram à cogitação de um sistema doméstico para condução das eleições. Entretanto, tal solução deve ser ao mesmo tempo segura, de rápida apuração, capaz de garantir um resultado confiável e, acima de tudo, que preserve o sigilo do eleitor como prioridade absoluta. Com este propósito, foram estabelecidos os objetivos do trabalho, na segunda etapa, conforme apresentados na Seção 1.2.

A terceira etapa constituiu-se basicamente da pesquisa bibliográfica e documental em conjunto com a elaboração dos requisitos funcionais e não funcionais necessários ao sistema, partindo de uma proposta de protocolo eleitoral que se adequasse, principalmente, às restrições de tempo impostas pela legislação vigente. Nesta etapa, alcançou-se a produção dos artefatos planejados na DSR. Segundo Bax (12, p. 3892), na metodologia DSR "os artefatos podem ser dos tipos: construtos (entidades e relações), modelos (abstrações e representações), métodos (algoritmos e práticas) e instanciações (implementação de sistemas e protótipos)". O presente trabalho, segundo esta classificação, tem como principal artefato a elaboração **métodos**, na forma de um protocolo eleitoral e requisitos do sistema de votação eletrônico proposto.

Para a construção do método (protocolo eleitoral), foi realizada uma Revisão Sistemática de Literatura, conforme protocolo registrado em 2.1, e revisão documental, na forma da legislação vigente para os processos de consulta à comunidade dos IF, conforme apresentado na Seção 3.2. Estas revisões subsidiaram as informações necessárias à consecução do objetivo deste trabalho.

Inicialmente, houve a intenção de analisar os processos de consulta à comunidade para eleição de diretores-gerais e reitor de um IF, realizados em duas ocasiões distintas, após a implantação dos IF, em 2011 e 2015, segundo cronograma estabelecido pelo Ministério da Educação nos respectivos anos. Além do cronograma utilizado em cada processo, poderiam ser detectados os riscos potenciais, a forma de atuação das comissões eleitorais na solução dos problemas, o comportamento dos agentes, recursos impetrados, enfim, toda documentação que permitisse estabelecer a situação real em uma instituição.

Os processos foram solicitados através do Serviço de Informação ao Cidadão (SIC), utilizando o formulário eletrônico (e-SIC) disponibilizado pela Controladoria-Geral da União (CGU), sob o número de protocolo 23480004683201690. Até o momento de finalização do presente texto, a instituição não forneceu os processos para análise, sendo registrados recursos até a segunda instância (dirigente máximo da instituição), conforme a Lei de Acesso à Informação (LAI) e sua regulamentação (22, 24). Em segunda instância, foi determinado o acesso

ao material, mas este não foi transportado. Não foi impetrado recurso em terceira instância (CGU), pois acreditou-se que o material seria entregue em tempo hábil, antes do fechamento do sistema para apelação àquele órgão e conclusão do presente trabalho. Todavia, todos os esforços foram frustrados e nenhum material foi disponibilizado. Inicialmente, a justificativa para não disponibilizar cópia restringia-se ao volume elevado de um dos processos, que teria mais de vinte mil páginas, segundo contato telefônico com o responsável pelo SIC na instituição. Tal volume foi gerado por decisão da comissão eleitoral de arquivar, junto ao processo, todas as cédulas em papel utilizadas. Por fim, os processos seriam transportados para um dos *campi* da instituição, onde o autor poderia consultá-los sob supervisão local, fato não concretizado.

Finalizando as atividades do método DSR, têm-se as atividades de demonstração e avaliação, delineadas durante a etapa anterior (projeto e desenvolvimento). Estas atividades constituem-se da verificação de aderência do modelo proposto aos requisitos de segurança apresentados. A última atividade, comunicação, concretiza-se na forma estabelecida no regulamento do Programa de Pós-Graduação *Stricto Sensu* em Sistemas de Informação e Gestão do Conhecimento, através da presente dissertação e publicação de artigo.

2.1 Protocolo de Revisão Sistemática de Literatura

Para uma melhor compreensão das práticas recomendadas na literatura, visando a sistemas eleitorais auditáveis e mais resilientes a tentativas de fraude, foi proposta uma revisão sistemática de literatura, de acordo com o presente protocolo.

2.1.1 Questão de Pesquisa

Para o presente protocolo de revisão sistemática de literatura, foi estabelecida a seguinte questão principal de pesquisa: **Quais são as tecnologias de votação eletrônica mais encontradas na literatura?** Com o objetivo de auxiliar a avaliação dos trabalhos, durante a revisão, para responder à pergunta principal, delineiam-se as seguintes questões secundárias: (a) Quais mecanismos de segurança e de sigilo são recomendados? (b) Como as propostas mitigam os riscos de coerção do eleitor? (c) Quais são os métodos de auditoria dos votos para garantir a validade dos resultados?

2.1.2 Estratégias de Busca

A pesquisa foi realizada utilizando as seguintes fontes, informadas sem qualquer ordem de prioridade: *ACM Digital Library*[1], EBSCO *Host*[2], *Emerald Insight*[3], Portal de Periódicos da

[1] http://dl.acm.org/
[2] http://search.ebscohost.com/
[3] http://www.emeraldinsight.com/

CAPES[4], *Scopus*[5] e *Science Direct*[6]. Nas bases de dados, a pesquisa foi realizada utilizando os seguintes termos de busca (divididos em dois itens para fins de discussão):

1. `("eletronic voting" OR "voting systems" OR "voting machines")`
2. `AND ("voter verification" OR "verifiable elections" OR "trustworthy elections" OR "voter coercion" OR "software independence" OR "independent voter-verifiable" OR "voter auditing" OR "independent auditing")`

A primeira sequência selecionou os sistemas de votação eletrônica suportados por algum tipo de *hardware* e *software*, enquanto a segunda restringiu a busca aos critérios de auditabilidade por parte do eleitor ou por terceiros, de forma independente do *software*. Nas bases de dados em português, foram utilizados os termos em inglês e sua respectiva tradução, incluindo o sintagma "urna eletrônica" em conjunto com a primeira sequência, dado o uso mais comum do termo no País:

1. `("votação eletrônica" OR "sistemas de votação" OR "máquinas de votar" OR "urna eletrônica")`
2. `AND ("verificação do eleitor" OR "eleições verificáveis" OR "eleições confiáveis" OR "coerção do eleitor" OR "independência de software" OR "independentemente verificável pelo eleitor" OR "auditoria por eleitor" OR "auditoria independente")`

2.1.3 Critérios de Seleção

Após a seleção inicial, foi feita uma triagem por pesquisa no título, resumo (*abstract*) e palavras-chave (*keywords*). Para inclusão, foram considerados os textos publicados no período de 11 anos completos (2005–2015), em inglês ou português, em periódicos e conferências. Incluíram-se apenas os que a base forneceu acesso ao texto completo gratuitamente ou para a rede da instituição de ensino em que a pesquisa foi realizada. Artigos em anais de conferências foram considerados apenas quando explicitamente retornados na busca, sem expansão ao restante dos anais. Foram incluídos textos que propõem o uso de sistemas de votação eletrônica para ambientes supervisionados (como a cabine em uma seção eleitoral). Para que o texto fosse incluído, deveria ser o trabalho seminal do sistema proposto ou, no mínimo, um dos autores

[4] http://periodicos.capes.br/
[5] http://www.scopus.com/
[6] http://www.sciencedirect.com/

deveria ser autor do trabalho original. Se não fosse atendido esse requisito, o texto seria incluído somente se estendesse o sistema original e não se limitasse a descrevê-lo.

Excluíram-se os resumos (quando não estendidos), resenhas, patentes e textos não publicados. Também foram excluídos os textos que abordam votação exclusivamente via *internet* ou sistemas puramente remotos. Foram também removidos os trabalhos publicados em conferência que tivessem uma versão completa publicada em periódico, dos mesmos autores e conteúdo essencialmente idêntico. Por fim, após a primeira triagem, conforme indicado, foram analisados os textos completos. Nesta etapa, foram classificados em **relevante** (quando apresentada uma solução relevante à pesquisa) ou **irrelevante** (caso apresente os termos de busca, mas não estejam relacionados à pesquisa).

2.1.4 Estratégias para Extração de Dados

Selecionados os artigos para a revisão sistemática, os dados foram coletados e tabulados em planilha, buscando identificar os conceitos e os elementos de segurança, auditabilidade, mitigação de coerção, privacidade do eleitor e sigilo do voto apresentados. Desta forma, ao término do processo, foi possível identificar as propostas mais comuns na literatura e suas aplicações mediante análise dos documentos incluídos na pesquisa, observados os critérios de inclusão/exclusão.

2.2 Síntese dos Objetivos e Métodos

O presente trabalho pode ser sumarizado, em termos de objetivos e métodos, como apresentado na Tabela 1.

Tabela 1 – Síntese dos objetivos e métodos propostos para o trabalho

Objetivos	**Métodos**
Estudar os processos eleitorais existentes em uma instituição de ensino e suas características e regulamentações;	Revisão Bibliográfica e Documental, RSL
Identificar o protocolo, seus diversos estágios, atores, técnicas criptográficas e estruturas de dados para representação e intercâmbio de dados, ao longo do processo eleitoral;	RSL e DSR
Propor um sistema de informação que ofereça suporte ao protocolo eleitoral proposto, redução de custos e que permita a impressão e confirmação do voto pelo usuário antes de lançá-lo em urna lacrada.	DSR

Fonte: elaborado pelo autor.

3 Os Institutos Federais

Conforme o ato legal que os institui, os Institutos Federais de Educação, Ciência e Tecnologia, ou Institutos Federais (IF):

> "[...] são instituições de educação superior, básica e profissional, pluricurriculares e *multicampi*, especializados na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas" (23, Art. 2º).

São originados da fusão de Centros Federais de Educação Tecnológica (CEFET), Escolas Técnicas Federais (ETF) e Escolas Agrotécnicas Federais (EAF). Cada unidade federativa pode conter uma ou mais unidades autárquicas, compostas pela reitoria e seus respectivos *campi*. Fazem parte da Rede Federal de Educação Profissional e Tecnológica (Rede EPT), vinculados ao Ministério da Educação (MEC) por meio de sua Secretaria de Educação Profissional e Tecnológica (SETEC). Também compõem a Rede EPT o Colégio Pedro II (RJ), o CEFET-MG e o CEFET-RJ, a Universidade Tecnológica Federal do Paraná (UTFPR) e escolas técnicas vinculadas às Universidades Federais.

No âmbito administrativo, possuem autonomia para criação e extinção de cursos, registrar seus diplomas, administração patrimonial e financeira, equiparando-se às Universidades Federais. Atuam ainda como instituições acreditadoras e certificadoras de competências profissionais, atuando desde cursos de Formação Inicial e Continuada (FIC) ao *Stricto Sensu*. Por lei (23), são obrigados a destinar no mínimo 50% de suas vagas a cursos técnicos de nível médio e 20% em licenciaturas, em cada processo seletivo. As vagas restantes distribuem-se entre cursos de graduação nas modalidades de bacharelado e graduação tecnológica.

No presente capítulo, a estrutura administrativa e a regulamentação dos processos eleitorais são analisadas, respectivamente, nas Seções 3.1 e 3.2. Algumas vulnerabilidades inerentes aos processos de consulta à comunidade são apresentadas na Seção 3.3. A Seção 3.4 analisa brevemente os modelos gerais de conexão à *internet* destas instituições. A Seção 3.5 faz breves considerações acerca do conteúdo deste capítulo.

3.1 Organização Administrativa

Conforme apresentado nas considerações iniciais deste capítulo, os IF são instituições *multicampi*, integrantes da Rede Federal de Educação Profissional e Tecnológica. Atualmente, existem 38 IF espalhados pelo território nacional, em todas as unidades federativas e no Distrito Federal.

Sua estrutura administrativa, fixada no ato legal que os institui (23), pode ser resumida da seguinte forma:

Órgãos Superiores: Conselho Superior (deliberativo e consultivo) e Colégio de Dirigentes (consultivo);

Órgão Executivo: reitoria, composta por:

- reitor, eleito pela comunidade;
- pró-reitores, nomeados pelo reitor, totalizando cinco pró-reitorias;

***Campi*:** administrados por seu respectivo diretor-geral, eleito pela comunidade.

O Colégio de Dirigentes é constituído pelo reitor, pelos pró-reitores e pelos diretores-gerais dos *campi* que compõem o Instituto Federal. O Conselho Superior é composto por representantes dos docentes, dos estudantes, dos servidores técnico-administrativos, dos egressos da instituição, da sociedade civil, do Ministério da Educação e do Colégio de Dirigentes do Instituto Federal, assegurando-se a representação paritária dos segmentos que compõem a comunidade acadêmica (23, Art. 10). Além da estrutura fixada em lei, os IF apresentam outros conselhos, comissões e comitês, estabelecidos em seus estatutos, regimentos gerais ou, ainda, determinados pela legislação ou por atos administrativos do Ministério da Educação, ao qual estão vinculados.

Cada *campus* possui um conselho, cujo nome varia de acordo com o Regimento Geral da instituição (Conselho Escolar, Conselho Acadêmico, etc.), que reúne representações dos três segmentos da comunidade acadêmica (docentes, técnicos administrativos em educação e discentes), no âmbito do *campus*, espelhando algumas funções do Conselho Superior. Este conselho geralmente tem papel consultivo e deliberativo no *campus*, instituindo normatizações locais e apreciando matérias submetidas às suas reuniões.

A escolha do reitor e dos diretores-gerais dá-se por consulta à comunidade acadêmica, na qual cada segmento (docente, discente e técnico-administrativo) contribui com $\frac{1}{3}$ do peso dos votos, conforme Equação 3.1, sendo V_{c_i} o percentual total de votos nos três segmentos para o candidato c_i, e V_{Doc}, V_{TAE} e V_{Dis}, o número de votos obtidos pelo candidato nos segmentos docente, técnico-administrativo e discente, respectivamente. N_{Doc}, N_{TAE} e N_{Disc} correspondem ao quantitativo total de eleitores aptos a votar, respectivamente, nos três segmentos supracitados. A consulta ocorre simultaneamente para os dois cargos, em todos os *campi*, incluindo polos de educação à distância, cujo processo deve ser deflagrado pelo Conselho Superior com, no mínimo, 90 dias de antecedência do término dos mandatos em curso do reitor e dos diretores-gerais. Após a deflagração, o processo deve ser concluído no período de 90 dias e será conduzido por uma Comissão Eleitoral Central e por Comissões Eleitorais de cada *campus*, compostas por três

membros de cada segmento, eleitos por seus pares em um processo coordenado pelo Conselho Superior (21).

$$V_{c_i} = \left[\left(\frac{1}{3} \times \frac{V_{Doc}}{N_{Doc}}\right) + \left(\frac{1}{3} \times \frac{V_{TAE}}{N_{TAE}}\right) + \left(\frac{1}{3} \times \frac{V_{Dis}}{N_{Dis}}\right)\right] \times 100 \tag{3.1}$$

3.2 Processos de Consulta à Comunidade

O processo de consulta à comunidade, sem dúvida, é um dos mais amplos e complexos dentre os existentes nos IF. Nos demais casos, em geral, a votação é realizada em separado por segmento, utilizando totalização simples dos votos válidos. Independentemente do processo em execução, é necessário o máximo de transparência em sua condução.

Normalmente, são adotados a votação em cédula de papel e o escrutínio manual para a condução das consultas. Dada a dispersão geográfica típica dos IF, também é comum que a mesa receptora dos votos, ao término do horário de votação, exerça a função de mesa escrutinadora, totalizando os votos de cada seção eleitoral. Deve-se esta miscigenação de papéis ao intuito de agilizar o processo, sem depender dos deslocamentos para um local central de totalização.

Entretanto, estes são exatamente os pontos de fragilidade do processo. Com o número de locais de votação, as atividades de supervisão das respectivas comissões eleitorais tornam-se pulverizadas, tanto quanto o exercício do direito de fiscalização do processo por parte dos candidatos, que podem não ter recursos para envio de fiscais a todos os locais em que a votação esteja sendo realizada. A transparência do processo reside unicamente na idoneidade dos membros das mesas receptoras, que, por sua vez, possuem sua própria afinidade política. Casos de fraudes eleitorais, executados pelos mesários, não são impossíveis em eleições conduzidas pela Justiça Eleitoral, e seria excesso de confiança crer que não pudessem acontecer no ambiente acadêmico. A presunção de idoneidade não elimina o dever de fiscalização por parte da sociedade.

Conforme regulamentação (21), os processos de consulta à comunidade são deflagrados pelo Conselho Superior, com antecedência mínima de 90 dias em relação ao término dos mandatos de reitor e diretores-gerais dos *campi* (Art. 3º). Uma vez iniciados, os processos deverão finalizar em até 90 dias corridos (Art. 3º, parágrafo único). A primeira etapa do processo constitui-se pela convocação das eleições para os membros das Comissões Eleitorais Central e dos *campi*, normalmente conduzida por uma comissão temporária, indicada pelo próprio Conselho Superior.

Escolhidas as Comissões Eleitorais previstas no decreto presidencial (21), estas são incumbidas da execução do processo eleitoral para reitor e diretores-gerais. Nesta etapa, a Comissão Eleitoral Central procede com a elaboração e publicação do regulamento eleitoral. Em seguida, inicia-se o período de inscrição e homologação de candidaturas, com seus respectivos prazos de recursos e julgamento pelas Comissões Eleitorais. Estabelecidos os candidatos, estes

são autorizados a realizar suas campanhas, observado o regulamento eleitoral do processo e, por fim, a eleição propriamente dita, que pode ocorrer em um ou dois turnos, conforme estabelecido pelo Conselho Superior.

Durante todo o processo, as Comissões Eleitorais, nos seus respectivos âmbitos de competência, devem exercer a fiscalização das ações relativas aos procedimentos, visando ao cumprimento do regulamento eleitoral, bem como deliberar sobre os recursos interpostos. Devem providenciar o apoio necessário à realização do processo de consulta, publicar listas de eleitores, credenciar fiscais e fazer os encaminhamentos dos resultados às instâncias previstas no decreto (21).

Ainda, conforme o decreto (21), os processos de consulta ocorrem a cada quatro anos, sendo estabelecido que os mandatos de diretores-gerais são coincidentes em relação ao mandato do reitor. Os *campi* em processo de implantação, por outro lado, realizarão seus processos de consulta à comunidade após cinco anos de efetivo funcionamento, contados da publicação de ato ministerial autorizando o início das atividades.

3.3 Ameaças aos Processos de Consulta à Comunidade

Embora o processo apresentado na Seção 3.2 seja relativamente simples, existem vários problemas que podem ser elencados, que afetam a transparência e a qualidade do resultado, podendo ser divididos quanto ao agente responsável por sua execução.

Um dos elementos mais críticos, cujos agentes são as próprias Comissões Eleitorais, refere-se ao próprio tempo de execução. Por força legal, todo o processo deve estar compreendido no interstício de 90 dias, a contar da deflagração, no qual duas eleições devem ocorrer, a saber, a eleição das Comissões Eleitorais e as consultas à comunidade propriamente ditas. O intervalo entre a deflagração e a efetiva publicação do regulamento eleitoral reduz o tempo disponível para a execução dos processos realmente importantes, implicando em menor prazo para divulgação de plataforma de governo, interação com a comunidade acadêmica, debates, enfim, todos os elementos necessários a uma escolha bem informada e consciente. Embora possa ocorrer por razões externas, como atrasos na definição das Comissões Eleitorais, há uma possibilidade de que estas, intencionalmente, reduzam esses prazos, postergando a publicação do regulamento eleitoral, caso essa ação possa favorecer algum candidato.

Espera-se que os membros das Comissões Eleitorais ajam com ética e imparcialidade, mas não se pode esquecer que são servidores docentes e técnico-administrativos e discentes que constituem tais comissões. Eles trazem suas próprias inclinações e interesses para o processo e, havendo falha na fiscalização por parte da própria comunidade, terão praticamente poderes ilimitados em sua condução. São também esses membros os responsáveis pelo julgamento de recursos, aplicação de sanções aos candidatos e apuração dos resultados. Se o regulamento eleito-

ral não oferecer detalhamento de qualquer uma dessas atividades, ficará ao poder discricionário das Comissões Eleitorais decidi-lo.

A falta de isenção dos membros também pode influenciar os eleitores. Qualquer manifestação de um membro, verbalmente ou por escrito, no ambiente de trabalho ou em redes sociais, pode ser interpretada como apoio a algum candidato, fazendo com que o equilíbrio das campanhas deles seja afetado. O suposto apoio poderá induzir indivíduos na parcela de indecisos, que se deixariam persuadir pela autoridade eleitoral em vez de fazer uma análise minuciosa das propostas, com o propósito de definir seu voto.

Outra fragilidade do processo encontra-se nas ações dos candidatos e, em certo grau, dos próprios eleitores, baseada em motivações pessoais. Pela fórmula dada na Equação 3.1, pode-se deduzir que, embora os pesos de cada segmento sejam iguais, contribuindo equitativamente na composição do resultado final, os votos individuais não o são. Segmentos com maior número de membros, como o segmento discente, possuem uma contribuição individual menor que os demais. Um candidato poderá valer-se dos quantitativos dos eleitores e focar em estratégias de coerção ou de compra de votos dos segmentos que possuam maior peso individual, visando contrabalançar algum segmento em que esteja em situação desfavorável.

Em abril de 2016, o Ministério da Educação emitiu portaria criando um modelo de dimensionamento de cargos efetivos, cargos de direção, funções gratificadas e comissionadas, no âmbito da Rede Federal de Educação Profissional e Tecnológica (Rede EPT), que inclui os Institutos Federais (26). Cada unidade (reitoria, *campus*, unidade de ensino descentralizada de CEFET, etc.) recebeu uma classificação e um quantitativo de cargos para composição de sua estrutura organizacional.

A Tabela 2 apresenta a composição proposta pelo MEC para a Rede EPT. A coluna TAE refere-se ao quadro total de Técnicos Administrativos em Educação. As colunas CD1–CD4 referem-se ao número de Cargos de Direção, de níveis 1 a 4, atribuídos a cada unidade, conforme a classificação, assim como as colunas FG1–FG2, correspondem às Funções Gratificadas de nível 1 e 2, respectivamente. Não estão representadas as FCC (Função de Coordenação de Curso), que são distribuídas de acordo com o número de cursos técnicos de nível médio, de graduação ou de pós-graduação, presenciais ou à distância, com matrículas informadas nos sistemas de informação do Ministério da Educação, conforme regulamenta a portaria (26). Cargos de Direção e Funções Gratificadas são de livre designação do gestor, salvo disposição estatutária ou regimental em contrário, destinados à remuneração dos cargos e funções da estrutura organizacional. As FCC são concedidas à guisa de remunerar as atividades dos coordenadores de curso. A Tabela 3 apresenta os valores vigentes dos cargos e funções. Não fica explícito, no instrumento legal (26), se as funções dos níveis FG3 a FG9, quando previamente existentes no quadro da instituição, seriam devolvidas ao Ministério da Educação ou se continuariam disponíveis.

A partir da análise da Tabela 2, pode-se observar que o segmento técnico-administrativo terá sempre uma contribuição *per capita* superior aos demais segmentos, a partir do momento

Tabela 2 – Composição do modelo de dimensionamento de cargos e funções

Tipo de Unidades	TAE	Docentes	CD1	CD2	CD3	CD4	FG1	FG2
Reitorias de 01 a 09 *campi*	100	0	1	5	8	8	18	2
Reitorias de 10 a 16 *campi*	100	0	1	5	11	10	18	2
Reitorias de 17 a 24 *campi*	100	0	1	5	14	13	18	2
Reitorias de 25 ou mais *campi*	100	0	1	5	17	16	18	2
Direção-Geral do CEFET MG	100	0	0	1	4	17	18	2
Direção-Geral do CEFET RJ	100	0	0	1	5	9	18	2
IF *Campus* — 350	200	350	0	1	5	10	10	20
IF *Campus* — 250	150	250	0	1	4	8	8	16
IF *Campus* — 150 Agrícola	100	150	0	1	4	8	8	16
IF *Campus* — 150	100	150	0	1	4	8	8	16
IF *Campus* — 90/70 Agrícola	70	90	0	1	2	4	4	8
IF *Campus* — 90/60	60	90	0	1	2	4	4	8
IF *Campus* — 70/45	45	70	0	1	0	2	4	8
IF *Campus* — 70/60 Agrícola	60	70	0	1	0	2	4	8
IF *Campus* Avançado — 40/26	26	40	0	0	1	1	0	2
IF *Campus* Avançado — 20/13	13	20	0	0	1	1	0	2
IF Polo de Inovação	0	0	0	1	0	1	0	2
CEFET — SEDE	200	350	0	0	1	7	9	14
CEFET — UNED	45	70	0	0	1	7	9	14
Colégio Pedro II — *Campus*	76	90	0	1	0	2	4	8

Fonte: adaptado de Brasil (26).

em que o quadro de pessoal for implantado. Supõe-se que seja também mais suscetível à coerção por ameaça, pois muitos cargos de nível médio, como Assistente em Administração, podem ser lotados em praticamente qualquer unidade administrativa do órgão, desde que observadas as atribuições do cargo, que são bastante genéricas. Um agente coercitivo poderia ameaçar lotar, por exemplo, um Assistente em Administração em uma unidade que lhe seja desfavorável, banindo-o ao ostracismo dentro da instituição. Cada órgão tem suas particularidades, e não é incomum encontrar setores conhecidos como locais para retaliação, sem caracterizar assédio moral contra o servidor. Diante de tal ameaça, o servidor técnico-administrativo pode ver-se compelido a votar em um determinado candidato, por crer que possa sofrer represálias. Entretanto, não está no escopo do presente trabalho avaliar a predisposição dos agentes públicos a este tipo de coerção, sendo suficiente apenas o risco potencial dessa ameaça. O estudo de Fernandes (48, p. 112) acerca das manifestações de territorialidade no mesmo ambiente corrobora com esta interpretação, ao afirmar que "as estratégias territoriais podem interferir negativamente na interação dos servidores, [...] quando os limites territoriais deixam de atender os [*sic*] interesses organizacionais para atender a [*sic*] interesses particulares." A defesa ou a conquista de territórios na instituição, na forma de cargos e vantagens, podem subverter o próprio processo democrático, permitindo que a coerção ganhe espaço.

Tabela 3 – Valores das remunerações de cargos e funções a partir de 1/1/2015

Cargo ou Função	**R$ (100%)**	**R$ (60%)**
CD1	11.111,90	6.667,14
CD2	9.228,86	5.573,31
CD3	7.292,19	4.375,31
CD4	5.295,51	3.177,30
FG1	804,49	—
FG2	541,23	—
FG3	438,79	—
FG4	223,35	—
FG5	181,23	—
FG6	132,89	—
FG7	84,75	—
FG8	62,69	—
FG9	50,86	—
FCC	810,81	—

Ocupantes de Cargo de Direção (CD1–CD4) podem optar por receber o valor integral da remuneração do CD ou a remuneração do próprio cargo acrescido de 60% da remuneração do CD.

Fonte: adaptado de Brasil (25).

O segmento docente, por sua natureza, tem uma resistência maior a esse tipo de coerção, uma vez que não pode ser lotado fora de sala de aula e as matrizes curriculares determinam a demanda de atividades de cada professor. Por outro lado, o número de aulas pode ser usado como ferramenta do agente de coerção, que poderá ameaçar o docente com uma carga horária elevada em classe. Este cenário pode ocorrer especialmente quando a cultura da instituição for de distribuição de aulas feita por uma única autoridade, como um diretor de ensino ou coordenador pedagógico (dependendo da estrutura organizacional). Quando a distribuição é feita em reuniões em que todos os docentes da mesma área possam realizar um balanceamento ou, em grupo, resistir a pressões dessa natureza, esse ataque geralmente fica enfraquecido.

Outro ataque possível é a venda de votos. A moeda de troca pode ser, por exemplo, a distribuição de cargos e funções, que podem assumir um apelo de complementação salarial, conforme observado na Tabela 3. Além dos cargos e funções, as promessas de concessão de movimentação para outras localidades (remoção e/ou redistribuição) mais próximas da cidade de origem do servidor (docente ou técnico-administrativo) ou a ameaça de impedi-las de acontecer podem, conforme o caso, servir para venda de voto ou coerção do servidor.

3.4 Infraestrutura de TI Típica de um Instituto Federal

Os IF, em sua essência, são instituições bastante heterogêneas, mesmo quando observados dentro de seu próprio escopo. Foram criados em 2008 pela fusão de antigas autarquias, tais como Centros Federais de Educação Tecnológica e Escolas Agrotécnicas Federais, que possuíam suas respectivas particularidades. Desde sua implantação, novos *campi* foram criados, com o intuito de atender metas governamentais de universalização da educação profissional e tecnológica. Esta diversidade reflete-se na própria infraestrutura de tecnologia da informação. Normalmente, é possível observar que as reitorias e os *campi* mais antigos e bem estabelecidos são providos com rede de acesso através de *links* ISDN (*Integrated Services Digital Network* — Rede Digital de Serviços Integrados) primários ou E1 (HDSL — *High-Bit-Rate Digital Subscriber Line* — Linha Digital de Assinante de Alta Taxa de Bits). Muitos destes *links* são contratados pela Rede Nacional de Ensino e Pesquisa[7] (RNP) e ligados diretamente às operadoras de telecomunicações do País. Outros são licitados pela própria instituição, independentes da RNP. Além disso, possuem infraestrutura melhor planejada, com o intuito de prover serviços tais como portais de notícias, sistema acadêmico, correio eletrônico institucional, dentre outros, alguns dos quais sob gerenciamento interno, contando com *firewall*, entre outros ativos de rede.

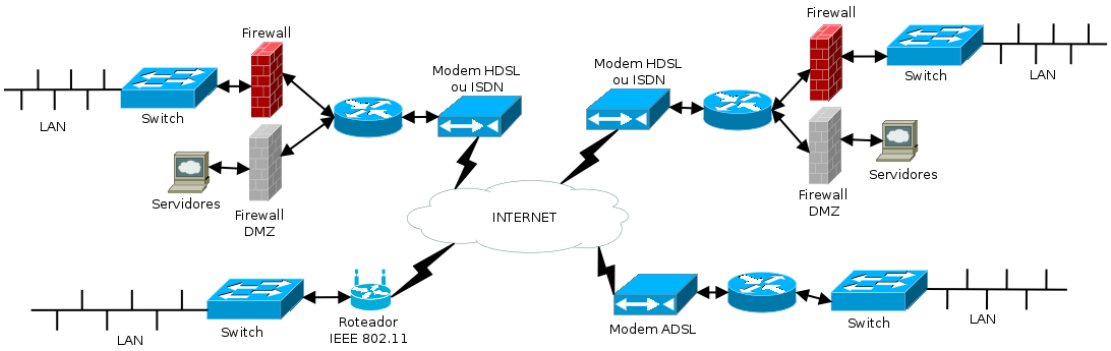
Por outro lado, em função da própria expansão, da disponibilidade de recursos humanos e financeiros, existem *campi* menores que não desfrutam desta infraestrutura. Seus serviços de *internet* são hospedados por terceirização ou na própria reitoria à qual estão vinculados, e sua rede de acesso pode dar-se por *links* ADSL (*Asymmetric Digital Subscriber Line* — Linha Assimétrica Digital de Assinante) das operadoras de telefonia ou até mesmo por redes sem fio, através de provedor de serviços de *internet* (ISP — *Internet Service Providers*). Esta infraestrutura rudimentar, quase doméstica, não dispõe de grande largura de banda e alta velocidade de acesso, nem garantia de serviço, correspondendo às limitações do próprio enlace de dados utilizado. Em especial, devido ao uso de conexões assimétricas, a velocidade de *upload* é inferior, dificultando a adoção de soluções tecnológicas que demandem grande volume de dados nessa direção. Para mais informações sobre algumas destas conexões e serviços, *vide* Stallings (103).

A Figura 1 ilustra este cenário. No canto superior esquerdo, apresenta-se uma estrutura de conexão à *internet* da reitoria, que, por hospedar, em geral, a maior parte dos serviços e, na maioria das vezes, por encontrar-se em ambientes urbanos com mais recursos, dispõe de melhores condições tecnológicas. Seguindo em sentido horário, observa-se a estrutura de um *campus* que tenha vindo de uma autarquia já consolidada e que, portanto, dispõe de estrutura similar à reitoria. Os próximos *campi* representam, respectivamente, uma conexão por ADSL e outra por redes sem fio, que, por ofertarem pequena largura de banda e baixa velocidade, se comparadas às linhas privativas (LP), sustentam apenas conexões locais e quase nenhuma infraestrutura, especialmente no que se refere a ativos de rede voltados para segurança. Destaca-se ainda que esta última rede de acesso, ao contrário das anteriores, não está diretamente ligada à rede das

[7] www.rnp.br

operadoras de telefonia, e sim à rede de um provedor de acesso, que, por sua vez, encarrega-se da conexão ao *backbone* de alguma operadora. Para fins de clareza, foram omitidos os *modems* na outra ponta do *link*, implícitos no *backbone* das operadoras e ocultos na "nuvem".

Figura 1 – Infraestrutura de conexão típica



Fonte: elaborado pelo autor.

Convém ainda destacar que algumas funcionalidades, como *firewall* e roteamento, podem estar presentes no mesmo equipamento, na instalação física, sendo representadas separadamente para ressaltá-las. Por exemplo, o equipamento (seja *appliance* dedicado ou um servidor com sistema para *firewall* configurado) pode encarregar-se de roteamento, da proteção do acesso à rede interna por meio de regras de acesso mais restritivas e o provimento de uma zona desmilitarizada (DMZ) para os serviços de *internet* oferecidos, da mesma forma que podem ser equipamentos independentes e dedicados a cada finalidade.

Com o objetivo de que a transmissão dos dados dentro do sistema eleitoral seja realizada de forma segura, é importante que ocorra em ambiente protegido, mesmo quando utilizadas redes públicas. De acordo com Andersson e Madsen (5), uma rede privada virtual (VPN — *Virtual Private Network*) é um termo genérico que cobre o uso de redes públicas ou privadas para criar grupos de usuários que são separados de outros, na rede, e que podem comunicar-se entre si como se estivesse em uma rede privada. A comunicação entre grupos de usuários geograficamente separados como se estivessem na mesma rede privada possui diversas vantagens, entre as quais pode-se citar o acesso a recursos compartilhados dentro da rede, sem a necessidade de expô-los publicamente na *internet*.

Os recursos para implementação de uma VPN, seja em camada 2 ou 3, podem ser geridos pelo cliente ou pelo provedor de acesso (5). No primeiro caso, os pacotes trafegam pelo *backbone* do provedor (ou operadora de telecomunicações) sem que qualquer dispositivo tenha ciência de que se trata de um pacote pertencente a uma VPN. No segundo, os ativos podem identificar à qual VPN o pacote pertence, conhecendo sua estrutura, além do gerenciamento ser responsabilidade do provedor.

Neste trabalho, a ênfase recai sobre as VPN implementadas sob responsabilidade do cliente e, principalmente, executadas sobre *backbones* que utilizam o protocolo IP (*Internet Protocol*), conforme descrito em Gleeson *et al.* (53). Redes privadas geridas pelo provedor podem

usar vários tipos de encapsulamento para enviar o tráfego pela rede, como, por exemplo, mas não restrito a, GRE (*Generic Routing Encapsulation* — Encapsulamento Genérico de Roteamento), IP-in-IP, IPsec (*IP Security Protocol*) ou MPLS (*Multiprotocol Label Switching* — Comutação de Rótulos Multiprotocolo), conforme descritos por Andersson e Madsen (5). A não utilização de serviços de terceiros, além de reduzir custos, visa atender às situações em que a infraestrutura presente ainda é precária, pois independe de interoperabilidade de ativos da rede local. A proposta é o uso de uma arquitetura segura de redes IP, denominada IPsec, proposta em Kent e Seo (65) e seus requerimentos para cenários remotos (64), utilizando criptografia para tunelamento dos dados. Com IPsec é possível utilizar protocolos da camada 2 como o L2TP (*Layer Two Tunneling Protocol*) para estabelecimento do enlace através da *internet* (83, 102, 109).

A implementação utilizando IPsec não exige que *hardware* dedicado seja instalado nas duas pontas do túnel, para que o tráfego seja criptografado. Existem implementações livres que podem ser instaladas em diversos sistemas operacionais, integrando-se com infraestruturas de menor custo de modo satisfatório, da mesma forma em que possuem suporte nativo em diversos *appliances* comerciais que podem ser utilizados nas estruturas melhor equipadas.

3.5 Reflexões Finais

No presente capítulo, foi apresentada a estrutura organizacional dos IF e como a legislação determina a execução do processo de consulta à comunidade para o preenchimento dos cargos de reitor e de diretor-geral de *campus*. Também foram abordados os tipos de ameaças e a infraestrutura de TI tipicamente encontrados nessas instituições. Embora sejam constituídos como instituições de ensino, observa-se que, potencialmente, não se trata de um ambiente livre de coerção.

A própria estrutura de cargos e salários, bem como as gratificações por cargos e funções comissionadas, introduzem um potencial para ações coercitivas sobre os eleitores, especialmente em relação ao segmento dos servidores técnico-administrativos em educação. A oferta de vantagens pecuniárias, na forma de cargos, ou a ameaça de represália podem comprometer a livre escolha do servidor quando estiver frente à cabine de votação. Não foram aprofundados, no entanto, estes tópicos que por si só são dignos de pesquisa independente. A observação apenas do risco latente, independentemente da comprovação, é suficiente para a análise do cenário de segurança e não compromete os resultados, embora estudos sobre territorialidade reforcem esta percepção.

Em relação à infraestrutura de TI para implantação de um sistema eleitoral, observa-se que, mesmo dentro de uma mesma instituição, coexistem diversos cenários. O sistema deverá apresentar o máximo de flexibilidade e independência em relação à infraestrutura disponível no local de votação e não deve pressupor conexão contínua à *internet*, nem altas velocidades.

4 Sistemas de Votação Eletrônica

No Capítulo 3, foi apresentado o contexto em que o presente trabalho se insere. Neste capítulo, serão abordados os fundamentos dos sistemas de votação eletrônica, com o intuito de embasar a proposta tecnológica para as eleições nos IF, assim como os tipos de fraudes às quais esses sistemas podem ser expostos. Apresenta, brevemente, informações referentes ao sistema eleitoral brasileiro (urna eletrônica), antes de discorrer acerca da auditabilidade de sistemas eleitorais, com o intuito de mitigar a ocorrência de fraudes.

4.1 Taxonomia dos Sistemas Eleitorais

Em 2002, o Congresso dos Estados Unidos aprovou o HAVA (*Help America Vote Act*), que, entre outras medidas, estabeleceu a *U. S. Election Assistance Comission* — EAC (107). A EAC tem como atribuição desenvolver e adotar novas diretrizes para sistemas de votação voluntária e prover meios para testes, certificação e cancelamento das certificações expedidas. O HAVA também estabeleceu o *Technical Guidelines Development Committee (TGDC)*, com a missão de assistir a EAC no desenvolvimento de novas diretrizes, sendo coordenado pelo NIST (*National Institute of Standards and Technology*), que também provê suporte técnico ao trabalho do comitê. Segundo Palazzolo *et al.* (81), o HAVA foi o resultado de dois anos de debates sobre reforma eleitoral, após a crise das eleições presidenciais de 2000 nos Estados Unidos.

Um sistema de votação, segundo TGDC (107), é a combinação completa de equipamentos mecânicos, eletromecânicos ou eletrônicos, *software*, *firmware* e documentação que é usada para a execução de uma eleição. Entre as atividades desenvolvidas pelo sistema de votação, encontram-se definir o formato das cédulas, lançar e contar votos, relatar ou exibir os resultados da eleição, além de manter e produzir qualquer informação de auditoria. Também fazem parte do sistema as práticas e a documentação usada para identificar os seus componentes e as suas versões, testá-lo durante seu desenvolvimento e manutenção, manter registros de erros e defeitos apresentados por ele, dentre outras.

O histórico do uso de sistemas de votação, nos Estados Unidos, é bastante rico, conforme descrito em Craig *et al.* (41), Mohen e Glidden (72), Post (88) e Saltman (96) e outros autores. Destaca-se pela introdução ao uso das cédulas australianas, que foram criadas no estado de Victoria (Austrália) em 1856, com a impressão padronizada dos nomes dos candidatos, realizada pela autoridade eleitoral, para uso em ambiente secreto pelo eleitor, que faria suas marcações em sigilo. Na década de 1890, o estado americano de New York introduziu o sistema de alavancas mecânicas. Na década de 1970, foram introduzidos os cartões perfurados no processo eleitoral, permitindo sua leitura por sistemas computadorizados. Posteriormente, este sistema se aperfeiçoaria em leitura óptica, realizada por marcações a lápis ou caneta no papel, em vez de

perfurá-lo (*marksense*), chegando aos sistemas de registro direto eletrônico (DRE), no qual o voto é apenas um registro em um sistema computacional.

Entretanto, não há uma padronização no uso dos sistemas de votação. Ao contrário do Brasil, que utiliza uma urna eletrônica (analisada na Seção 4.3) padronizada pelo Tribunal Superior Eleitoral, cada condado americano tem autonomia para escolher seu próprio sistema eleitoral, de tal modo que diversas das tecnologias supracitadas coexistem atualmente. Por isso, a eleição presidencial de 2000 foi um marco histórico, pois a dificuldade de estabelecer uma recontagem segura dos cartões perfurados da Flórida foi amplamente noticiada em todo o mundo e demonstrou a fragilidade desse sistema. Cf. (41, 47, 99, 114).

Para fins de classificação dos sistemas eleitorais, é necessário estabelecer uma taxonomia. Para este propósito, foram consideradas as categorias propostas na literatura consultada (60, 78, 107). Excluíram-se da classificação as instâncias específicas desses, visando estabelecer categorias gerais que possam abranger os sistemas eleitorais disponíveis.

Segundo TGDC (107), a classificação tradicional é baseada no tipo de mecanismo usado para registro do voto e, posteriormente, quanto ao local em que as cédulas são apuradas. Em relação a este, podem ser sistemas de votação de **apuração no recinto** (*precint count*) ou de **apuração centralizada** (*centralized count*). Estes correspondem, respectivamente, aos casos em que a totalização dos votos ocorra no recinto de votação (seção eleitoral, usando terminologia brasileira) ou estes sejam transportados para um ponto central onde todos os dados serão tabulados em conjunto.

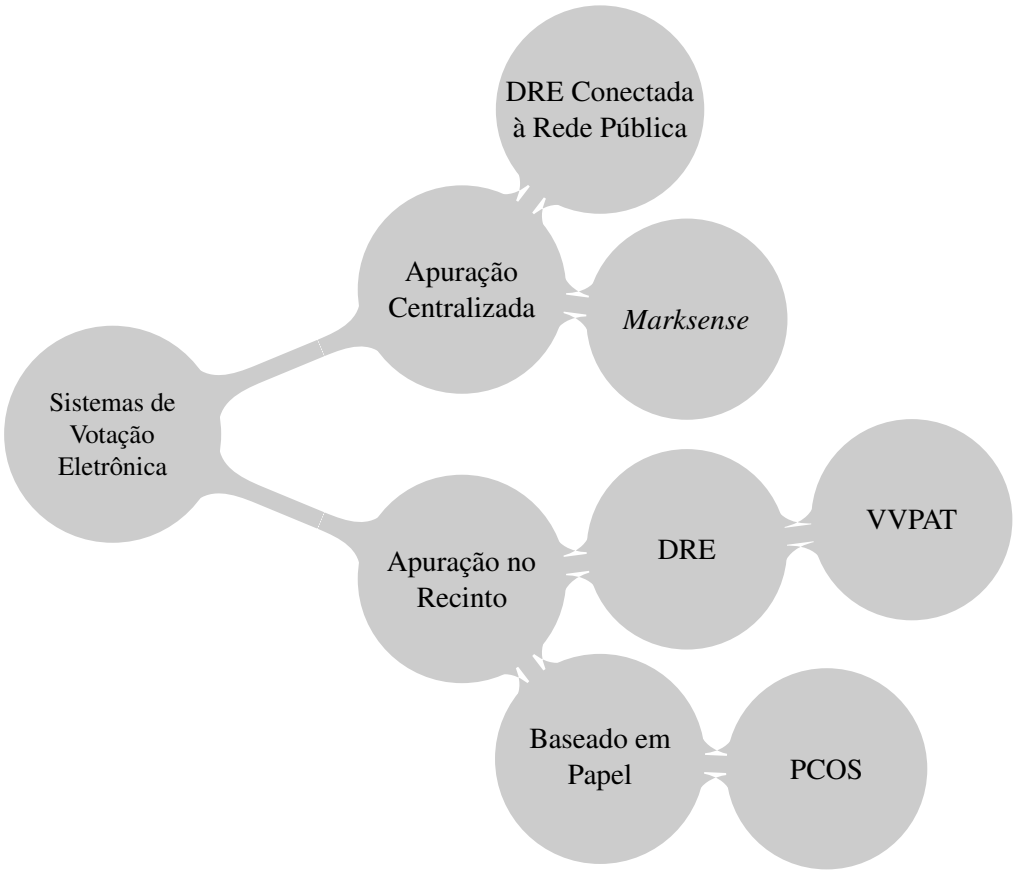
Quanto ao mecanismo de registro do voto, os sistemas eleitorais podem ser **baseados em papel** (*paper-based*), **DRE** ou **DRE conectadas à rede pública de dados**. No primeiro tipo, os votos são marcados pelo eleitor (ou por equipamento auxiliar que não registre a sua opção) em cartões ou folhas de papel, que serão tabulados posteriormente em equipamento dedicado a esse fim (*marksense*). Máquinas DRE coletam os votos por meio de interface com o eleitor, gravam, contam e geram relatórios em mídia eletrônica e/ou impressa. O terceiro tipo é uma especialização do primeiro, que se conecta a uma rede pública de dados para transmitir voto a voto, em lotes ou ao término do período de votação. Por sua natureza, possuem requisitos de segurança específicos, que justificam sua separação em TGDC (107). Podem-se enquadrar, nesta categoria, não apenas as máquinas de votação, mas também os sistemas de votação remotos, via *internet*, como uma especialização desta categoria.

Em Jardí-Cedó *et al.* (60) e Norden (78), encontra-se uma segunda especialização dos sistemas DRE, que foram denominados **DRE com VVPAT** (*Direct-Recording Electronic with Voter Verifiable Paper Audit Trail*). Este sistema de votação é composto por uma máquina que registra o voto eletronicamente em uma base de dados e produz um registro impresso dele, que é conferido e aceito/rejeitado pelo eleitor como prova. Este registro é recolhido pelo equipamento e utilizado para recontagens, como evidência física. No mesmo texto, sistemas que utilizam cédulas marcadas pelo eleitor e submetidas a um *scanner* óptico para apuração são denominados

PCOS (*Precinct Count Optical Scan*), uma especialização dos sistemas *marksense* com apuração no recinto de votação.

A Figura 2 ilustra as categorias apresentadas e como se relacionam.

Figura 2 – Categorias de sistemas de votação eletrônica



Fonte: elaborado pelo autor.

4.2 Fraudes Eleitorais

Conforme apresentado na Seção 3.2, o processo de consulta à comunidade para eleição de reitor e diretores-gerais é um dos mais complexos, dentre as diversas eleições que geralmente ocorrem no âmbito de uma instituição de ensino. Entre outros fatores, destaca-se a pequena janela de tempo disponível para a realização de todo o processo, a dispersão geográfica dos *campi* na área de atuação do IF e, de certa forma, a própria tensão do processo.

Normalmente, são adotados a votação em cédula de papel e o escrutínio manual para a condução das consultas. Dada a dispersão geográfica típica dos IF, também é comum que a mesa receptora dos votos, ao término do horário de votação, exerça a função de mesa escrutinadora, apurando-os em cada seção eleitoral. Deve-se esta miscigenação de papéis ao intuito de agilizar o processo, sem depender dos deslocamentos para um local central de totalização.

Entretanto, estes são exatamente os pontos de fragilidade do processo. Com o número de locais de votação, as atividades de supervisão das respectivas comissões eleitorais tornam-se pulverizadas, tanto quanto o exercício do direito de fiscalização do processo por parte dos candidatos, que podem não ter recursos para envio de fiscais a todos os locais em que a votação estiver sendo realizada. A transparência do processo reside unicamente na idoneidade dos membros das mesas receptoras, que, por sua vez, possuem sua própria afinidade política. Casos de fraudes eleitorais, executadas pelos mesários, não são impossíveis em eleições conduzidas pela Justiça Eleitoral, e seria excesso de confiança crer que não pudessem acontecer no ambiente acadêmico. A presunção de idoneidade não elimina o dever de fiscalização por parte da sociedade.

A questão que paira no processo é quem fiscalizará os trabalhos das comissões eleitorais e das mesas receptoras[8]. O processo eleitoral transparente deve garantir que todas as etapas, desde o cadastramento dos eleitores, o depósito dos votos na urna, sua apuração, a totalização e a divulgação dos resultados, possam ser acompanhadas por qualquer indivíduo. Dúvidas lançadas no processo, que não possam ser esclarecidas com fatos e registros indubitáveis, maculam-no de forma indelével.

Segundo Norden (78), uma forma de pensar no processo eleitoral é visualizá-lo como um fluxo de informação. O fabricante apresenta ao eleitor as opções de voto por meio da máquina de votação; este registra suas escolhas, que serão apuradas ao término do horário destinado a este fim; os resultados locais serão disponibilizados aos mesários e transferidos a um centro de totalização, onde serão consolidados junto aos demais para compor resultados regionais, estaduais ou nacionais. Portanto, ataques em sistemas eleitorais com o intuito de alterar o resultado podem acontecer em qualquer ponto desse fluxo de informação, ilustrado na Figura 3.

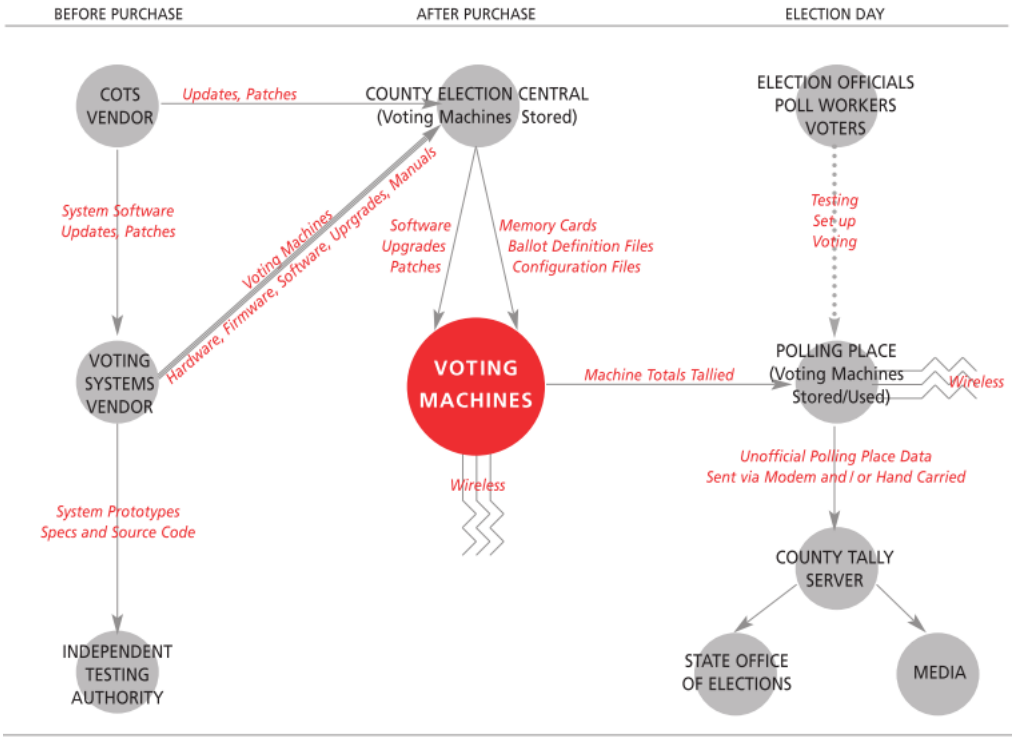
Para Norden (78), existem 9 categorias de ataques a esse fluxo de informação:

Inserção de *software* corrompido nas máquinas antes do dia da eleição: é um ataque direcionado à máquina propriamente dita, que ocorre antes de sua instalação nas seções eleitorais. Qualquer pessoa com acesso ao equipamento (fabricante, autoridade eleitoral, etc.) pode introduzir *software* corrompido ou um *malware* que force o mau funcionamento de alguma forma, como registro incorreto ou desvio de votos, adicionar ou perder votos, saltar cargos, etc.

Redes sem fio e outros ataques de controle remoto: este também se configura em um ataque à máquina de votação, podendo ocorrer no dia da eleição ou até mesmo antes. Geralmente está associado a ataque de *software* corrompido, em máquinas que possuam componentes de comunicação sem fio. Usando um dispositivo móvel com acesso a redes sem fio, um

[8] "*Quis custodiet ipso custodes?*" é uma clássica frase latina, geralmente traduzida como "quem nos guardará dos guardiões?", aplicável no contexto em função da necessidade de transparência nos processos eleitorais e ampla fiscalização da comunidade.

Figura 3 – Fluxo típico de informação de e para máquinas de votação



Fonte: Norden (78).

atacante pode instruir a máquina a ativar ou desativar o ataque de *software*, mandar suas próprias instruções maliciosas ou tentar obter acesso aos dados registrados.

Ataque aos servidores de totalização: o servidor de totalização é um tabulador central que calcula o total de votos para uma determinada jurisdição. O ataque ocorre após o término da eleição e do registro dos votos nas máquinas e pode ser direto (nas bases de dados que armazenam os totais) ou indireto (interceptação da comunicação para o servidor). Em ambos os casos, o ataque visa à alteração ou exclusão dos totais reportados ou dos dados usados para computá-los.

Descalibração das máquinas: as máquinas de votação usam algum método para interpretar e registrar eletronicamente a opção do eleitor. Quando usado um *display touch screen*, o eleitor toca em uma região na tela para selecionar uma opção. Se a calibração estiver incorreta, uma área da tela pode ser considerada como seleção de um candidato diferente do desejado pelo eleitor. Mesmo que vários eleitores percebam a troca e mudem a opção, corrigindo o voto, há alguma chance de que alguns não percebam esse registro incorreto, tendo seus votos desviados em favor de outro candidato.

Desligamento de partes do sistema destinadas à assistência ao eleitor: este é outro ataque direcionado à máquina, com o intuito de desativar mecanismos que auxiliem o eleitor durante o processo de registro do voto. Por exemplo, em sistemas PCOS, caso o eleitor assinale um número maior (*overvote*) ou menor (*undervote*) de opções, o *scanner* pode

devolver a cédula para que o eleitor a corrija. Se esse mecanismo for desativado, o voto do eleitor poderá ser anulado (o *overvote* pode ser compreendido, dentro do sistema eleitoral brasileiro, como o voto nulo, em que o eleitor marca mais de um candidato para o mesmo cargo) ou incompleto (equivalente ao voto em branco, caso o eleitor tenha condições de selecionar mais de uma opção por cargo). Em ambos os cenários, a intenção do eleitor poderá ser registrada de forma diferente, sem receber auxílio do sistema para corrigi-lo antes de lançá-lo.

Ataques de negação de serviços: este ataque cobre uma ampla gama de possibilidades. Essencialmente, visa evitar que as pessoas votem, tornando difícil ou impossível registrar o voto. Por exemplo, pode ocorrer pela inserção de *software* corrompido ou pelo dano físico a uma máquina ou a um conjunto destas, geralmente orientado àquelas seções em que o candidato favorecido pelo atacante tenha menor preferência entre os eleitores.

Ações por mesários corruptos/terceiros para afetar o lançamento dos votos: estes ataques variam da ativação de um ataque por *software* já inserido no equipamento ao desligamento de funcionalidades da máquina de votar, ou, até mesmo, dando instruções incompletas ou informações enganosas a certos eleitores. Pode envolver ataque às máquinas, ao eleitor ou às informações que devem ser levadas das seções eleitorais aos centros de totalização. Este ataque também pode incluir a provisão de instruções incompletas ou não acuradas aos mesários, que, por sua vez, podem ser induzidos ao erro e afetar os resultados da seção.

Esquemas de compra de votos: este tipo de ataque visa à oferta de vantagens (financeiras ou não) ao eleitor, com o intuito que ele vote em um candidato designado ou deixe de comparecer a sua seção eleitoral.

Ataques em cédulas ou VVPAT: este ataque pode ocorrer em diversos pontos. As cédulas podem vir adulteradas antes de chegar à seção eleitoral ou a adulteração ocorre no recinto da seção (assim como os registros VVPAT) ou enquanto são transportadas para um centro de apuração, sendo substituídas ou rasuradas.

Em Norden (78), encontram-se os detalhamentos destes ataques em vários tipos de sistemas eleitorais, assim como recomendações de contramedidas que visam a sua prevenção.

Segundo Brunazo Filho e Cortiz (31), existem várias fraudes que podem acometer um processo eleitoral, sendo algumas específicas de sistemas informatizados, outras em processos manuais. Sem o objetivo de elaborar uma listagem exaustiva destas, destacam-se algumas das possibilidades elencadas pelos autores:

Eleitor fantasma: fraude de cadastro eleitoral na qual eleitores inexistentes são inseridos na listagem, permitindo a venda de votos, por parte dos portadores do cadastro fantasma, aos candidatos. No Brasil, independe da urna eletrônica, pois o título eleitoral não possui foto do eleitor, podendo persistir mesmo com o equipamento.

Clonagem de urna eletrônica: fraude que pode ocorrer nos cartórios eleitorais, com o uso do mesmo *flashcard* para carregamento (inserção do programa, cadastro de eleitores e listagem de candidatos) em duas urnas, sem a anotação da urna clonada nas tabelas de correspondências, permitindo sua troca após a votação.

Voto de cabresto: fraude fundamentada na coerção do eleitor, para que este vote em um candidato da escolha do agente coercitivo. O eleitor é induzido a crer que seu voto poderá ser descoberto (violação do sigilo) e ser recompensado ou penalizado de acordo com o voto registrado. Na prática, segundo os autores, não é necessário que haja real quebra do sigilo, bastando que o eleitor creia que seja possível.

Compra de votos: modalidade em que o eleitor vende o próprio voto em troca de recompensa financeira ou pessoal. Por não haver garantias de que o eleitor cumpra o acordo, é muito comum haver o "aluguel" do título de eleitor, aproveitando-se da inexistência de foto no documento eleitoral, para que alguém de confiança vote no lugar do eleitor verdadeiro.

Engravidamento de urna: fraude que ocorre por conluio da mesa receptora, em que votos de eleitores ausentes são introduzidos como se estes de fato tivessem votado. Realiza-se normalmente alguns minutos antes do término do período de votação, aproveitando as abstenções existentes. Pode acontecer até com a urna eletrônica biométrica, uma vez que o presidente da mesa pode autorizar um voto mesmo que a leitura da impressão digital tenha falhado.

Eleitor anulado: com o uso de urnas eletrônicas e a impossibilidade de voto simultâneo na mesma seção, em cabines separadas, o programa permite que o presidente da mesa receptora anule a votação de um eleitor que esteja demorando muito além do período estimado, visando agilizar o atendimento da fila. Isso abre precedentes para que o presidente possa anular a votação, de forma irrevogável, de um eleitor que ele suponha que irá votar em um candidato que não desfrute de sua simpatia política. Geralmente, votos para cargos majoritários (presidente, governador ou prefeito) ocorrem no final da votação, após aqueles para cargos proporcionais, podendo ser afetados por esta prática.

Adulteração dos programas da urna eletrônica: alteração dos programas que compõem o sistema eleitoral da urna eletrônica, para que os votos não sejam registrados para o candidato da escolha do eleitor, mesmo que seja corretamente apresentado na foto, antes da confirmação. Pode ocorrer dentro do processo de desenvolvimento do *software* da urna ou por outros meios (vírus ou cavalos de Troia) ao longo do processo.

Adulteração de mapas de votação: fraude que ocorre em processos de votação e apuração manuais, nos quais os votos são registrados de forma diferente do encontrado na urna, durante a apuração (mapa de votação). Facilitada pela ausência de fiscalização, pode ocorrer concomitantemente com a troca dos votos originais por cédulas fraudadas ou até pela troca da urna, visando encobrir sua existência.

Em sistemas eleitorais em que o eleitor enumera os candidatos em ordem de prioridade, torna-se possível uma fraude conhecida na literatura como **ataque italiano** (92): o agente da coerção solicita ao eleitor que registre o voto usando um determinado padrão, que poderá ser verificado pelo atacante em um boletim público. Se houver uma quantidade suficiente de opções, podem ser montadas sequências únicas que identifiquem o voto de cada eleitor. Este ataque também pode ser possível na urna eletrônica brasileira, pela análise do registro digital de voto (RDV), descrito na Seção 4.3, combinando candidatos com baixa probabilidade de votos em alguns cargos ou usando valores para voto nulo preestabelecidos, caso não haja remapeamento deste valor nulo para uma sequência que impeça o ataque.

Sistemas que utilizam cédulas pré-impressas para que o eleitor marque sua opção e a digitalize, como o *Prêt a Voter* (38), estão sujeitos ao denominado **ataque de aleatorização** (60). Nele, um agente malicioso força os eleitores a marcar uma posição específica na lista de candidatos, impressa aleatoriamente em cada cédula. Havendo número suficiente de candidatos, o atacante reduz estatisticamente a quantidade de votos para qualquer concorrente e pode verificar no boletim público se foi obedecido.

Os tipos de fraude apresentados visam apenas demonstrar que são inúmeras as possibilidades para sua ocorrência e que podem sobrevir em vários momentos ao longo do processo eleitoral. Este não deve ser reduzido, de forma simplória, ao período de votação, pois todas as etapas, do cadastro dos eleitores à apuração, são pontos de vulnerabilidade. Um fator fundamental para que possam acontecer é a falta de fiscalização, que se torna mais difícil em sistemas puramente informatizados.

Neste sentido, Benaloh (14) destaca que tecnologias modernas podem desafiar todas as medidas de proteção contra a coerção e venda de votos, como a gravação do processo de votação de forma imperceptível dentro da cabine. O processo de fiscalização, por parte de todos os atores do processo, deve ser repensado e construído com o objetivo de mitigar tais riscos às eleições.

Segundo Bogdan (20), a corrupção eleitoral como uma forma de manipulação pode ser dividida em três categorias, de acordo com o objeto de manipulação: as regras (a base legal), os eleitores (formação de preferência e expressão), o voto (administração eleitoral). Os autores ainda dividem os ilícitos em negligência (*malpractice*) ou fraude, de acordo com a intenção dolosa do agente.

Segundo este mesmo autor, os agentes podem atuar da seguinte forma:

Atores em fraudes eleitorais: eleitores, partidos políticos, oficiais eleitorais, candidatos, mídia de massa e sociedade civil, etc.

Atores em negligência eleitoral: oficiais eleitorais e servidores públicos.

A negligência pode acarretar danos ao processo eleitoral como ação culposa. Por exemplo, a lista de votantes desatualizada pode permitir, de forma indireta, o surgimento de eleitores

fantasmas ou a impossibilidade de um eleitor legítimo registrar sua intenção de voto. Caracteriza-se como fraude quando assume a natureza dolosa da ação, ou seja, o intento claro de utilizar registros inválidos de eleitores para fins de favorecimento do ato ilícito.

Esta distinção entre o dolo e a culpa é importante ao analisar a responsabilidade e a intenção de fraudar o processo eleitoral. Para Brunazo Filho e Cortiz (31), há o chamado **golpe do candidato nulo**, uma fraude que, na visão dos autores, pode valer-se da morosidade da justiça, ocorrendo pela não inserção de um ou mais candidatos na listagem da urna eletrônica. Todos os votos que não possuem correspondência são considerados nulos e, mesmo que haja percepção do eleitor, a mesa receptora não pode fazer nada. Os autores relatam caso em que vereadores deixaram de ser eleitos em função da ausência do número, na urna, ocorrendo uma nova eleição três anos após a eleição original, por decisão judicial. Entretanto, trata-se de uma negligência da autoridade eleitoral e dos demais atores responsáveis por sua fiscalização, na verificação das bases de dados utilizadas. Neste texto, considera-se fraude a ação delituosa e premeditada, ou seja, a existência de ação dolosa no processo. Portanto, para que o candidato nulo seja realmente uma fraude, deve preexistir a intenção de prejudicar tal candidato ou favorecer um terceiro, e, no cenário apresentado por Brunazo Filho e Cortiz (31), sob a perspectiva de Bogdan (20), é um ato de negligência não somente da autoridade eleitoral, mas de todos os responsáveis por sua fiscalização efetiva.

Portanto, para a constituição de um processo que seja robusto, minimizando a ocorrência de fraudes, torna-se necessário um sistema que favoreça a fiscalização a qualquer instante, independentemente do *software* e das pessoas envolvidas no processo, por mais idôneas que sejam.

4.3 A Urna Eletrônica Brasileira

Ao longo do presente capítulo, foram apresentadas a taxonomia dos sistemas eleitorais e algumas das possíveis fraudes que podem ocorrer. A presente seção visa apontar as características da urna eletrônica brasileira e as dificuldades do seu uso nos processos de consulta à comunidade, tendo em vista as dificuldades operacionais e técnicas desta solução.

4.3.1 Implementação da Urna Eletrônica Brasileira

A urna eletrônica brasileira, ou, simplesmente, urna eletrônica, é um dispositivo de votação da classe DRE, em que o voto é armazenado apenas digitalmente. Segundo Brasil (27), é composta por dois terminais:

- Terminal do mesário: responsável pela identificação e autorização do eleitor, com uso de biometria em alguns modelos;
- Terminal do eleitor: onde o eleitor efetua o registro de seu voto.

A Figura 4 apresenta uma urna eletrônica. Observa-se o terminal do eleitor à esquerda e o terminal do mesário com o leitor de impressão digital em sua parte superior. Pouco é publicado, por parte do TSE, a respeito da constituição do *hardware* e do *software* da urna eletrônica, ou de detalhes de seu projeto; tampouco disponibiliza equipamentos para que sejam analisados. Em relação aos detalhes do *hardware*, são raros, encontrados principalmente nos editais licitatórios para aquisição dos equipamentos por parte do TSE e em Gallo *et al.* (50). Nesse trabalho, os autores propõem um sistema baseado em *hardware* confiável, que permitiria a execução somente de *software* assinado digitalmente e empregado nas eleições presidenciais de 2010. No entanto, a proposta destes autores transfere toda a confiabilidade para a integridade *software* que será executado no equipamento, que é de total responsabilidade da equipe de desenvolvimento do TSE.

O *software*, por sua vez, não é isento de problemas graves de segurança. Como apresentado por Aranha *et al.* (7), existem diversas falhas no sistema que não se restringem apenas à falta de qualidade do código, mas perpassam pela ausência de procedimentos e conhecimentos técnicos para condução de auditorias eficazes durante o ciclo de vida dele. Segundo os autores, o programa inclui vulnerabilidades, detectadas no código, conhecidas desde 1995 e que afetam o sigilo do voto. Portanto, ao transferir ao *software* o destino da eleição, a equipe do TSE não conseguiu entregar um sistema que possa receber alguma confiabilidade.

Figura 4 – Urna eletrônica brasileira: (a) terminal do eleitor, (b) terminal do mesário com identificação biométrica do eleitor

Fonte: adaptado de Brasil (27).

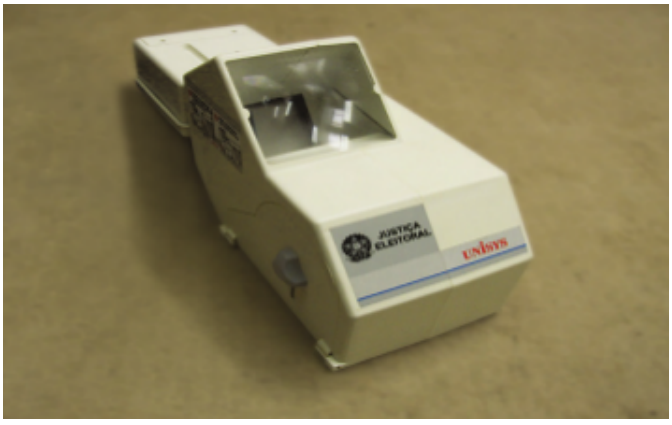
Segundo Brasil (27), o processo de votação da Justiça Eleitoral, utilizando a urna eletrônica, inicia-se às 7h30 do dia da eleição, quando ela é ligada e é feita a impressão do boletim de urna denominado "zerésima", constituído pela identificação da urna e a listagem de cada candidato seguido pelo número de votos igual a zero, de onde vem seu nome. Os mesários e fiscais presentes assinam e arquivam este relatório, como parte da documentação eleitoral. A partir das 8h, inicia-se o processo de votação, no qual cada eleitor é identificado pela digitação de seu título no terminal do mesário, com a liberação da urna para registro de seu voto. Pode

ocorrer, neste momento, a identificação biométrica, caso seja uma das seções eleitorais que tenham o cadastro atualizado para este fim. A votação continua até as 17h, com o encerramento da eleição. A urna grava os dados de seus *flashcards* em um disquete ou *pendrive* (mídia de resultados), criptografados, para que sejam levados ao local próprio para transmissão ao Tribunal Regional Eleitoral (TRE). A urna ainda emite cinco vias do boletim de urna, que são assinadas pela mesa receptora e por fiscais dos partidos políticos presentes, que contêm a identificação da seção eleitoral e da urna, o número de eleitores que registraram seu voto e o total de votos por candidato/legenda. Uma via é afixada em local visível na seção, três são encaminhadas junto com a ata para o Cartório Eleitoral e a quinta é entregue aos fiscais/representantes dos partidos políticos presentes. Se necessário, o presidente da seção poderá imprimir mais vias do boletim de urna.

Os *flashcards* mencionados são utilizados para a carga da urna, ou seja, a instalação do *software* e dos dados utilizados para o processo eleitoral, durante todo o seu funcionamento. Após a finalização, os boletins de urna são gravados na mídia de resultados.

Cabe destacar que, em 2002, por força de alteração na legislação vigente, foi aprovada a impressão do voto para conferência do eleitor. O TSE, atendendo a legislação, determinou que 8% do eleitorado nacional utilizariam a urna eletrônica com módulo impressor nas eleições daquele ano, compreendendo todo o estado de Sergipe, o Distrito Federal e pelo menos uma cidade por unidade federativa, totalizando 149 municípios e 19.223 seções eleitorais. Em função do número de problemas apresentados com esta experiência, o TSE conseguiu nova mudança da legislação, determinando o fim da impressão obrigatória do voto, ao mesmo tempo que introduziu o registro digital do voto (RDV), dentre outras medidas para aumentar a segurança da urna (90).

Figura 5 – Módulo impressor da urna eletrônica, utilizado em 2002



Fonte: TRE-RS (90).

Os motivos do insucesso na impressão dos votos são apresentados, sob a perspectiva da Justiça Eleitoral, em publicações próprias (27, 90). Arrolam-se entre eles o aumento das filas de votação e dos custos (módulo impressor, bobinas), os problemas técnicos durante os procedimentos nas seções, a dificuldade em manter o sigilo do voto em caso de travamento do papel, dentre outros. Como o foco deste trabalho não é propriamente avaliar a urna eletrônica e a

validade dos argumentos apresentados, esta discussão não será aprofundada neste texto, embora possa ser encontrada em outros autores (31, 43, 71, 111).

O Registro Digital de Voto (RDV) é mais detalhado, dentre as publicações da Justiça Eleitoral, em Brasil (29) e, de forma independente, em Aranha *et al.* (7, 8). É constituído por um arquivo em que os votos dos eleitores são registrados na urna e de onde são consolidados a "zerésima" e o boletim final de urna. Registra o voto da forma exata como digitado pelo eleitor, sem processamento e sem acréscimo de dados, sem vinculá-lo a ele. Os votos são armazenados em posições aleatórias, inclusive com registro dos cargos em localizações distintas, com o intuito de preservar o seu sigilo. Foi introduzido a partir da alteração da legislação em 2003, como ferramenta para auditoria dos partidos políticos e das coligações.

De acordo com as publicações oficiais do TSE, referenciadas nesta seção, a urna eletrônica utiliza uma cadeia de confiança entre *hardware* e *software*, ou seja, o primeiro utiliza técnicas de assinatura digital para permitir a execução de programas que sejam assinados digitalmente pelo TSE. De forma similar, o *software* verifica se o *hardware* subjacente corresponde a uma urna eletrônica oficial, abortando sua execução caso seja detectado *hardware* diferente do esperado.

Ainda quanto ao *software* da urna eletrônica, Cunha *et al.* (43, p. 39) afirmam que "para a eleição de 2008, visando padronizar o *software* de todos os seis modelos de urnas eletrônicas, o TSE adotou o Linux, de código aberto, como sistema operacional." Estes autores mencionam ainda que, nas eleições de 2000, "dois terços do *software* das urnas eletrônicas, que incluía o Sistema Operacional VirtuOS da Microbase e a biblioteca de criptografia da ABIN, **foram mantidos secretos** aos partidos e até aos próprios funcionários do TSE." (43, p. 23, grifo dos autores). O relatório técnico de van de Graaf e Custódio (111) também elenca o WindowsCE como sistema operacional do modelo 2002 das urnas eletrônicas. Em Brasil (29), menciona-se o uso de Linux e a presença de *hardware* criptográfico, referindo-se ao processo eleitoral de 2014, sem qualquer menção a código da Agência Brasileira de Inteligência (ABIN) em seu conteúdo. Em seu relatório, van de Graaf e Custódio (111, p. 26) destacam que, até onde puderam observar, "são infundadas as suspeitas de que tivesse havido interferência ou manipulação eleitoral do lado da ABIN através das funções de criptografia". Informações quanto ao sistema operacional, encontradas em Aranha *et al.* (7, 8) e van de Graaf e Custódio (111), coadunam com a informação oficial, enquanto, por outro lado, apresentam várias vulnerabilidades do sistema e fazem recomendações para sua correção.

O uso da urna eletrônica brasileira, da Justiça Eleitoral, em empréstimo a outras instituições está sujeito a regulamentação específica (28), que define a antecedência mínima de 60 (sessenta) dias para solicitação. Este prazo nem sempre é possível em função de regulamentações próprias para alguns processos eleitorais. Conforme apresentado na Seção 3.2, os processos de consulta à comunidade para eleição de dirigentes devem ocorrer no período de 90 (noventa) dias a partir de sua deflagração.

Considerando que a Justiça Eleitoral consiga desenvolver o sistema e parametrizá-lo dentro do prazo de 60 dias de antecedência do dia de votação, restam 30 dias que devem ser distribuídos no início do processo (constituição da comissão eleitoral, períodos de cadastro, impugnação e recurso de candidaturas, elaboração das listas de eleitores por segmento, etc.) e após a votação propriamente dita (interposição de recursos, recontagem de votos, finalização dos autos do processo, envio dos resultados para publicação, etc.). Portanto, em termos puramente operacionais, torna-se inexequível uma eleição com a urna eletrônica brasileira.

A regulamentação (28) também exclui a possibilidade de auditoria nos programas e nos conteúdos das mídias da urna eletrônica por entidades alheias à Justiça Eleitoral (*op. cit.*, Art. 10, § 1º). Tal limitação impede que as partes interessadas (candidatos, eleitores, comissões eleitorais, etc.) possam atestar sua confiabilidade.

A auditabilidade é fator determinante para o pleno exercício da cidadania e do princípio da publicidade na Administração Pública. Além do impedimento de auditar os equipamentos cedidos, a urna eletrônica torna impossível realizar uma recontagem externa, uma vez que o voto se desmaterializa e consiste apenas em um registro lógico. Para fins de transparência, seria necessário que qualquer parte interessada pudesse solicitar sua recontagem para a certificação dos resultados publicados.

Em função desta desmaterialização do voto, a urna eletrônica brasileira é criticada por diversos setores da sociedade, sendo um dos principais representantes a equipe do fórum Voto Seguro, que publicou suas preocupações em Maneschy e Jakobskind (71) de forma veemente. Segundo Brunazo Filho *et al.* (30), o sistema eleitoral brasileiro não permite uma efetiva auditoria dos resultados, e as restrições impostas pela autoridade eleitoral impedem a determinação da confiabilidade dos registros de votação e apuração das urnas.

De fato, o uso de urnas como as brasileiras, pertencentes à categoria DRE, ou seja, registro digital direto, sem suporte material, tem sido questionado e abolido em vários países, sendo declaradas inconstitucionais na Alemanha (33, 44, 57, 58, 67, 89, 112, 113). Segundo Maneschy e Jakobskind (71), a impressão do voto para verificação do eleitor são requisitos básicos para garantia da transparência do processo.

Além destas preocupações, também figura na literatura a redução dos riscos de coerção do eleitor, aos quais, além da distorção dos resultados, encontram-se associadas as quebras do sigilo do voto e da livre escolha do eleitor. A coerção do eleitor permite a prática conhecida no Brasil como “voto de cabresto”, no qual alguém força o eleitor a registrar um determinado voto alegando que terá meios para saber qual foi o voto registrado e, desta forma, puni-lo caso não obedeça. Nota-se que não é necessário que o agente coercitivo realmente tenha condições, de fato, de quebrar o sigilo do voto, mas apenas induzir o eleitor a crer que seja capaz de fazê-lo.

O sigilo do voto, por si mesmo, é um item da mais urgente necessidade. Qualquer sistema eleitoral, eletrônico ou não, deve garantir que apenas o eleitor tenha conhecimento de sua

intenção de voto registrada. Caso não seja garantido, além da coerção, torna-se possível a prática de compra e venda de votos, seja em vantagem pecuniária ou de qualquer outra natureza. Como apresentado na Seção 4.4, o sigilo é um dos requisitos mais encontrados na literatura.

Os sistemas eletrônicos de votação, além de permitirem o uso de tecnologias criptográficas que garantam o sigilo do voto até o momento de sua apuração, favorecem este último processo, permitindo que os resultados sejam conhecidos de maneira mais rápida. No entanto, de acordo com diversos autores referenciados neste trabalho, observa-se que somente o registro eletrônico e imaterial do voto seja insuficiente para garantir que esse resultado possa ser verificado e comprovado em casos de dúvidas, garantindo a lisura dos pleitos e afastando as suspeitas acerca do comprometimento do *hardware* e do *software* subjacentes.

4.3.2 Características Semióticas da Urna Eletrônica Brasileira

Por fim, em relação à urna eletrônica brasileira, é necessário analisar a Engenharia Semiótica do projeto de sua interface e sua alegada usabilidade. Esta análise fundamenta algumas das decisões do presente trabalho, no que se refere às demais soluções conceituadas e apresentadas nas Seções 4.1 e 4.6, e no tocante à forma como o eleitor registra sua intenção de voto.

O homem, como ser dotado de cognição, interage com diversos sistemas ao longo de sua existência, interpretando a realidade circundante em signos que a representam em modelos mentais. Notadamente, nas últimas décadas, a interação com sistemas constituídos por artefatos tecnológicos, baseados em sistemas computacionais, tem se intensificado. O objetivo primário de um *designer* de interfaces é desenvolvê-las com o foco na usabilidade. Para Leite e Souza (69, s. p.), "a usabilidade é um conceito que se refere à qualidade da interação de sistemas computacionais interativos com os seus usuários". Para estes autores, no entanto, os atuais modelos de interação são baseados em modelos e técnicas pautadas em características cognitivas do usuário, considerando-os insuficientes para o desafio de usabilidade por não considerarem o papel do projetista da própria interface no processo de apreensão do modelo de usabilidade pelo usuário.

Segundo Leite e Souza (69), a Engenharia Semiótica observa o *design* de interfaces considerando que os sistemas são, na realidade, artefatos de metacomunicação. E afirmam:

> Nesta perspectiva a interface é vista como uma mensagem unidirecional e indireta de *designers* para usuários. Esta mensagem se caracteriza pela sua capacidade de, ela própria, enviar e receber mensagens durante o processo de interação entre o usuário e o sistema. O aspecto de usabilidade que a Engenharia Semiótica visa resolver é como o conhecimento que o usuário precisa adquirir para utilizar melhor o sistema pode ser melhor "ensinado" através de interface de usuário. (69, s. p.)

Portanto, o projeto de interface homem-máquina baseado em conceitos de Semiótica visa transmitir, ao usuário, as instruções de como a interação deverá ocorrer para alcançar os objetivos desejados:

> Na Engenharia Semiótica o foco está na comunicação interpessoal entre o *designer* e os usuários. O que o *designer* transmite não é uma mensagem como a de um documento multimídia, um livro, ou um filme, mas uma mensagem interativa e dinâmica: um sistema de comunicação (para a interação) e um resolvedor de problemas (a funcionalidade da aplicação). Visto por esta perspectiva, o *design* de interfaces envolve não apenas a concepção do modelo de interação, mas a comunicação deste modelo de maneira a revelar para o usuário o espectro de usabilidade da aplicação. (69, s. p.)

Segundo Santaella (97, p. 13), "a Semiótica é a ciência que tem por objeto de investigação todas as linguagens possíveis, ou seja, que tem por objetivo o exame dos modos de constituição de todo e qualquer fenômeno como fenômeno de produção de significação e de sentido." O termo vem da raiz grega *semeion* (signo), constituindo-a como a ciência dos signos.

Neste trabalho, será considerada a Semiótica proposta pelo cientista e filósofo C. S. Peirce (1839–1914), sem demérito das demais escolas de pensamento semiótico fundadas concomitantemente aos trabalhos de Peirce (97).

De acordo com Santaella (98), Peirce classifica os signos em três modalidades, de acordo com sua relação com o objeto a que se refere:

Ícone: quando o fundamento da relação é qualitativo, como formas, cheiros, sons, volume, texturas, etc., de tal forma que o signo se pareça com o objeto que representa, seja imagem, diagrama ou metáfora. Por exemplo, a imagem de uma cruz representa, por semelhança do formato, o próprio objeto.

Índice: quando o fundamento da relação é de existência, ou seja, o signo aponta para um objeto que existe (no tempo e no espaço). Retomando o exemplo da imagem de uma cruz, seu caráter indicial aponta para objetos como "fé", "religião", "sacrifício", etc.

Símbolo: quando o fundamento da relação é uma lei (convenções socioculturais), que atribui um significado ao signo de acordo com alguma generalização. Neste caso, o signo cruz representa uma convenção que o associa a uma religião denominada Cristianismo, permitindo a associação abstrata de que os portadores deste símbolo sejam vinculados a ela.

Segundo Santaella (98), todos os signos são, simultaneamente, ícone, índice e símbolo, mas uma das características da associação será preponderante e, desta forma, se impõe sobre as demais. No exemplo, o caráter simbólico da cruz, associando-se a uma religião, é mais forte que as demais características.

É esta apreensão do significado que desempenha um papel fundamental na usabilidade de um sistema. Todo sistema é composto por diversos signos, que devem ser apreendidos, interpretados e desencadear uma ação do usuário. Quanto mais clara for a mensagem transmitida pelo *designer*, mais simples será o uso do sistema por parte do usuário.

> Quando o usuário entra em contato visual (ou, mais genericamente, sensorial) com a interface, ele realiza um esforço de interpretação e compreensão a respeito do significado de todos os seus dispositivos e da informação que eles veiculam. O conceito de signo como apresentado por Peirce (1931) mostra-nos que a mensagem que o designer envia para os usuários têm [*sic*] como expressão a interface de usuário e como conteúdo a funcionalidade e o modelo de interação definidos pelo programa que implementa o sistema. O interpretante deste signo é, para o usuário, o modelo conceitual que ele adquire a partir da interpretação da interface — que é a expressão da mensagem — durante o processo de interação. (69, s. p.)

Com o intuito de avaliar estes conceitos em uma interface, foi selecionada a urna eletrônica brasileira (27). Utilizada desde 1996, em diferentes versões de *hardware*, possui uma interface praticamente inalterada com o usuário, se considerado apenas o terminal do eleitor, onde este registra seu voto (Figura 6).

Figura 6 – Terminal do eleitor da urna eletrônica brasileira – modelo 2013

Fonte: Brasil (29).

De acordo com TRE-RS (90), uma das preocupações desde o período de incubação do projeto de uma máquina de votação eletrônica era com os eleitores com menor escolaridade. Desta forma, a interface homem-máquina deveria ser simples e funcional, ou, em termos de Engenharia Semiótica, deveria deixar claro para o usuário como é a interação esperada, para que o objetivo de introduzir os votos seja alcançado sem esforço cognitivo e, preferencialmente, sem erros. A respeito da interface, o Tribunal Superior Eleitoral (TSE) afirma:

> [...] era necessário quebrar o paradigma de como o eleitor iria indicar seu voto em um equipamento eletrônico, especialmente os idosos, os analfabetos e os cidadãos com pouca instrução.
>
> Decidiu-se, então, pela utilização de números, já que mesmo os eleitores com pouca instrução e os idosos seriam capazes de votar no novo equipamento. Por isso, o teclado da urna eletrônica foi elaborado com as teclas correspondentes aos números na mesma disposição do telefone.
>
> A indicação dos números conforme o teclado do telefone também facilitaria a votação para os deficientes visuais, diferentemente do que ocorria na votação manual. Além da facilidade, a novidade resultou na redução da quantidade de votos nulos. (27, p. 9–10)

Pode-se observar que a decisão do TSE é rica em signos, como a metáfora do teclado de telefone, as cores das teclas, além da própria inserção de dados numéricos. Em tese, essa interface foi bem-sucedida, dada a alegada redução da quantidade de votos nulos, decorrentes de erros do eleitor (usuário). No entanto, não há na literatura ou em publicações do TSE qualquer estudo de usabilidade utilizando modelos ou heurísticas de avaliação de interfaces, em parte, devido à própria indisponibilidade dos equipamentos para realização de estudos ou auditorias (28).

A interface do eleitor com o sistema de votação está limitada, primariamente, ao terminal do eleitor. Este é constituído por uma tela de cristal líquido e um teclado numérico, disposto na sequência do teclado de um aparelho telefônico, seguido de três teclas de função (**branco**, **corrige** e **confirma**), conforme apresentado na Figura 6. Todas as teclas possuem indicação impressa de seu valor ou função em português e em *braille*. As teclas numéricas são pretas, com impressão em branco, e as de função são apresentadas, respectivamente, nas cores branca, laranja e verde, com inscrições em preto. A Figura 7, extraída da capa de Brasil (29), apresenta um recorte da urna eletrônica, exibindo o teclado e suas características.

Conforme previamente apresentado, a urna eletrônica é rica em signos. O teclado (nível macro) e seus componentes (nível micro) evidenciam vários elementos semióticos ao eleitor.

Partindo do maior para o menor, observa-se que o teclado em si é um forte ícone, pois representa-se a si mesmo. A disposição das teclas conforme a configuração dos aparelhos telefônicos fortalece essa metáfora em diversos aspectos e foi explorada na mídia pelo TSE. Primeiro, traz a experiência pregressa do eleitor com aparelhos telefônicos, independentemente do grau de instrução. Em um segundo nível, a metáfora remete à característica indicial do número telefônico: uma sequência de dígitos corresponde a um destinatário da mesma forma que equivale a um candidato de forma inequívoca.

As teclas numéricas também apresentam várias características importantes. Se for considerado o eleitor analfabeto, sua votação não será prejudicada, pois o próprio TSE recomenda que o eleitor leve sua "cola" com os números de seus candidatos anotados. De fato, a prática da propaganda eleitoral é que os chamados "santinhos" do candidato sejam apresentados com os números, na sequência correta de votação, em seu verso, que podem ser utilizados pelo eleitor.

Figura 7 – Teclado da urna eletrônica brasileira

Fonte: Brasil (29).

Mesmo partindo do pressuposto de que o eleitor não tenha nenhum conhecimento dos números, a própria natureza icônica dos dígitos permite a votação. Por exemplo, o signo **5** é um ícone do dígito indoarábico **5**, que possui qualidades próprias, como seu contorno específico e *sui generis*, que pode ser comparado pelo eleitor e encontrado. Além disso, sua natureza indicial remete ao conceito de cinco objetos contáveis, que pode ser interpretado por aqueles que tenham desenvolvido esta competência, que geralmente é independente de escolarização (normalmente, o ser humano desenvolve o conceito de contagem na primeira infância, antes de desenvolver a capacidade de operar sobre estas grandezas). A mesma inferência é aplicável à representação em *braille*.

Nas teclas de função, encontram-se mais signos associados. O voto em branco, que representa a abstenção do eleitor em relação àquele cargo apresentado na tela (e, por consequência, representa um voto inválido, não ponderando para candidato(a)), está associado a uma tecla que possui a palavra **branco** grafada em caracteres latinos e em *braille*, além da coloração branca aplicada à tecla. Com um único toque, o eleitor registra sua ausência de intenção de selecionar um candidato para aquele cargo específico.

Caso tenha feito uma inserção incorreta, que a urna interpreta como um voto nulo, ou caso mude de ideia durante o próprio processo de votar, o eleitor pode alterar sua seleção em andamento pressionando a tecla **corrige**, representada por um botão na cor laranja. Ao ser pressionada, o valor atual é apagado e o eleitor pode fazer uma nova digitação. A cor laranja foi

convencionada, pelo TSE, como um estado de alerta, como normalmente acontece com a cor âmbar em sistemas de sinalização. É um signo associado ao símbolo de interromper uma ação, prestar atenção e repetir o processo. A cor laranja, no círculo cromático, é uma cor secundária produzida pela fusão do amarelo e do vermelho, situando-se entre ambos, que convencionalmente representam atenção e parada, respectivamente. Por analogia, pode-se entender que a correção do voto situa-se entre o estado de atenção do eleitor a uma situação indesejada, sem paralisar completamente o ato de votar.

Por fim, a última tecla de função é **confirma**, que embora apresente algumas das características das demais, distingue-se não apenas pela cor verde (símbolo convencional para prosseguir, aceitação, etc.), mas possui um tamanho maior em relação às demais, destacando-se no canto inferior direito do teclado. Sua proeminência atrai a atenção do usuário, sinalizando que, ao pressioná-la, sua vontade será **confirmada**, de forma irrevogável, pelo sistema, passando para o próximo cargo ou finalizando a votação, de acordo com o estágio atual.

Analisadas as teclas individualmente, é necessário observar o processo de votação propriamente dito, ou seja, o uso do sistema. Os dígitos são inseridos em sequências com, no mínimo, dois algarismos. Este valor não representa uma quantidade ou uma sequência, mas uma convenção social que o associa a uma legenda partidária. De fato, em eleições para cargos majoritários (presidente, governador e prefeito), o número do candidato é o mesmo que representa sua legenda, com dois dígitos. Para cargos proporcionais, o número do partido é seguido por uma sequência de outros dígitos que identifiquem, de forma única, um determinado candidato, como senador, deputado, vereador, etc. Ao eleitor é facultado votar, nesses casos, apenas na legenda, ou seja, digitar apenas os dois algarismos do partido de sua preferência. Essa natureza é dupla, indicial (refere-se a um objeto existente) e simbólica (a opção filosófica do eleitor em relação ao partido político).

Um diferencial apresentado pela urna eletrônica, sob o aspecto semiótico, é a apresentação da foto do(a) candidato(a), caso o número seja válido. Uma foto é um signo indicial que representa aquela pessoa, permitindo ao eleitor, mesmo que não possa ler os dados na tela (nome, filiação partidária, etc.), identificar os traços fisionômicos e certificar-se de estar votando em quem realmente deseja (27). Sistemas baseados em alavancas para perfuração da cédula, marcação a tinta em cédula em papel, menus em telas sensíveis ao toque, comuns em outros sistemas de votação, não costumam apresentar esta característica.

O uso do sistema, por si mesmo, tem todo um apelo indicial e simbólico. O eleitor registra o número do candidato, que, ao mesmo tempo, apresenta as duas naturezas, de índice e símbolo. A interface na tela vai apresentar um novo índice, a foto do candidato, para que o eleitor analise se há correspondência entre sua intenção e o que foi obtido pela urna. Por fim, após essa análise, selecionará os símbolos convencionados para sinalizar uma alteração de estado mental para correção do voto ou confirmar sua escolha. O fator simbólico encontra-se não apenas na cor ou no tamanho das teclas, mas no próprio signo que representa a ação, grafado em sua superfície.

No processo de informatização do voto, a votação indicial e simbólica dos números ocupou o lugar da marcação de uma opção ou a escrita do nome do candidato, nas cédulas de papel. Na votação em papel, era possível escrever o número, nome do candidato ou legenda para os cargos com votações proporcionais (vereadores, deputados e senadores), enquanto os cargos com votação majoritária (prefeito, governador, presidente) tinham os nomes impressos para que o eleitor assinalasse a opção desejada. A marcação poderia ser facilmente implementada com uma tela sensível ao toque, talvez ao custo da acessibilidade aos portadores de deficiência visual ou dificuldades motoras. Mas a substituição da escrita do nome do candidato pelo número, em um teclado simples, e a padronização de todos os votos por meio da digitação dos números representaram de fato um grande avanço. Aos eleitores analfabetos, a grafia de um dos nomes registrados pelo candidato para votação aumenta as chances de anulação do voto, por questões ortográficas ou simplesmente por exclusão, pois eles não têm como manifestar sua opção com facilidade.

O uso dos números, diante das características semióticas apresentadas, tem condições de realmente favorecer a redução do quantitativo de votos incidentalmente nulos, ou seja, aqueles invalidados sem intenção do eleitor. A interface homem-máquina, sob a óptica da Engenharia Semiótica, deixa claro, por várias pistas visuais e cognitivas, qual é o uso desejado e leva o eleitor atento à conferência detalhada daquilo que é apresentado. O sistema também apresenta baixa viscosidade, ou seja, para desfazer uma ação indesejada, o efeito é contido apenas ao cargo em votação no momento e requer somente o pressionamento de uma tecla, para voltar ao estado inicial e permitir uma nova inserção dos números. Entretanto, para alcançar essa baixa viscosidade, traz como efeito colateral a irreversibilidade dos votos confirmados, o que se destaca pela proeminência da tecla **confirma** no painel do dispositivo.

4.4 Requisitos de Sistemas Eleitorais

Um dos procedimentos que assumem importância na implementação de qualquer sistema é uma elicitação de requisitos satisfatória. Os requisitos podem ser funcionais, ou seja, determinam o funcionamento do sistema, ou não funcionais, isto é, não se relacionam diretamente a como o sistema executará suas ações. Estes últimos são importantes por definirem comportamentos esperados ou por serem percebidos pelo usuário e estão mais ligados à percepção da qualidade ou segurança de um sistema.

Observando-se a literatura, podem-se encontrar os seguintes requisitos de segurança (não funcionais) em sistemas de votação eletrônica, independentemente do tipo utilizado (Seção 4.1). Foram listados, em ordem lexicográfica, para fins de organização e, pelo número de referências que os endereçam, pode-se perceber quais são os mais frequentemente cotados:

Auditabilidade: devem existir meios para auditar a eleição em caso de reclamações (49, 106).

Autenticação: os eleitores devem comprovar sua identidade para obter acesso ao sistema eleitoral (49, 104, 106).

Certificabilidade: o processo eleitoral completo, incluindo *hardware* e *software* utilizado, deve ser certificável de acordo com critérios preestabelecidos (49, 104).

Completude: todos os votos válidos devem ser contados corretamente (68, 82, 116).

Confiabilidade/Robustez: o sistema deve funcionar sem comprometer os votos, mesmo na ocorrência de falhas de sistema. Um sistema também é robusto se tolera um comportamento faltoso de uma coalizão de participantes de tamanho razoável, sem afetar a eleição e permitindo a detecção dos eleitores maliciosos (35, 59, 70, 104, 116).

Controle de acesso: somente autoridades eleitorais podem acessar certos processos e/ou dados dentro do sistema eleitoral (106).

Democracia: quando observados os requisitos de elegibilidade e unicidade (101).

Elegibilidade: somente eleitores aptos e registrados previamente podem participar do processo de votação (1, 35, 49, 68, 82, 104, 116).

Equidade: o eleitor não possui nenhum conhecimento da distribuição de votos até que a apuração seja anunciada, de tal forma que ele possa lançar seu voto independentemente e não influenciado (1, 11, 35, 68, 82, 101, 116).

Livre arbítrio: eleitores devem ser capazes de votar com livre arbítrio e não sob coerção (54).

Integridade ou acurácia: certificar que as seleções do eleitor no terminal de votação correspondam aos dados gerados pelo sistema de tabulação (apuração). Inclui o conceito *counted as cast*, ou seja, o que foi selecionado pelo eleitor será tabulado com exatidão pelo sistema eleitoral. Um sistema é acurado se e somente se nenhum voto pode ser modificado, adulterado, duplicado, inserido ou removido sem detecção, após seu registro (35, 54, 59, 101, 104, 106, 116).

Isenção de disputas: deve prover mecanismo para resolver todas as disputas em qualquer estágio, referentes à validade da eleição, usando informações que são publicamente disponíveis (1, 59, 116).

Privacidade, anonimato ou sigilo: impossibilidade de correlacionar o voto ao eleitor, identificando sua manifestação na cédula (1, 11, 35, 49, 54, 59, 68, 70, 82, 101, 104, 106, 116).

Proteção contra ameaças externas: garantir que sistemas de votação sejam protegidos de vírus, *malware* ou *hackers* (106).

Rastreabilidade: todo eleitor deve receber uma prova de que seu voto foi contado corretamente, podendo ser uma trilha em papel que não seja mantida pelo eleitor (49).

Segurança de transmissão de dados: garantir a confidencialidade dos votos, durante a transmissão dos dados (106).

Sem comprovantes ou incoercibilidade: eleitores não podem provar a terceiros como votaram, visando à prevenção de venda de votos ou coerção (11, 35, 49, 54, 68, 70, 82, 101, 104, 116).

Solidez: qualquer voto inválido deve ser excluído da apuração (68, 82, 116).

Unicidade, exatidão ou cédula não reutilizável: somente um voto por eleitor é contado na apuração, impedindo que a mesma cédula seja utilizada mais de uma vez pelo eleitor ou por outros (1, 49, 68, 70, 82, 104, 116).

Verificabilidade: deve ser possível verificar que todos os votos foram contados. Pode ser **individual**, quando cada eleitor é apto a verificar se seu voto foi contado adequadamente, ou **universal**, se e somente se qualquer observador, passivo ou não, puder ser convencido de que a apuração final é corretamente computada a partir dos votos lançados (1, 11, 35, 49, 59, 68, 70, 101, 104, 116).

Observando-se a frequência dos requisitos entre os autores, é possível determinar que, entre eles, a privacidade ou sigilo do voto ocupa posição preponderante, com 13 menções. Em seguida, com 10 autores cada, encontram-se a incoercibilidade, tratada principalmente como a impossibilidade de emitir comprovantes que provem o voto do eleitor, e a verificabilidade. Esta última baseia-se principalmente na capacidade de o eleitor verificar se seu voto está registrado corretamente e pode ser estendida como verificabilidade universal, através da publicação de boletins que permitam a qualquer indivíduo conferir se a totalização está correta.

Os requisitos de integridade, elegibilidade, unicidade e equidade seguem com 7 menções dos autores. O primeiro visa à garantia de que nenhum voto seja alterado na cadeia de custódia do sistema eleitoral. O segundo determina que o sistema de votação deva garantir que o cadastro eleitoral esteja correto e assegure o direito ao voto a todos os eleitores registrados e se relaciona ao terceiro com o intuito de garantir que a cada eleitor seja permitido somente um voto. O último, normalmente registrado como *fairness*, determina que o sistema eleitoral não deve vazar informações que possam influenciar o eleitor a votar de forma diferente, por exemplo, indicando resultados parciais que possam induzir os indecisos a escolher alguém que já esteja com considerável número de votos, objetivando não "perdê-lo" na eleição.

A confiabilidade do sistema perpassa pela resistência a falhas de *hardware* e *software* e se estende à tolerância à coalizão de partes interessadas em fraudar uma eleição. Dos autores, cinco

consideraram-na digna de observação e, aliada às demais, está no cerne de qualquer sistema de votação que venha a ser proposto.

Os demais requisitos, embora menos referenciados, não são menos importantes e capturam, de certa forma, a perspicácia dos autores a elementos que geralmente não são considerados na construção de sistemas, especialmente os eleitorais (segurança de transmissão de dados, proteção contra ameaças externas ou até mesmo internas, endereçadas pelo controle de acesso), ou relacionam-se com os demais, como, por exemplo, a rastreabilidade com a verificabilidade individual.

Portanto, compor um sistema eleitoral implica em observar os requisitos e estabelecer os critérios para mensurar seu atendimento, traduzindo-os em requisitos funcionais. Por exemplo, a rastreabilidade e a verificação individual podem ser mapeadas no requisito de impressão do voto ou de um comprovante (que não viole a privacidade ou sigilo do voto) que possa ser usado pelo eleitor para garantir que seu voto foi corretamente contado.

Além dos requisitos de segurança, também podem ser elencados outros, referentes à usabilidade e ao custo:

Acessibilidade: qualquer eleitor em potencial deve ser capaz de votar, sem discriminação de qualquer capacidade e/ou restrição física, motora ou cognitiva (54).

Conveniência ao eleitor: os eleitores devem ter acesso conveniente ao processo eleitoral e devem ser aptos a votar em um tempo razoável (49, 104).

Flexibilidade: o sistema deve permitir uma ampla variedade de tipos de votos ou questões, i. e., diversos formatos de cédulas físicas ou eletrônicas, conforme o caso (49, 104).

Mobilidade: não devem existir restrições de locais em que o eleitor possa votar (49).

Simplicidade/Transparência: o processo de votação deve ser compreensível e fácil, de modo geral (54, 104).

Usabilidade: a cédula deve indicar claramente as opções a serem feitas, como selecioná-las e fácil o bastante para ser usada por todos. Incorpora o conceito "*cast as intended*", em que o eleitor pode registrar seu voto sem ser frustrado por procedimentos ou pela tecnologia (49, 54, 59).

Viabilidade custo/eficácia: a estrutura eleitoral deve ter custo razoável em equipamentos e acesso para permitir participação universal, sem que seus custos para aquisição ou operacionais inviabilizem sua adoção em locais com poucos recursos (49, 54, 104).

4.5 Segurança e Auditabilidade de Sistemas Eleitorais

Antes de discutir as soluções propostas ao contexto em que o problema de pesquisa se insere, é necessário definir alguns conceitos relacionados à segurança computacional e, por consequência, à auditabilidade. Na presente seção, serão apresentados os conceitos fundamentais de segurança computacional (Seção 4.5.1) e sua aplicação em sistemas eleitorais (Seção 4.5.2).

4.5.1 Fundamentos de Segurança Computacional

Segurança é, tradicionalmente, definida em função de três princípios básicos, de acordo com Albuquerque e Ribeiro (3):

Confidencialidade: capacidade de um sistema de permitir o acesso aos dados e/ou informações apenas a usuários autorizados, impedindo acesso indevido.

Integridade: atributo de uma informação que determina que esta não foi alterada de forma não autorizada e, por consequência, a capacidade de um sistema de impedir as alterações indevidas e detectar sua ocorrência.

Disponibilidade: relação entre a quantidade de solicitações de acesso a um recurso (dado, informação, sistema, etc.) atendidas sobre o número de vezes em que foi solicitado. Em outras palavras, é a capacidade de prover um dado ou um serviço sempre que um usuário necessitar, sem falhas internas.

Um sistema pode ser considerado seguro se estes três princípios forem atendidos. A ausência de um caracteriza um incidente ou falha de segurança. Além disso, outros aspectos podem ser observados, além dos três principais que foram previamente apresentados, de certa forma complementando-os ou cobrindo características que favoreçam sua aplicação. Albuquerque e Ribeiro (3) elencam:

Autenticação: capacidade de garantir que o solicitante de um acesso, seja usuário, sistema ou informação, seja realmente quem alega ser.

Não repúdio: capacidade do sistema de provar que um usuário executou determinada ação nele.

Legalidade: observância de normas e preceitos legais.

Privacidade: capacidade de manter incógnito um usuário, impossibilitando a associação entre agente e ação. É, portanto, totalmente distinto da confidencialidade, referindo-se normalmente ao sigilo, como, por exemplo, o sigilo do voto.

Auditoria: capacidade do sistema de auditar as ações realizadas pelos usuários, detectando fraudes ou tentativas de ataque. Normalmente, é necessário um *trade-off* entre privacidade e auditoria para que possam se conciliar de acordo com a necessidade do sistema.

Um dos aspectos importantes da auditoria é a gravação e a manutenção de uma trilha de ações realizadas no sistema, mediante análise ou visualização. Esta trilha de auditoria é composta pelos registros de tudo o que foi feito, para que, na detecção de qualquer problema, possa ser identificado o que ou quem o causou (3).

Segundo estes autores, trata-se de um conceito simples de implementar, mas extremamente complexo de se projetar em um sistema, pois passa prioritariamente pela definição dos tipos de eventos que devem ser registrados e quais de suas informações devem ser registradas. O excesso de registro leva a problemas de armazenamento, de lentidão e até mesmo de análise futura. A escassez de registros, por outro lado, pode deixar despercebida alguma ação que permita desvendar o problema. Soma-se ainda a questão da privacidade, sendo necessário definir o que será registrado e de que forma, caso necessário um compromisso entre auditoria e privacidade. O projeto de auditoria deve contemplar todas estas nuances para que registre os eventos realmente relevantes.

Tão importante quanto definir o que será registrado em trilha de auditoria é determinar quando esta trilha será analisada. Seu uso apenas quando houver suspeita de um incidente de segurança pode fazer com que eventos insuspeitos passem despercebidos. Uma política de segurança deve estabelecer não apenas o que registrar para auditoria, mas os atores, os eventos e a frequência com que deve acontecer, para que seja realmente efetiva.

Portanto, para a concepção de um sistema seguro, é necessário compreender o problema e a tecnologia que será utilizada. Em especial, as limitações da própria tecnologia podem se tornar fatores críticos para a segurança. Sem tal compreensão, a falsa sensação de segurança, causada pelo uso de criptografia e outros recursos tecnológicos, pode comprometer todo o projeto de segurança de um sistema. O projeto deve prospectar, da melhor forma possível, as ameaças e as limitações às quais a solução estará sujeita, visando a sua mitigação.

Outro conceito importante para o presente trabalho é a criptografia. É composta pelo conjunto de técnicas utilizadas para ocultar o conteúdo de uma mensagem de pessoas não autorizadas, através de processos matemáticos de transformação desta mensagem (dados, informação, etc.), usando uma chave de codificação.

A criptografia moderna divide-se em duas categorias: simétrica, em que a chave para codificar é a mesma utilizada para decodificar a mensagem; e assimétrica, na qual uma chave é usada para cifrar, e outra, correlata, para decifrar a mensagem. Dependendo do tipo de criptografia utilizado, outros recursos podem ser empregados, tais como assinatura digital (integridade e não repúdio), autenticação de mensagem (autenticidade), protocolos de comunicação de chaves, etc.

Conforme apresentado na Seção 5.2, as primitivas criptográficas dependem do tipo de *hardware* e bibliotecas utilizadas na implementação. Por este motivo e com o intuito de evitar uma enfadonha lista de protocolos criptográficos e suas respectivas descrições, dado o volume de criptossistemas disponíveis e suas diversas combinações, estes não serão detalhados neste

trabalho. O leitor poderá encontrar uma lista de referências que incluem os sistemas criptográficos e suas aplicações em sistemas eleitorais nos trabalhos referenciados na Seção 4.6. Havendo necessidade ao longo do texto, uma descrição em alto nível é apresentada.

4.5.2 Sistemas Eleitorais Auditáveis

O projeto de um sistema eleitoral auditável não se resume ao ato de votar. Abrange desde as fases iniciais do processo, definindo uma trilha de auditoria que possa ser validada por **qualquer** membro da comunidade. As listagens de eleitores e candidatos devem ser publicadas e verificáveis, com antecedência, visando impedir tanto a ausência de eleitores legítimos quanto a presença dos eleitores fantasmas.

Da mesma forma, todos os atos devem permitir a fiscalização por qualquer pessoa. Os boletins individuais de cada urna devem ser publicados, assim como os relatórios de totalização. Mas nenhum destes pode substituir o registro impresso do voto, conferido pelo eleitor, que permita sua recontagem.

Esta medida não conflita com a **privacidade** ou sigilo do voto. No ato da votação, apenas o eleitor poderá ver o voto antes que seja depositado em uma urna física, inviolável e completamente opaca. Segundo Maneschy e Jakobskind (71), a única forma válida de recontagem de voto, que garanta que a intenção original do eleitor seja preservada, é através do registro físico. As diretrizes de TGDC (107) excluem a possibilidade de adoção, para eleições americanas, de máquinas de votação que não tenham registro impresso do voto. A ausência de uma trilha física para auditoria, no caso, por meio de recontagem, não garante a preservação da intenção do eleitor, uma vez que uma urna eletrônica sempre mostrará a contagem que foi programada para fazer.

Além disso, as trilhas de auditoria registradas pelo sistema em meio eletrônico não devem incluir informações acerca do eleitor ou do voto registrado. É necessário um *trade-off* entre o nível de detalhamento dos registros e o sigilo do voto lançado pelo eleitor. No entanto, eventos importantes, que permitam auditar o correto funcionamento do sistema, devem ser registrados para futuras verificações.

Ainda acerca da **privacidade** do voto, não basta o uso de uma cabine indevassável para ocultar o eleitor durante o ato. O registro do voto eletrônico deve ocorrer de tal forma que a sequência de votação jamais seja reconstruída, permitindo que um observador, anotando a sequência de comparecimento dos eleitores, possa violar seu sigilo, abrindo possibilidade para técnicas de coerção (“voto de cabresto”).

Maneschy e Jakobskind (71) também acrescentam que a identificação do eleitor não pode ocorrer no mesmo *hardware* em que o voto é registrado, pois eventos podem ser cruzados e realizar a associação entre eleitor e voto. Em Brunazo Filho e Cortiz (31), destaca-se que a identificação do eleitor no mesmo equipamento permite a coerção, pois ainda que não haja

acesso aos dados para a quebra do sigilo, o eleitor é levado a crer que seja possível, pois seu título eleitoral é digitado na mesma máquina, segundos antes de registrar seu voto.

Desta forma, a segurança de qualquer processo eleitoral informatizado depende de dois fatores: da independência de *software* e do poder de fiscalização da sociedade. O primeiro pode ser assegurado pelo registro impresso do voto, que deixa de ser um dado imaterial, pela publicação das trilhas de auditoria, relatórios, etc. (31, 71, 107, 115). Por independência de *software*, adota-se a definição de Rivest (91), que um sistema de votação é independente de *software* se uma mudança ou erro (não detectados) em seu *software* não possam causar uma mudança ou erro indetectáveis no resultado da eleição.

Rivest (91) afirma, ainda, que o intuito da definição de independência de *software* é capturar a noção que um sistema de votação é inaceitável se um erro de *software* puder causar uma mudança no resultado da eleição, sem nenhuma evidência disponível que algo deu errado. Para o autor, um sistema independente de *software* não poderia, de forma imperceptível, adulterar o resultado final devido ao *software*.

O segundo fator depende exclusivamente da conscientização e educação da comunidade, para que exerça o seu direito de fiscalizar e lutar pela transparência e licitude dos processos, por meio de engajamento ativo. Entretanto, para que possa ser assegurado, o sistema não deve exigir nenhum conhecimento específico para sua interpretação e compreensão, caso contrário, torna-se totalmente inócuo.

4.6 Resultados da Revisão Sistemática de Literatura

Conforme apresentado no Capítulo 2, foi estabelecido um protocolo de revisão sistemática de literatura (RSL) com o propósito de determinar tendências em sistemas de votação eletrônica. A análise, conforme apresentado pelo protocolo (Seção 2.1), restringiu-se a sistemas eletrônicos de votação que utilizem ambientes supervisionados, nos moldes das conhecidas seções eleitorais brasileiras. Utilizando a *string* de busca escolhida, nas bases de dados selecionadas, foram obtidos os quantitativos apresentados na Tabela 4, com acesso ao texto completo. Antes de aplicar os critérios de inclusão e exclusão, foram removidas as duplicatas encontradas, restando um total de 144 artigos.

Nestes 144 textos, foram aplicados os critérios de inclusão e exclusão em etapas sucessivas. Em um último estágio, foram lidos os textos completos dos trabalhos excluídos, em busca de remoção indevida de textos nas etapas iniciais, com apenas uma reinclusão. Foram selecionados, de forma definitiva para a RSL, **24** títulos diferentes, entre publicações em conferências e revistas acadêmicas, conforme distribuição exibida na Tabela 5. O gráfico da Figura 8 mostra a distribuição das publicações por ano. Observa-se que os períodos 2004–2007 e 2009–2010 possuem o mesmo quantitativo de publicações, embora o segundo tenha uma maior produtividade, sob a

perspectiva do número médio de trabalhos/ano. Dentre os textos selecionados, os anos 2008 e 2011 não tiveram nenhuma contribuição.

Tabela 4 – Total de artigos obtidos nas bases de dados buscadas

Base	**Nº de Artigos**
ACM Digital Library	71
EBSCO Host	5
Emerald Insight	1
Portal de Periódicos da CAPES	11
Science Direct	34
Scopus	42
Subtotal	164
Duplicados	20
Total	144

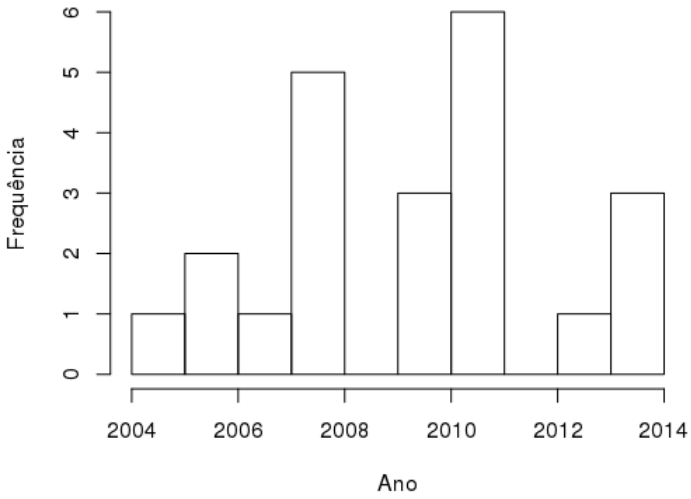
Fonte: dados da pesquisa.

Tabela 5 – Distribuição das publicações quanto ao meio

Meio de Publicação	**Quantidade**
Conferências	15
Revistas	9
Total	24

Fonte: dados da pesquisa.

Figura 8 – Distribuição das publicações no período 2004–2014



Fonte: dados da pesquisa.

As Tabelas 6 e 7 foram baseadas no *framework* proposto por Jardí-Cedó *et al.* (60), com algumas simplificações. Além dos requisitos já apresentados na Seção 4.4, os autores

estabelecem a **integridade da *ballot box*** (urna) como a consequência dos requisitos de elegibilidade, unicidade e integridade dos votos. Para todas as análises, foram consideradas apenas as informações presentes nos próprios textos.

Em relação à taxonomia dos sistemas avaliados (Seção 4.1), 8 correspondem a sistemas ópticos (PCOS), 9 do tipo DRE (um opcionalmente incluindo VVPAT) e 5 propostas do tipo VVPAT. Dos sistemas DRE, apenas um registra o valor do voto em cartão RFID como meio de armazenamento. A Tabela 6 relaciona os sistemas encontrados e algumas das propriedades de segurança. Quando o sistema não recebeu uma designação pelos autores, foram utilizadas, neste texto, as primeiras letras dos sobrenomes dos autores do trabalho, seguidas por um apóstrofo e o ano da publicação (e. g., *SJSW'2009*), exceto nos casos em que o trabalho teve um único autor, sendo utilizado seu sobrenome completo (como *Chaum'2004*, por exemplo). A análise considerou apenas a presença, mesmo que parcial, das propriedades analisadas, sem quantificá-las.

A Tabela 7 apresenta os mecanismos de segurança detectados nos trabalhos analisados. Conforme relatado, trata-se também de uma simplificação do *framework* de Jardí-Cedó *et al.* (60). Foram considerados os seguintes mecanismos:

Técnicas criptográficas: técnicas usadas com o objetivo de sigilo por meio de criptografia dos votos, tais como cifras e *commitments*.

Técnicas de anonimato: mecanismos usados com o objetivo de desfazer o vínculo entre eleitor e voto registrado, tais como redes de mistura (*mix-nets*) ou assinaturas cegas (*blind signature*), propiciadas pelos métodos criptográficos utilizados.

***Threshold Scheme*:** emprego de técnica de compartilhamento de segredo entre n entidades, das quais k devem se associar para recuperá-lo, como, por exemplo, a chave privada necessária para decriptografia dos votos.

Comprovantes: identifica se o sistema analisado emite recibos para que o eleitor possa comprovar o voto, se foi corretamente lançado e/ou apurado, por exemplo, pela publicação em um *bulletin board*, sem, contudo, revelar seu valor.

***Bulletin Board*:** identifica se o sistema utiliza um boletim público em que os dados são publicados (como os comprovantes de votação) para pública conferência.

***Zero-Knowledge Proof* (ZKP):** identifica se são usados mecanismos de prova de que uma informação permanece inalterada, sem torná-la pública.

Assinaturas digitais: técnica utilizada para garantir a autenticidade, integridade e não repúdio de uma informação, na qual um *hash* dos dados é assinado com uma chave privada de uma entidade e qualquer indivíduo pode verificá-la usando a chave pública correspondente.

Tabela 6 – Propriedades de segurança dos sistemas eleitorais analisados

Sistema	Tipo	Ano	Segurança								Referências
			Relacionada ao Eleitor				Relacionada à Votação				
							Verificabilidade Universal			Auditabi-lidade	
			Privacidade	Sem Comprovantes	Resistência à Coerção	Verificabilidade Individual	Integridade da *Ballot Box*	Acurácia da Apuração	Equidade		
Chaum'2004	VVPAT	2004	S	S	S	S	S	N.D.	N.D.	S	(36)
Prêt à Voter	PCOS	2005	S	S	N	S	S	S	S	S	(38, 92, 94)
Ryan'2005	VVPAT	2005	S	S	N	S	S	S	S	S	(93)
Scratch & Vote	PCOS	2006	S	S	N	S	S	S	S	S	(2)
GR'2007	DRE	2007	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	S	(51)
LCKLEA'2007	DRE†	2007	S	S	N.D.	S	S	S	N.D.	N.D.	(70)
Prime III	DRE‡	2007	S	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(42)
ProVotE	VVPAT	2007	S	S	N.D.	S	S	N.D.	N.D.	S	(108)
ZK'2007	DRE	2007	S	S	S	S	S	S	S	N.D.	(116)
CG'2009	VVPAT	2009	S	S	S	S	S	S	S	N.D.	(35)
DVVSBS	DRE	2009	S	S	N.D.	S	S	N.D.	N.D.	N.D.	(19)
SJSW'2009	DRE	2009	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(105)
ClearVote	PCOS	2010	S	S	N	S	S	S	S	S	(87)
LPMKW'2010	VVPAT	2010	S	S	S	S	S	S	S	S	(68)
Scantegrity II	PCOS	2010	S	S	S	S	S	S	S	S	(34)
Split-Ballot	PCOS	2010	S	S	S	S	S	S	S	S	(74)
T-DRE	DRE	2010	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(50)
Voter-Verifiable Farnel	DRE	2010	S	S	S	S	S	S	N.D.	S	(9)
Hover	PCOS	2012	S	S	S	S	N.D.	N.D.	N.D.	S	(46)
*Audiotegrity**	PCOS	2013	S	S	S	S	S	S	S	S	(63)
EasyVote	PCOS	2014	S	S	N.D.	S	N	N	N.D.	N.D.	(33)
SES	DRE	2014	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(95)

† armazenamento em cartões RFID ‡ Opc. VVPAT * Considerado o *back-end Scantegrity II*

S: Sim, N: Não, N.D.: Não disponível no texto, Opc.: Opcional

Fonte: dados da pesquisa, inspirado em Jardí-Cedó *et al.* (60).

Tabela 7 – Mecanismos de segurança dos sistemas analisados

Sistema	Técnicas de Segurança							Referências
	Técnicas Criptográficas	**Técnicas de Anonimato**	***Threshold scheme***	**Comprovantes**	***Bulletin Board***	**ZKP**	**Assinaturas Digitais**	
ZK'2007	Merkle's *puzzles*, cifra simétrica, *hash*	*Mix-net*	S	S	S	S	S	(116)
Prêt à Voter	ElGamal / Paillier / RSA	Mix-net	S	S	S	S	S	(38, 92, 94)
LPMKW'2010	ElGamal	*Mix-net*	S	S	S	N.D.	N.D.	(68)
ClearVote	ElGamal	*Mix-net*	N	S	S	N.D.	S	(87)
SES	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(95)
LCKLEA'2007	ElGamal	*Mix-net*	S	N	S	S	S	(70)
T-DRE	RSA, AES	N.D.	N.D.	N	N.D.	N.D.	S	(50)
Scratch & Vote	Paillier	*Homomorphic counter*	S	S	S	S	S	(2)
Voter-Verifiable Farnel	ElGamal	*Mix-net*	S	S	S	N.D.	S	(9)
DVVSBS	RSA	*Blind signature*	N.D.	Opc.	N.D.	N.D.	S	(19)
EasyVote	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(33)
Scantegrity II	*Commitments*	*Mix-net*	S	S	S	N.D.	S	(34)
CG'2009	ElGamal	*Mix-net*	S	S	S	N.D.	S	(35)
Chaum'2004	Visual	*Mix-net*	N.D.	S	S	N.D.	S	(36)
Prime III	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(42)
Hover	*Hash*, Visual	*Mix-net*	N.D.	S	S	N	N.D.	(46)
GR'2007	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(51)
Audiotegrity	*Commitments*	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(63)
SJSW'2009	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	(105)
Ryan'2005	N.D.	*Mix-net*	N.D.	S	S	N.D.	Opc.	(93)
ProVotE	N.D.	N.D.	N.D.	N.D.	N.D.	N.D.	S	(108)
Split-Ballot	Paillier	*Mix-net*	Opc.	S	S	S	N.D.	(74)

S: Sim, N: Não, N.D.: Não disponível no texto, Opc.: Opcional

Fonte: dados da pesquisa, inspirado em Jardí-Cedó *et al.* (60).

Na sequência, serão analisados os sistemas obtidos na RSL. Não se intenta fazer uma descrição detalhada do funcionamento deles, mas estabelecer uma visão geral que permita compreender uma linha evolutiva nas propostas. Para mais detalhes, recomenda-se a leitura dos trabalhos originais, além de uma ampla gama de estudos que foram excluídos da RSL por não atenderem aos critérios de inclusão e exclusão, os quais descrevem os sistemas mais conhecidos. Deve-se destacar que não fez parte da presente RSL uma análise bibliométrica das citações dos trabalhos.

O sistema que foi denominado neste texto (conforme método exposto na pág. 68 e na Tabela 6) como *Chaum'2004*, proposto por Chaum (36), é um dos precursores da votação com verificabilidade fim a fim (E2E), no qual o eleitor é empoderado com a capacidade de verificar se o seu voto foi corretamente registrado e tabulado. Considerando a dificuldade humana em executar cálculos complexos para fins criptográficos, lança mão da criptografia visual: o voto é impresso em duas folhas transparentes que, quando sobrepostas, revelam o voto original do eleitor. O conteúdo de cada folha é similar, em uma análise superficial, a um conjunto de *pixels* aleatoriamente dispersos pela folha, praticamente indistinguíveis de mero ruído. Uma chave usada pelo sistema gera as imagens. Ao terminar de votar, o eleitor destrói uma das páginas e retém a outra como comprovante do seu voto, utilizando-o para verificar, em um boletim, se seu voto foi contabilizado, podendo apresentar reclamação caso não o encontre. Sem a página complementar, o eleitor não é capaz de comprovar a terceiros qual o valor de seu voto e, portanto, pode resistir à coerção.

O autor utiliza redes de mistura (*mix-nets*) para prover o anonimato dos votos. Propõe como analogia as bonecas russas aninhadas, ou seja, que são guardadas dentro do vão central de bonecas sucessivamente maiores. Cada misturador retira a boneca mais externa e passa ao seguinte o seu conteúdo, até que se obtenha o voto do eleitor, decriptografado. A chave de decifragem do voto é compartilhada entre várias entidades, usando um esquema de limiar (*threshold*) para reconstruí-la na apuração.

O sistema *Ryan'2005* estende a proposta original de *Chaum'2004*, substituindo a criptografia visual por uma cédula com o centro picotado, que permite a separação em duas metades (93). A da esquerda contém a lista de candidatos, e a da direita, o espaço para o eleitor assinalar um "X" em sua opção. A cédula é emitida por um sistema eletrônico, no qual o eleitor autentica-se e é gerado um número serial q, usado para produzir um deslocamento aleatório da lista canônica de candidatos (i. e., rotação cíclica). O eleitor vota, sendo impressa a cédula com a lista de candidatos e a marcação correspondente a sua opção, com informações adicionais, como o parâmetro q e os valores $Doll_L$ e $Doll_R$, que codificam as permutações das duas metades, em um esquema de mistura semelhante a *Chaum'2004*. O eleitor, enfim, seleciona qual delas reterá como recibo, e a impressora adiciona a informação, em cada parte, de qual será retida (e o valor da sua semente criptográfica) ou destruída, de acordo com a seleção. A metade selecionada para descarte é entregue aos mesários, que a destroem na presença do eleitor, que retém a outra

metade como comprovante para verificação da apuração. O processo de apuração segue o modelo de *Chaum'2005*, usando redes de mistura e a abertura das bonecas russas (*dolls*).

Com as informações no recibo, não é possível restabelecer a votação original do eleitor, dificultando, mas não eliminando as ações coercitivas. Ele não é capaz de provar em quem votou, mas pode ser forçado a selecionar sempre a primeira opção, tornando-o vulnerável a um ataque de aleatorização, no qual os votos seriam distribuídos fortuitamente aos candidatos que ocupem esta posição na cédula. Este ataque pode ser eficaz em cenários nos quais a disputa esteja acirrada, com intenções de votos muito próximas, levando a uma pequena margem de diferença, cuja aleatorização poderia beneficiar um dos candidatos.

O sistema *Prêt a Voter* foi proposto originalmente em 2005, em Chaum; Ryan e Schneider (38), descrito em Ryan *et al.* (94) e expandido em Ryan (92), para uso de cifra de Paillier no lugar de ElGamal. Surgiu como uma alternativa ao modelo original (*Chaum'2004*), que demandava a impressão de duas páginas transparentes superponíveis para criptografia visual. Na proposta de *Prêt a Voter*, esta última é substituída pela impressão de uma cédula similar às usadas no voto em papel, com os nomes dos candidatos à esquerda e espaço para marcação do voto à direita destes, como proposto para o sistema *Ryan'2005*. No centro, uma linha picotada permite que as duas metades sejam separadas, sendo a da direita lida por um *scanner* (sistema PCOS) e retida pelo eleitor como um comprovante, para futura verificação. A metade esquerda é destruída e, sem ela, o eleitor não pode demonstrar a associação entre a posição assinalada em seu comprovante e a permutação dos nomes dos candidatos (geralmente na forma de deslocamentos cíclicos). O *scanner* registra a posição em que o eleitor assinalou o "X" e o valor de *onion* (lit. uma referência às camadas de uma cebola ou, como no sistema anterior, às bonecas russas). Este valor, junto com o índice da marcação, é passado por uma rede de mistura que remove as camadas criptográficas e, ao final, é capaz de reconstruir o deslocamento da metade esquerda que foi destruída, e permitindo contabilizar o voto corretamente.

O eleitor pode usar o comprovante para verificar se a posição da marca e o valor de *onion* foram corretamente incluídos no boletim público, certificando-se da correta apuração de seu voto. Embora não seja possível comprovar a relação entre as duas metades, caso seja garantida a destruição da metade contendo os nomes, o sistema não é resistente a formas de coerção, como ataques de aleatorização, votação em cadeia ou ataque italiano, dentre outros descritos em Ryan *et al.* (94).

O sistema *Scratch & Vote* foi proposto em 2006 (2), com o objetivo de minimizar custo e complexidade para implementação. Utiliza uma cédula impressa, com as mesmas características básicas dos outros sistemas: disposição em duas colunas, com os candidatos à esquerda e o espaço para o eleitor assinalar sua opção à direita. As colunas são separáveis por uma linha picotada, e o eleitor descarta a metade esquerda após registrar seu voto. À direita, há um código de barras 2D, que armazena os valores dos parâmetros públicos da eleição, permitindo verificar se a cédula está formatada conforme o protocolo. Abaixo deste código, há uma região coberta

com tinta raspável, sob a qual encontram-se os valores aleatórios usados para produzir os valores cifrados do código de barras. O eleitor pode auditar cédulas aleatoriamente, raspando a superfície e usando o código visível para conferir se a ordem da aleatorização da lista canônica está em conformidade com os valores impressos na cédula.

Ao registrar seu voto, o eleitor entrega a metade direita ao mesário, que deve inspecionar se a área encoberta por tinta não está danificada, violando o sigilo da cédula. Esta área raspável também possui uma linha picotada, usada pelo mesário para removê-la da cédula e descartá-la, na presença do eleitor. Este, por fim, recebe de volta o restante, que, a partir desse momento, contém somente sua marcação e o código de barras, passa-o por um *scanner* para registrar seu voto e retém a cédula como um comprovante. Depois da apuração, o eleitor poderá usá-lo para verificar se seu voto foi incluído na apuração, em um boletim público.

Em uma abordagem diferente, o sistema *GR'2007* (51) propõe independência de *software* e auditabilidade sem utilização de cédulas impressas. Com o objetivo de reduzir os riscos de segurança em sistemas DRE que possam ter o *software* comprometido, utiliza uma abordagem de virtualização para estes sistemas. Nessa proposta, o sistema operacional hospedeiro implementa um protocolo de reconhecimento e captura das telas do sistema de votação, em execução no sistema hóspede, executado em uma máquina virtual. Por reconhecimento de padrões, registra-se no hospedeiro a intenção do eleitor, de acordo com o que ele visualiza na tela do sistema. Esse registro constitui trilha de auditoria, que permite, segundo os autores, detectar um mau comportamento do sistema e resgatar a verdadeira intenção do eleitor. Os autores, entretanto, destacam que não endereçaram os ataques direcionados ao sistema hospedeiro. Também não registram detalhes a respeito do formato em que a trilha de auditoria é armazenada, com o intuito de evitar ou detectar qualquer adulteração nela, que venha a interferir no resultado.

LCKLEA'2007 (70) também é um sistema eleitoral baseado em DRE, utilizando uma abordagem diferente, uma vez que o voto não é registrado em uma base de dados no mesmo dispositivo usado para votar, e sim em uma *tag* RFID (*Radio-Frequency Identification* — Identificação por Radiofrequência). O eleitor recebe essa *tag* após definir sua elegibilidade e se dirige à cabine de votação, na qual encontram-se dois dispositivos independentes: um para votar e outro para verificar. Ao inserir a *tag* no verificador, ele certifica-se de que ela não foi utilizada e dirige-se ao terminal de votação, registrando seu voto, que será gravado nela, após confirmação do eleitor. O identificador desta é inserido em uma base de dados para impedir seu reuso e o terminal de votação é desativado, para que o eleitor não insira alguma outra *tag*. O terminal verificador pode ser usado pelo eleitor tantas vezes quantas desejar, para certificar-se de que o voto criptografado nela corresponde a sua intenção, depositando-a em uma urna lacrada até o momento da apuração, que será realizada lendo todas as *tags* e decritografando os valores dos votos.

Prime III (42) é um sistema eleitoral focado na usabilidade, com o usuário no centro do processo. Constitui-se por um dispositivo DRE, opcionalmente equipado com VVPAT, no qual

o usuário pode interagir pela tela sensível ao toque, por síntese e por reconhecimento de voz. Pode, ainda, usar qualquer combinação dessas modalidades simultaneamente. Trata-se de um sistema preliminar, que teve como objetivo avaliar a usabilidade por diversos perfis de usuário e, portanto, não detalha nenhuma característica de segurança. Embora estes detalhes não estejam presentes, é uma abordagem promissora, considerando-se que a acessibilidade do sistema como um todo deve permear o processo, permitindo a qualquer eleitor exercer seu direito ao voto.

O sistema *ProVotE* (108) é uma iniciativa italiana, com o objetivo de desenvolver um sistema de votação eletrônico para a província de Trento, na Itália. Os autores deram maior ênfase ao projeto do sistema e à ferramenta desenvolvida para auxiliar neste processo, que converte diagramas de estados da UML (*Universal Modelling Language*) para código Java. Trata-se de um sistema VVPAT que executa a aplicação Java (*jprovote*) em ambiente Linux. O foco do projeto recai sobre a geração de código e a validação do modelo na forma de máquina de estados, constituindo-se, na prática, como uma prova de conceito, experimentada em quatro eleições locais e de representantes de escola de ensino médio local. Segundo os autores, mais de 11.000 cidadãos utilizaram o sistema e não foram encontradas falhas.

Em *ZK'2007* (116), encontra-se um sistema eleitoral DRE, segundo os autores, bastante flexível para permitir diversos tipos de usos, desde votos empregando sistemas semimecânicos a votação puramente eletrônica. Utiliza enigmas de Merkle (*Merkle's puzzles*) para prover um sistema de autenticação anônima, mesmo que as conexões à *internet* sejam associadas, de alguma forma, ao usuário. O eleitor envia o voto com suas credenciais a um contador, que soma-o e publica uma prova anexada a ele, sem necessidade de realizar cálculos criptográficos complexos.

Retornando ao modelo *Chaum'2004*, o sistema *CG'2009* (35) volta a aplicar criptografia visual impressa em duas folhas superpostas. A contribuição do sistema consiste na adaptação das camadas criptografadas para submissão a um sistema de mistura centrado no usuário. O eleitor se empodera com a capacidade de definir rodadas extras do protocolo, se desejar um nível maior de anonimato. Caso sejam encontrados misturadores defeituosos, estes podem ser compensados aumentando-se as rodadas de mistura.

O sistema DVVSBS (*Distributed Voter-Verifiable Secret Ballot System*), apresentado em Biagioni *et al.* (19), utiliza um ambiente distribuído para autenticação do eleitor e apuração dos resultados. Pode ser usado para votação puramente remota, mas permite a adoção em ambiente supervisionado (cabine eleitoral), no qual um cliente de eleitor (*VC — voter client*) é empregado para gerar a cédula com as opções do eleitor. O *VC* envia a credencial secreta do eleitor e uma versão ofuscada da cédula, por um fator $k < n$, ao servidor de assinatura de cédulas (*BAS — ballot authentication server*), que assina digitalmente esta última, caso o eleitor seja elegível e não tenha votado ainda. A assinatura cega (*blind signature*) é devolvida ao eleitor, que remove o ofuscamento, recuperando o valor original da cédula, assinada digitalmente por *BAS*, enviando-a ao servidor de apuração (*VTS — vote tally server*), que procederá com a totalização dos votos com assinatura válida. O uso de múltiplos servidores aumenta a disponibilidade

e segurança do sistema, segundo os autores. O *VC* pode ser um computador com o sistema executado a partir do *boot* em um CD seguro, provido pela autoridade eleitoral.

SJSW'2009 é mais um sistema DRE, proposto em Sturton *et al.* (105), baseado em máquinas de estados finitos. Seu *design* visa habilitar verificação e teste. Foi implementado em Verilog como prova de conceito, com funcionalidades mínimas, demonstrando a validação formal da proposta.

ClearVote (87) é um sistema PCOS que provê o sigilo do voto por meio da impressão das cédulas em três camadas transparentes. Cada camada é produzida por uma impressora diferente, de tal forma que o sigilo do voto somente é quebrado caso haja colusão entre as autoridades responsáveis por elas. Em uma camada, são impressos os nomes dos candidatos em uma coluna à esquerda. Outra camada associa a estes, na coluna à direita, um conjunto de letras aleatórias, que indicarão qual posição deve ser assinalada, com os espaços circulares com as letras em uma ordem diferente na terceira camada. O voto é registrado apenas na primeira delas, com o nome dos candidatos, que o eleitor levará a um PCOS para digitalização e a guardará como recibo. As camadas inferiores serão destruídas, impedindo ao eleitor a comprovação a terceiros de sua intenção de voto. Assim como os sistemas PCOS previamente apresentados, o sistema não é imune a ataques de aleatorização por um agente coercitivo.

Lee *et al.* (68) propõem o sistema que foi denominado, neste trabalho, *LPMKW'2010*. Baseia-se no sistema *Chaum'2004*, mas substitui a criptografia visual por um conjunto de valores criptografados usando o algoritmo ElGamal (cifra assimétrica que apresenta propriedades homomórficas) e números aleatórios. Cada candidato c_i recebe um número (i), que será criptografado por dois valores aleatórios como chave: w_i' e w_i''. Estes valores são mostrados na tela do sistema em uma tabela, com cada candidato em uma linha. O eleitor, aleatoriamente, escolhe um valor cifrado de cada candidato, os quais serão mantidos para votação, e os restantes serão abertos e impressos, lado a lado, com o valor da chave usada para criptografar. O eleitor verifica se os valores impressos correspondem aos mostrados na tela e seleciona seu voto, dentre aqueles que não tiveram a chave impressa. Após confirmá-lo, o valor correspondente à criptografia do número do candidato e a chave que permaneceu oculta são impressos. O eleitor poderá utilizar essa impressão para verificar se os valores estão corretamente cifrados (usando qualquer implementação de ElGamal disponível) e conferir se o voto cifrado no final do comprovante encontra-se no boletim público.

Um dos raros relatos de sistemas utilizados efetivamente em eleições é encontrado em Carback *et al.* (34), descrevendo o *Scantegrity II*. Este sistema foi utilizado em novembro de 2009 para as eleições municipais de Tahoma Park, no estado de Maryland, EUA. Os eleitores marcam as cédulas com caneta, preenchendo o espaço oval que corresponde ao candidato de sua escolha. A caneta utilizada reage com a tinta invisível presente no espaço, exibindo um código numérico de confirmação, que pode ser anotado pelo eleitor, junto com o número de série da cédula, e verificado posteriormente em um boletim público. Cada código de confirmação é

gerado aleatoriamente para cada cargo e cédula, não revelando o voto correspondente. Como outros sistemas PCOS, a cédula é digitalizada e depositada para contagem manual posterior, conforme descrito pelos autores.

O sistema *Split-Ballot* (74) é um precursor do *ClearVote*. A primeira proposta, em 2007 (73), não foi incluída na RSL em função do critério de exclusão, por ser duplicata publicada em conferência, sendo considerada apenas a versão mais recente, publicada em periódico. Utiliza cédulas sobrepostas, com áreas vazadas para dar visibilidade ao conteúdo da cédula posicionada abaixo. A última cédula possui várias colunas com um caracter representando arbitrariamente um candidato, de conhecimento do eleitor, cada uma com ordenação distinta das demais. A área vazada seleciona uma das colunas, que fica visível para o eleitor selecionar a área de marcação correspondente, que fica na terceira e última camada. Esta será digitalizada após a destruição das duas camadas superiores, sendo entregue ao eleitor como comprovante de sua votação, para conferência posterior.

Uma característica do sistema *Split-Ballot* é que o eleitor recebe dois conjuntos de cédulas das camadas superiores. Um deles será escolhido por ele para auditar, confirmando, através do código de verificação, se a cédula corresponde a sua representação lógica. O eleitor poderá guardar esse conjunto completo para auditoria posterior. Após fazer esta averiguação, ele recebe a camada inferior, em que o voto será registrado em cabine individual. A responsabilidade da impressão pode ser dividida entre duas autoridades, cada uma com uma das camadas que compõem o sistema.

O sistema eleitoral *T-DRE* (50), previamente apresentado na Seção 4.3, é uma proposta de mecanismos para execução de *software* assinado digitalmente, que passou a fazer parte da urna eletrônica brasileira a partir do modelo 2010. Conforme já discutido, a proposta contempla uma abordagem para garantir que apenas o *software* autorizado seja apto a executar no dispositivo, evitando agentes maliciosos de terceiros. Por outro lado, poucas informações são dadas em relação aos mecanismos de segurança do voto. Um efeito colateral da abordagem é que toda a confiança passa a ser depositada no desenvolvimento do sistema pelo TSE, gerando um único ponto de falha cujas consequências podem afetar toda a eleição. Trata-se, portanto, de um sistema efetivamente utilizado em eleições brasileiras.

A proposta do sistema *Voter-Verifiable Farnel* (9) é uma extensão do sistema de votação conhecido por Farnel, proposto em 2001, permitindo a verificabilidade do eleitor e uma implementação eletrônica. Neste trabalho, apenas esta última será apresentada. Após a identificação e elegibilidade do eleitor, este inicia o processo de votação em uma cabine contendo um dispositivo DRE, que gera os dois *commitments* de cada opção, impressos na cédula, ainda oculta ao eleitor. Ele seleciona quais deles serão abertos para confirmação, sendo impressos no comprovante. Em seguida, registra sua opção de voto, imprimindo o *commitment* correspondente, que não foi aberto. Neste estágio, a cédula é exibida ao eleitor, que procederá com a verificação visual das informações quanto à conformidade em relação às seleções prévias. Se estiver satisfeito,

confirmará seu voto e os *commitments* não abertos serão apagados com uma tarja impressa sobre seus valores. O dispositivo também imprime um código de barras que representa o voto do eleitor e adiciona uma assinatura digital ao comprovante, que será retido por ele, enquanto os demais dados são enviados para o boletim público.

Em seguida, o eleitor utiliza um leitor de código de barras para adicionar seu voto a uma urna especial (farnel), que o adiciona à sua lista privada de votos, seleciona um elemento aleatório desta lista, contendo algum voto, decriptografa-o e o adiciona à impressão, no final do comprovante. Este, portanto, passa a conter a lista de *commitments* cifrados, seguidos pelo respectivo valor em texto claro, para verificação da formação correta da cédula. Em seguida, contém o voto cifrado do eleitor e os valores decifrados de algum voto aleatório, para que sejam verificados no boletim público após as eleições. Assim, o eleitor tem a garantia da formação adequada do voto, da sua presença no boletim e que a sua decriptografia está correta, conferindo um voto de terceiro, como na proposta original do sistema. Para que os primeiros eleitores possam ter maior probabilidade de ter o voto adicionado ao comprovante que não seja o seu próprio, na etapa inicial são adicionados votos aos candidatos à urna especial, que são descontados após a apuração e publicados no boletim.

O sistema *Hover* (46) emprega uma proposta de um sistema eleitoral extremamente simples e com o uso mínimo de criptografia. Baseia-se no emprego de *hash* para realizar os *commitments* verificáveis pelo usuário sem conhecimento de técnicas criptográficas. A cédula é composta pela lista de candidatos e uma sequência de caracteres permutados entre si, ao lado do espaço reservado para preenchimento pelo usuário. Ao fazer sua marcação, o eleitor produz um recibo com o número de série da cédula e a cópia do caracter de confirmação presente ao lado da opção escolhida. Após a eleição, o eleitor interessado em auditar poderá copiar uma planilha com os dados da eleição, o algoritmo de *hash* usado, recalculá-lo e verificar a validade dos dados em uma planilha eletrônica.

A proposta do *Audiotegriy* (63) é construída sobre o *Scantegrity II* e aplicada com o mesmo propósito, nas eleições municipais de Tahoma Park, em 2011. Com o intuito de endereçar alguns problemas de resolução de disputas entre usuário e sistema de votação, de coerção e da acessibilidade dos sistemas eleitorais, propõe um *front-end* que auxilia o preenchimento das cédulas do *Scantegrity II*, utilizado como *back-end*. Após a autenticação do eleitor, este dirige-se a uma cabine com o dispositivo, protegendo a sua privacidade enquanto vota. Uma impressora e o *scanner* para digitalização do voto são posicionados fora da cabine, em público. O sistema do *Audiotegrity* provê uma saída em áudio e vídeo para o eleitor, que pode fazer suas escolhas usando um teclado e microfone. Após a votação, o sistema imprime uma cédula bastante similar à do *Scantegrity II*, com o intuito de impedir uma discriminação das cédulas a distância ou em um exame superficial, junto com um cartão de confirmação, que corresponde à cópia do código de verificação anotado pelo eleitor ao usar o *Scantegrity II*. As impressões são realizadas com a face impressa para baixo, e ele, ao sair da cabine, declara publicamente se deseja auditar ou lançar o

voto, antes de manusear o material. Esta declaração aberta visa estabelecer um canal público e auditável, pelas testemunhas, da opção do eleitor. Se declarar o propósito de auditar, o eleitor leva as cópias para casa, com o intuito de conferir sua conformidade. Caso contrário, a cédula será digitalizada conforme o protocolo do *Scantegrity II*, e ele leva o cartão de confirmação como comprovante e mecanismo de auditoria.

O penúltimo sistema analisado é o *EasyVote* (33), cujo protótipo foi utilizado nas eleições universitárias da Technische Universtität Darmstadt, em junho de 2013. Constitui-se de um computador que contém apenas memória volátil, com o sistema em um CD-ROM e sem armazenamento secundário e unidades de rede. Um dispositivo de habilitação conecta-se ao equipamento, com um único botão que o habilita para o uso de um novo eleitor. Este último interage com o sistema, gerando uma cópia impressa do voto em formato legível por humanos e um código de barras 2D, para leitura automatizada. Após conferi-lo, o eleitor dobra-o e o deposita em uma urna lacrada, até o início da apuração. Esta se dá com a abertura da urna e, com um leitor de código de barras, a informação registrada é comparada com o registro legível por humanos em um monitor, enquanto, em um segundo monitor, o voto é adicionado em um resultado intermediário.

Por fim, o sistema *SES* (*Smart E-Voting System*), proposto por Saad; Roseli e Zullkeply (95), para substituir a votação em papel usada na Universiti Kuala Lumpur (Malásia). Trata-se de um sistema de votação executado em um PC, habilitado pelo cartão RFID de cada estudante para um voto. O equipamento de votação está ligado ao sistema de administração eleitoral (*SES Manager*), que se encarrega do gerenciamento dos eleitores, e a um servidor de banco de dados, usando VLAN (*Virtual Local Area Network* — Rede Local Virtual). Os autores não disponibilizam nenhum detalhe dos mecanismos de segurança da solução além da autenticação do usuário, não provendo meios de avaliar o nível de proteção ao sigilo do voto e as demais características desejáveis em um sistema eleitoral.

Analisados os trabalhos, pôde-se determinar que eles apresentam uma tendência em relação ao uso de criptografia homomórfica para emissão dos comprovantes de votação, com verificabilidade fim a fim pelo eleitor. Para garantir o anonimato e sigilo dos votos, redes de mistura são bastante utilizadas, presentes em metade dos sistemas examinados.

Dentre os mecanismos de votação, sobressaem-se, ainda, os dispositivos DRE. Entretanto, esta também é a categoria com o menor número de informações quanto aos critérios de segurança observados. Embora o ápice desses sistemas seja observado em 2007, apenas um exemplar foi proposto na década atual.

Os sistemas PCOS são encontrados em maior número em relação aos VVPAT. Esta tendência justifica-se pela similaridade das cédulas usadas nesses sistemas em relação aos mecanismos de votação baseados em papel adotados nos EUA, como cartões perfurados ou com preenchimento para digitalização. Considerando-se que a maioria destes trabalhos é originária deste país, é natural supor que o formato mais familiar seja agraciado sob a égide da usabilidade

dos usuários. Além desse fato, observa-se a influência do sistema *Chaum'2004*, que se tornou uma referência para novos sistemas eleitorais, com uma ampla gama de derivações.

Dentre os sistemas observados, a verificabilidade do eleitor, seja na forma de trilha impressa (VVPAT) ou um comprovante que possa ser verificado em boletim público, é contemplada em diversas soluções. Esta medida, sem dúvida alguma, aumenta a confiabilidade do eleitor no sistema. Diversas técnicas criptográficas são utilizadas nesses comprovantes, mas não há análise estabelecida da compreensão do usuário acerca do seu significado e importância e se essa compreensão (ou sua ausência) tem algum impacto na confiabilidade. De fato, a maioria dos sistemas apresentados é formada por propostas conceituais, com poucas indicações de uso real em eleições ou em simulações.

4.7 Trabalhos Relacionados

A adoção de sistemas de informação digitais em processos eleitorais pode trazer benefícios, como a apuração mais rápida de resultados e a dificuldade na prática de algumas fraudes que dependem do processo manual. Por outro lado, pode introduzir novas vulnerabilidades que podem ser exploradas para a ocorrência de novos tipos de fraudes, até então inexistentes. Sob esta perspectiva, a comunidade acadêmica vem despertando interesse pelo tema, propondo mecanismos para votação eletrônica que sejam cada vez mais seguros. Além dos trabalhos apresentados na RSL (Seção 4.6), destacam-se também os sistemas discutidos nesta seção.

Urnas eletrônicas, como as utilizadas no Brasil, são categorizadas como DRE (*Direct Recording Electronic*) ou de registro eletrônico direto do voto. Os trabalhos apresentados nesta seção visam propor soluções para o risco de que o *software* subjacente registre um voto diferente da intenção original do eleitor, utilizando diversas técnicas.

Hao e Kreeger (56) e Hao *et al.* (57) propõem um protocolo denominado DRE-i (*Direct Recording Electronic with Integrity* — Registro Eletrônico Direto com Integridade) como sistema de votação verificável fim a fim (E2E — *End-to-End*). Para garantir a integridade dos votos, utiliza técnicas criptográficas que, aliadas à publicação de dados de auditoria e de tabelas com os criptogramas (votos codificados), permitem que a apuração seja realizada por qualquer pessoa que conheça o protocolo. Além de propiciar que o eleitor possa certificar-se de que seu voto encontra-se entre os apurados (por meio de boletim público), alegam garantir o sigilo do voto e a detecção de tentativas de fraude pelo equipamento, tanto no registro dos votos quanto nos dados de auditoria. Mesmo com a publicação dos votos em boletim, os autores afirmam que, desde que não haja vazamento dos fatores aleatórios e dos criptogramas pré-computados (utilizados antes do registro do voto do eleitor), o sigilo do voto é garantido pelo protocolo proposto, impedindo a coerção.

O trabalho de Chaum *et al.* (37) propõe um sistema sem uso de papel, no qual o eleitor verifica o voto por meio de um assistente digital que interage com o sistema eleitoral. Esse

assistente pode ser um *hardware* dedicado ou simplesmente um *smartphone*. Alegam que essa proposta reduz o risco de coerção do eleitor e garante que o voto seja corretamente registrado, desde que o dispositivo seja mantido em uma estação de ancoragem durante o processo de votação e ao usuário não seja permitida a entrada de dados, apenas a sua visualização. Por outro lado, os autores não apresentam nenhuma análise da adulteração do assistente via algum *malware*, que possa comprometer os resultados.

Ben-Nun *et al.* (17) apresentam um método que utiliza um sistema duplo (criptografia e registro em papel) para sistemas de votação. Nele, o equipamento de votação imprime o voto em texto plano e em uma versão criptografada, codificada em *QR-code*. Após conferi-la, o eleitor dobra a cédula, ocultando a informação em texto claro, deixando visível apenas a parte codificada. Dirige-se então à autoridade eleitoral, que faz a leitura do voto cifrado e codificado, que será enviado para apuração, e, em seguida, destaca esta parte, que é entregue ao eleitor como um recibo e mecanismo para conferir se o voto encontra-se na lista dos apurados. A parte dobrada e colada, com o voto não criptografado (texto claro), é depositada em uma urna, podendo ser conferida posteriormente, sem uso de *hardware* ou *software*.

Nos trabalhos de Bell *et al.* (13) e Benaloh *et al.* (15), encontra-se uma proposta que também combina métodos criptográficos e votos impressos para um sistema eleitoral seguro e auditável. Ainda em relação à auditabilidade, Benaloh *et al.* (16) sugerem uma abordagem para validação da consistência dos resultados de uma eleição a partir de uma trilha de auditoria (cédulas eletrônicas ou em papel) e outras estruturas de dados publicadas, ao mesmo tempo em que visa manter o sigilo do voto.

No Brasil, foi proposto um sistema de votação mecatrônico, apresentado por Nadaf (77). A concepção do autor constitui-se em uma urna eletrônica ou *tablet*, conectados a leitores biométricos de impressões digitais e de reconhecimento facial. Após identificar-se por meio da biometria, o eleitor registra o seu voto, que é impresso em papel oficial, podendo incluir elementos de segurança, como nas cédulas de dinheiro. O registro do voto é feito em três formatos diferentes: em texto, em código de barras bidimensional e outro em código Braille. O eleitor finaliza o voto no sistema DRE, gerando uma cédula impressa que é depositada em uma urna independente, que valida o voto, armazena-o aleatoriamente em seu interior e sinaliza ao equipamento DRE que ele pode ser gravado. Caso contrário, o eleitor pode anular aquele registro, inserindo-o em outra urna, que realiza a fragmentação e reinicia o processo de votação.

Por fim, Benaloh (14) discute como a tecnologia tornou inefetivas muitas técnicas utilizadas para mitigar a coerção (conhecida no Brasil como “voto de cabresto”) e a venda de votos. Recomenda um reexame dos esforços e contramedidas utilizados para eliminar esses tipos de fraudes e quais defesas são possíveis e razoáveis contra a coerção do eleitor.

4.8 Reflexões Finais

No presente capítulo, foram analisados os sistemas de votação eletrônicos quanto a sua taxonomia, aos tipos de fraude possíveis e aos requisitos de segurança indicados na literatura. Também foi analisada a urna eletrônica brasileira, como o sistema mais amplamente conhecido no País.

A revisão sistemática de literatura apontou tendências em relação ao uso de criptografia e dos tipos de sistemas disponíveis. A maior contribuição, no entanto, é a indicação de que, independentemente do sistema utilizado para verificabilidade do eleitor, esta é uma parte importante da maioria dos sistemas analisados, como garantia da independência de *software*. Além disso, traz como benefício um registro mais próximo ao dia a dia do eleitor e de processos clássicos, em que o voto em papel carrega a intenção do eleitor e pode ser conferido e validado, sem os inconvenientes registrados na literatura dos sistemas manuais ou mecânicos.

5 Resultados e Discussão

No Capítulo 3, foram apresentados a estrutura administrativa e os processos de consulta à comunidade acadêmica para eleição de dirigentes dos IF. Em seguida, no Capítulo 4, analisaram-se sistemas eleitorais na literatura, suas vulnerabilidades e requisitos de segurança.

No presente capítulo, são abordados o protocolo eleitoral e o sistema de informação subjacente que deve implementá-lo. Apresenta também características propostas para a máquina de votação, denominada, no texto, urna eletrônica, dada a familiaridade com o termo.

5.1 Protocolo Eleitoral

Conforme apresentado na Seção 3.2, o processo eleitoral para dirigentes dos IF, uma vez deflagrado, deve ser concluído em 90 dias corridos. Não se discutirá, no presente trabalho, o mérito da suficiência do prazo. Sendo este determinado legalmente, compete às instituições de ensino estabelecer um cronograma de atividades no qual todo o processo seja realizado.

Neste trabalho, propõe-se um protocolo eleitoral que visa à maximização do período entre a homologação das candidaturas e a realização da votação. Neste intervalo, ocorrem as campanhas eleitorais, a apresentação das propostas de trabalho e os debates entre candidatos. Em relação ao cargo de reitor, em especial, um maior prazo permite mais condições de visitação aos *campi*, geograficamente dispersos. Um período mais longo, nesta etapa, também oferece condições de definir se a eleição será realizada em um ou dois turnos, conforme regulamentado (21).

A proposta apresentada na sequência desta seção visa delinear um panorama geral do protocolo elaborado neste trabalho. Retratará o fluxo normal das atividades, sem adentrar nos detalhes de fluxos alternativos, apresentados na Seção 5.2, que também abordará características técnicas do sistema eleitoral.

Para estabelecer o protocolo, identificam-se os seguintes atores:

Conselho Superior: responsável pela deflagração do processo e homologação final dos resultados finais, na condição de órgão máximo da instituição (CS).

Comissão Pré-Eleitoral: designada pelo Conselho Superior no ato de deflagração do processo, tendo como incumbência a condução da eleição da Comissão Eleitoral Central e das Comissões Eleitorais Locais. Representa a autoridade eleitoral inicial ($\mathcal{A}_E$).

Comissão Eleitoral Central: responsável pela condução da eleição para o cargo de reitor, bem como do processo como um todo, coordenando as atividades das Comissões Eleitorais Locais. No protocolo, é representada por $\mathcal{A}_C$, na forma de autoridade eleitoral central.

Comissão Eleitoral Local: responsável pelas atividades do processo em cada *campus* em que ocorra consulta para o cargo de diretor-geral, sendo representada por $\mathcal{A}_L$.

Candidatos: indivíduos legalmente habilitados a concorrer aos cargos em eleição. No protocolo, o conjunto de candidatos é dado por $\mathcal{C}$, e c_i representa o i-ésimo candidato do pleito.

Fiscais: pessoal designado pelos candidatos para acompanhar e fiscalizar as atividades dos mesários durante o período de votação, nas seções eleitorais, e da mesa escrutinadora, durante o período de apuração dos votos. O conjunto de fiscais é representado por $\mathcal{F}$, enquanto o fiscal do candidato c_i é dado por f_i.

Mesários: pessoal convocado pelas comissões eleitorais, por seção de votação, responsável por identificar e habilitar eleitores para votar. Também se responsabilizam pela guarda do equipamento de votação, dos documentos da seção (listas de presença, boletins de urna, etc.). Ainda incluem-se os responsáveis pela apuração dos votos, no presente protocolo, durante as contagens de auditoria. O conjunto de mesários ($\mathcal{M}$) é constituído por pelo menos 3 indivíduos: o presidente da mesa (m_p), o vice-presidente (m_{vp}) e o secretário (m_s), podendo haver mais dois suplentes, se necessário.

Eleitores: indivíduos legalmente habilitados a exercerem o direito ao voto. Devem ser previamente cadastrados em um rol de eleitores ($\mathcal{E}$), que é publicamente disponibilizado para validação da comunidade. O i-ésimo eleitor do rol é representado por e_i. O rol é composto por todos os servidores que compõem o quadro de pessoal ativo permanente da instituição e por todos os alunos regularmente matriculados nos cursos de ensino médio, técnico, de graduação e de pós-graduação, tanto na modalidade presencial quanto à distância (21, Art. 9º).

Outros agentes, que não participam do processo de consulta à comunidade, tais como funcionários de empresas de terceirização de serviços, professores substitutos e temporários, sindicatos, membros da comunidade externa, etc., não são representados no protocolo. Entretanto, eles podem exercer o papel fundamental de auditoria externa dos procedimentos, fiscalizando as atividades desempenhadas pelos atores. No entanto, não lhes pode ser atribuída nenhuma outra função no processo, nem admitida qualquer intervenção destes em sua execução.

Um dos gargalos do processo eleitoral encontra-se na regulamentação interna do processo. Ao disciplinar os processos em âmbito nacional, o decreto federal estabeleceu que uma das competências da $\mathcal{A}_C$ é "elaborar as normas, disciplinar os procedimentos de inscrição dos candidatos e de votação, e definir o cronograma para a realização dos processos de consulta" (21, Art. 6º, inc. I). Esta lacuna foi deixada para não ferir a autonomia das instituições de ensino e garantir que suas características locais sejam respeitadas. No entanto, um regimento eleitoral, para ser discutido e aprovado, pode ocupar um considerável espaço no cronograma, reduzindo o período de campanha. Algumas instituições podem, inclusive, determinar que o regimento seja

aprovado pelo Conselho Superior, o que pode aumentar o tempo necessário para mobilização de seus membros e para publicação, até que entre em vigência.

Se for considerado que existem dois regimentos eleitorais, para disciplinar a eleição da Comissão Eleitoral e o processo de consulta à comunidade propriamente dito, observam-se dois períodos que afetarão o montante disponível para as demais atividades. O presente protocolo propõe que seja aprovado pelo Conselho Superior um Regimento Eleitoral Geral que discipline todos os processos eleitorais da instituição, estabelecendo um conjunto mínimo de regras que deverão ser observadas pelos atores nos processos, responsabilidades e sanções aos desvios de conduta. Este documento deve ser aprovado fora do processo de consulta à comunidade, com bastante antecedência, com o intuito de evitar que interesses e articulações, às vésperas da deflagração da consulta, maculem o regramento com o objetivo de beneficiar ou prejudicar possíveis candidatos. Este documento poderá ser revisado pelo Conselho Superior a qualquer tempo após cada processo eleitoral, com o objetivo de aperfeiçoá-lo.

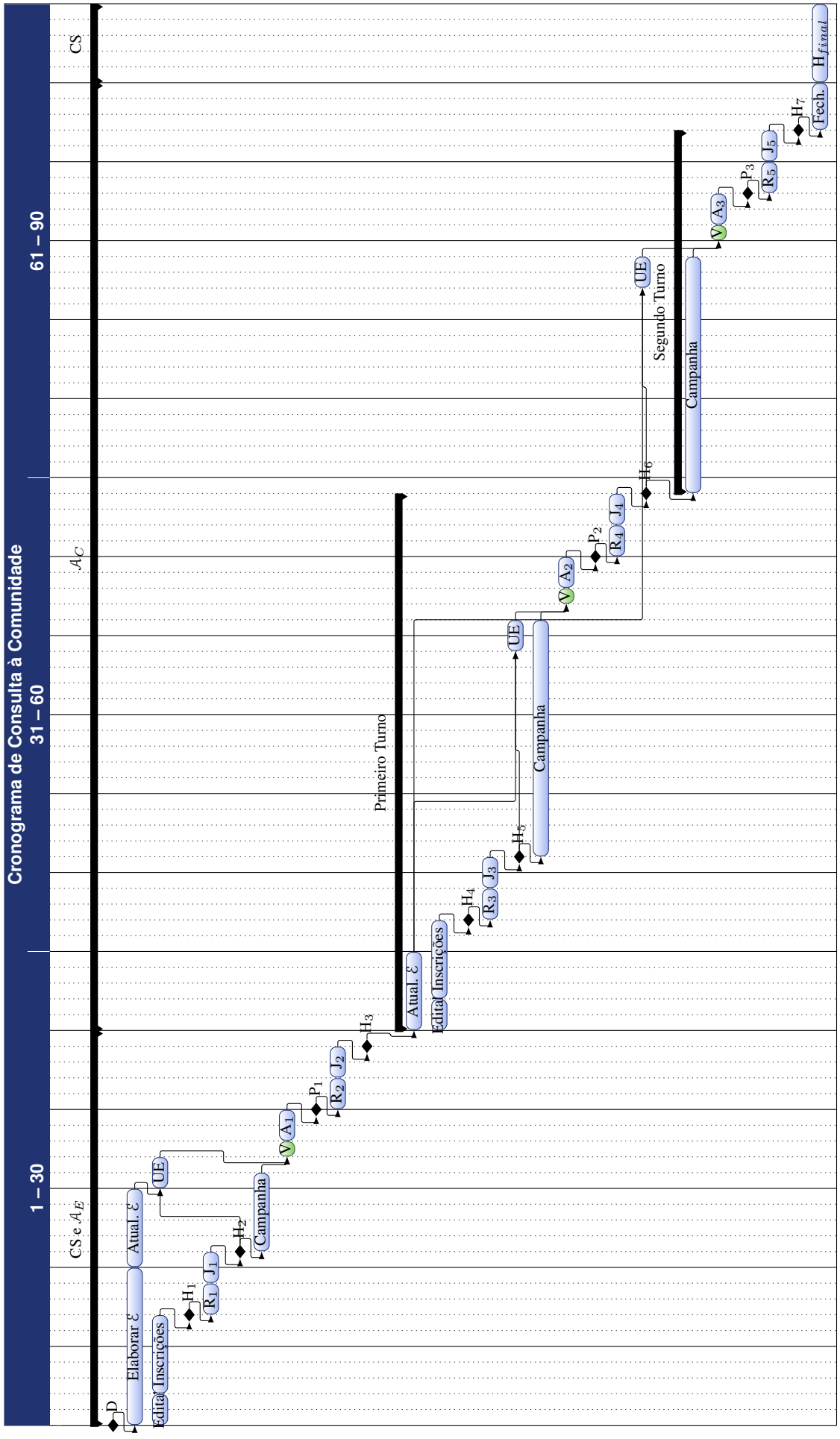
Tal proposta não implica em violação do dispositivo legal previamente mencionado (21), tendo em vista que o Regimento Eleitoral Geral, para ser flexível e atender às diversas situações, delegaria à $\mathcal{A}_C$ o papel de publicar edital convocatório, no qual constam normas para campanha, procedimentos de inscrição e de votação e o cronograma de atividades de cada processo. Pode, inclusive, estabelecer uma minuta de edital que serviria como gabarito, agilizando o processo.

A Figura 9 apresenta uma proposta de instanciação do protocolo para uma eleição em dois turnos. Sem dúvidas, dividir as atividades em dois turnos eleitorais, dentro do período de 90 dias, demanda uma análise crítica de cada atividade, com o intuito de garantir total transparência e flexibilidade. A partir do modelo, torna-se simples a adaptação para eleição em turno único, que, inclusive, garante maior período para campanha dos candidatos. Os prazos de cada etapa foram arbitrariamente escolhidos pelo autor, levando em consideração sua experiência prévia em processos eleitorais. Ressalva-se, ainda, que os prazos podem ser adaptados, considerando-se o próprio calendário da instituição, uma vez que compreende dias corridos, sem levar em conta recessos, fins de semana ou feriados que eventualmente possam ocorrer. Assim, cada atividade pode ser redimensionada, de acordo com suas características intrínsecas, e ainda foram planejados alguns dias para finalização, que podem ser realocados consoante o grau de maturação do processo e as características do período em que a consulta recair.

O processo de consulta à comunidade inicia-se com a deflagração do Conselho Superior do IF, que estabelecerá uma Comissão Pré-Eleitoral ($\mathcal{A}_E$) que conduzirá o processo de formação das comissões eleitorais. No diagrama da Figura 9, estima-se que esta atividade seja conduzida em 25 dias, em média. Períodos superiores a 30 dias prejudicam a condução do processo eleitoral propriamente dito e devem ser evitados.

A primeira atividade da $\mathcal{A}_E$ é elaborar o edital, em conformidade com o Regimento Eleitoral Geral proposto, para dar início às inscrições de candidaturas. Paralelamente, inicia-se também o processo de formação do rol de eleitores ($\mathcal{E}$), com as listas oficiais geradas pelos setores

Figura 9 – Cronograma proposto para o protocolo eleitoral em dois turnos



Fonte: elaborado pelo autor.

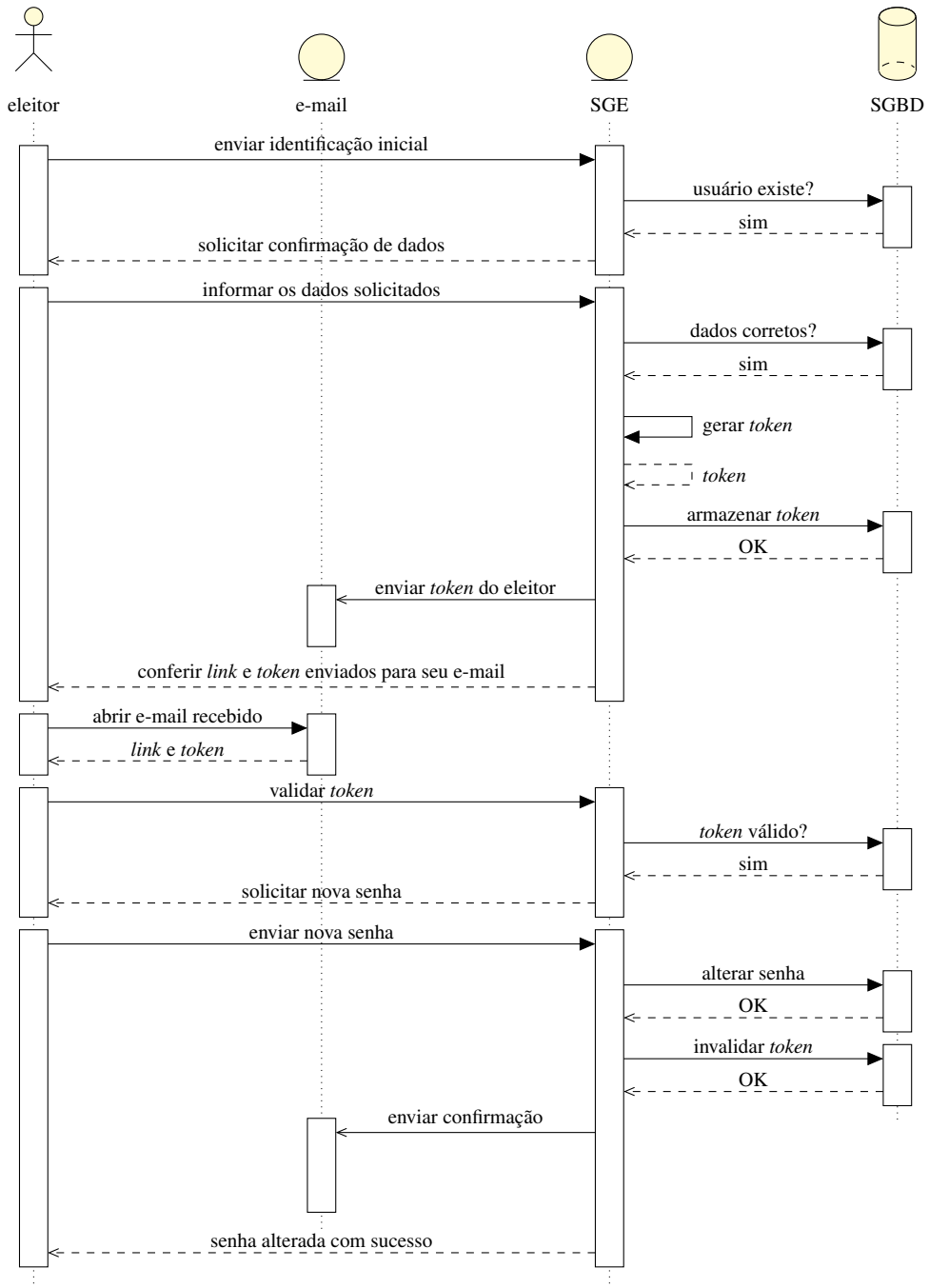
de Gestão de Pessoas e de Registro Acadêmico, respectivamente responsáveis pela relação de servidores (docentes e técnico-administrativos) e de discentes regularmente matriculados até a data de deflagração do processo.

Publicado o edital convocatório, inicia-se o processo de inscrições dos candidatos, que, após finalizado, terá a primeira homologação (H_1) pela $\mathcal{A}_E$. Abre-se um período para impetração de recursos (R_1), no qual podem ser revisados os motivos de não credenciamento ou até mesmo solicitadas impugnações de candidatura, que serão julgados pela $\mathcal{A}_E$ (R_2), produzindo uma homologação definitiva (H_2), com a definição ou sorteio do número do candidato, que será usado na votação (i. e., se usado um número de registro acadêmico ou de matrícula SIAPE ou se serão números sorteados pela $\mathcal{A}_E$). A partir deste momento, principia-se o período de campanha dos candidatos, nos moldes definidos no edital que rege o processo.

Paralelamente a estas atividades, empreende-se o processo de atualização do rol de eleitores ($\mathcal{E}$), através do sistema de gerenciamento da eleição. As listas são publicadas para conferência por parte da comunidade, com o intuito de verificar se não existem vícios nas listagens, como eleitores inexistentes, arrolados em dois segmentos simultaneamente (violando o princípio da unicidade) ou ausência de nomes. A $\mathcal{A}_E$ procede com as correções apontadas e fundamentadas, para preparar para a votação. Durante a revisão, o sistema também permite aos eleitores o cadastramento de uma senha de votação, que será utilizada na seção eleitoral para habilitá-los. O cadastramento é disposto na forma *challenge-response*, na qual o eleitor confirma algumas informações pessoais, constantes do cadastro, recebendo um *e-mail* com um *link* associado a um *token* (um registro com um identificador alfanumérico suficientemente longo, a fim de evitar repetições, que indica que o eleitor está apto a alterar os dados associados a ele) que o capacita a cadastrar uma nova senha. Os eleitores que não o fizerem terão uma senha inicial definida de acordo com alguma das informações pessoais cadastradas e não publicadas.

A Figura 10 apresenta o protocolo *challenge-response* de um cenário em que o e_i (representado pelo ator eleitor) altera sua senha de votação no sistema de gerenciamento eleitoral, que será apresentado com mais detalhes na Seção 5.2.1, representado no diagrama pela entidade SGE (sistema de gerenciamento eleitoral). Após e_i enviar uma identificação inicial, por exemplo, número de registro e endereço de correio eletrônico, o controlador SGE verifica sua existência em um sistema de gerenciamento de banco de dados (SGBD). Caso o eleitor exista, SGE exibirá uma página solicitando a confirmação de valores cadastrados na base de dados, que sejam de conhecimento do eleitor (dados documentais, nome dos pais, etc.). Se este for capaz de informá-los corretamente, SGE gera um *token* que é armazenado no banco de dados por um período predefinido, durante o qual o eleitor poderá utilizá-lo para atualizar a senha. Como camada adicional de confirmação, o *token* é enviado para o endereço de correio eletrônico cadastrado, ao qual supõe-se que somente e_i tenha acesso. Após recuperar a mensagem do gerenciador de *e-mail* do próprio eleitor (representado pela entidade de mesmo nome), este obterá um *link* para a página que fará a validação do *token* e permitirá, caso este último não tenha sido usado ou

Figura 10 – Processo de cadastro de senha de votação pelo eleitor



Fonte: elaborado pelo autor.

expirado, efetivar a alteração da senha. Uma vez alterada, o *token* é definitivamente invalidado, para que terceiros não possam utilizá-lo em lugar de e_i. Por fim, uma mensagem de confirmação é enviada ao endereço de correio eletrônico cadastrado, com o intuito de notificar o usuário acerca de todas as alterações em seus dados cadastrais. No diagrama, não foram representados os fluxos alternativos em que qualquer parte do processo não seja completada com sucesso, com o intuito de simplificá-lo.

Findos os prazos de campanha e de atualização das listas de eleitores, inicia-se a preparação das urnas eletrônicas, representadas por *UE* na Figura 9. Nesta etapa, as urnas são testadas e os dados dos candidatos e eleitores são carregados para os terminais adequados, na presença dos candidatos ($\mathcal{C}$) ou de seus respectivos fiscais ($\mathcal{F}$). Qualquer urna utilizada como demonstração deve ter seus dados eliminados e as cédulas removidas do compartimento de votação, sob auditoria de $\mathcal{C}$ e/ou $\mathcal{F}$. Ao término do processo, todas as urnas são lacradas, rotuladas e separadas para os procedimentos de logística da eleição.

No dia e horários predefinidos, ocorrerá o processo de votação (V) em cada uma das seções eleitorais designadas. Para início dos trabalhos, o presidente da seção (m_p) digitará o código de habilitação no terminal do mesário, que gravará em cartão uma mensagem autenticada para que o terminal do eleitor inicie o processo de votação. Este terminal também emitirá um boletim de urna inicial ($\mathcal{BU}$), no qual serão listados todos os detalhes da seção (localidade, segmento, número de candidatos cadastrados, sua relação nominal e número de votos depositados em votação antecipada, se houver). O $\mathcal{BU}$ será assinado por $\mathcal{M}$ e por $\mathcal{F}$ que estiverem presentes. Não havendo fiscais, o primeiro eleitor rubricará o boletim inicial.

O eleitor dirigir-se-á a sua seção e passará por um processo de identificação civil (apresentação de documento oficial com foto) e verificação da presença na lista de eleitores (elegibilidade) pelos mesários ($\mathcal{M}$). Sendo considerado apto, digitará sua senha previamente cadastrada no terminal do mesário, que habilitará um cartão para acionamento do terminal do eleitor uma única vez. Após inserir o cartão neste último, o eleitor será conduzido pelo processo de votação que, no final, mostrará as opções escolhidas na tela e imprimirá uma cédula com os mesmos valores, para conferência sob uma janela transparente. Se estiver de acordo com as seleções feitas, o eleitor confirmará o voto, e a cédula será depositada em uma urna opaca e lacrada, para auditoria posterior. Caso haja algum erro, ele poderá cancelar aquela cédula, que será destruída na sua presença pelo terminal, e o processo reiniciará. Após votar, recolherá seus documentos pessoais e assinará a lista de presença, junto à $\mathcal{M}$.

Antes de discutir os procedimentos após o período de votação, é importante retomar o conceito de votação antecipada, previamente mencionado. O sistema eleitoral brasileiro, da forma como é implementado atualmente, não permite a votação em trânsito, e os eleitores fora de seu domicílio eleitoral devem justificar sua ausência, devido à obrigatoriedade do comparecimento às urnas. Em outros países, mesmo sendo facultativo o voto, existe a possibilidade do chamado voto por correio, no qual o eleitor solicita a cédula e a posta com destino à autoridade eleitoral, seguindo instruções para que o voto seja contabilizado corretamente (4). As diretrizes de TGDC (107) preveem a votação antecipada como uma funcionalidade que possa ser implementada. Esta característica pode ser desejável e deve ser um parâmetro de configuração da eleição.

Cada *campus* possui um horário de funcionamento diferente, assim como unidades conveniadas, que, muitas vezes, funcionam em prédios escolares emprestados pelo município para funcionamento noturno, quando estão disponíveis. Por isso, cada seção tem que ter um

horário de votação adequado a sua realidade. Se os horários não forem concomitantes, é possível estabelecer uma logística em que um mesário designado a uma mesa receptora fora de seu domicílio eleitoral, como, por exemplo, um polo de EaD, possa votar antes de se deslocar até o destino, tendo preservado seu direito ao voto. Nem sempre é possível garantir tal conveniência aos mesários, seja por força regimental que determine horário único de votação, seja por fatores puramente logísticos, como tempo hábil para deslocamento, o que pode impedir que o direito ao voto seja exercido. Neste aspecto, entra a antecipação do voto dos indivíduos convocados pela autoridade eleitoral para se dirigirem a outros pontos de votação e até mesmo aos fiscais designados pelos candidatos, também sujeitos às mesmas restrições e elementos inquestionáveis da auditoria dos processos.

O procedimento consiste em habilitar uma única urna por segmento da sede eleitoral que cederá indivíduos para seções externas. Essa função somente estará disponível nas urnas que a tenham habilitada no sistema de gerenciamento, para carga na configuração da urna. Após o carregamento dos dados e inspeção, conforme previamente discutido nesta seção, o presidente da $\mathcal{A}_E$ habilitará as urnas para que os mesários e fiscais registrem seu voto, em dia e horário determinados e na presença dos candidatos. A urna disponibilizará, além do código de ativação para eleição, um código para abertura e finalização da sessão de votação adiantada. Os eleitores serão habilitados, votarão nas mesmas condições de sigilo da eleição normal e a urna será finalizada, não podendo mais ativar a votação antecipada. O fato será registrado em ata, com identificação no formulário de ata da seção a que se destina a urna, para ciência dos mesários e conferência do $\mathcal{BU}$ inicial, se a situação foi registrada. As urnas serão guardadas sob responsabilidade da autoridade eleitoral, que deverá garantir que nenhuma violação ocorrerá. O sistema da urna eletrônica não deverá emitir nenhuma informação sobre os votos registrados, que serão contabilizados exclusivamente no $\mathcal{BU}$ final, no dia da votação, conforme se descreve na sequência.

Ao término do horário de votação, havendo eleitores aguardando para votar, o presidente da mesa receptora (m_p) distribuirá senhas, a partir do final da fila. Não existindo mais nenhum eleitor, ele utilizará o terminal de mesário para digitar o código de encerramento da sessão, que será gravado no cartão e inserido no terminal do eleitor. Neste momento, o terminal emitirá, no mínimo, 2 vias do boletim de urna ($\mathcal{BU}$), que serão rubricadas pelos mesários e no mínimo dois fiscais presentes. Não havendo representação de $\mathcal{F}$, os dois últimos eleitores procederão com a assinatura do $\mathcal{BU}$. Uma via será afixada à porta da seção e a outra será devolvida à $\mathcal{A}_E$ para inserção no processo. Os fiscais presentes, se desejarem, poderão solicitar a impressão de mais vias do $\mathcal{BU}$, para fins de fiscalização. Sob nenhuma hipótese esse pedido poderá ser negado por $\mathcal{M}$.

As urnas serão recolhidas à custódia da $\mathcal{A}_E$, que iniciará o processo de apuração seletiva e auditoria (A_1), previsto na Figura 9. Nesta etapa, será apurado um percentual de urnas, aleatoriamente escolhidas, conforme detalhadamente apresentado na Seção 5.2.3. Também serão

apuradas, obrigatoriamente, quaisquer urnas que sejam objeto de reclamação de divergência entre o registro eletrônico exibido e a cédula impressa para conferência, validados por m_p. A $\mathcal{A}_E$ convocará cada candidato c_i, que poderá fazer-se acompanhar ou ser representado por um fiscal credenciado (f_i), para uma sessão em que as urnas sorteadas serão abertas e terão seus votos contados um a um. Os resultados serão confrontados com o $\mathcal{BU}$ emitido no dia da eleição, conforme apresentado na Seção 5.3.

Realizada a auditoria por apuração aleatória, publica-se o resultado da votação (P_1), que será seguido pelos prazos regimentais de recursos (R_2), que serão julgados pela autoridade eleitoral (J_2) à luz da regulamentação. O resultado final, enfim, será homologado pela $\mathcal{A}_E$, com posterior edição de ato administrativo de nomeação das $\mathcal{A}_L$, que instalarão os trabalhos do processo de consulta à comunidade e definirão seus respectivos presidentes e indicarão os membros da $\mathcal{A}_C$, conforme regulamentado (21), para nomeação. A partir deste ponto, findam-se os trabalhos da $\mathcal{A}_E$, que passará a documentação autuada até o momento à $\mathcal{A}_C$, que assumirá a condução do processo.

Em relação aos procedimentos de cada turno, não existem muitas variações em relação ao apresentado nesta seção. Destaca-se a abertura de novo edital para convocar e reger as candidaturas aos cargos de reitor e de diretor-geral de *campus*, cujo processo seguirá as mesmas etapas já realizadas, apenas conduzidas pela $\mathcal{A}_C$ e pelas $\mathcal{A}_L$ em lugar da $\mathcal{A}_E$. Deve-se também salientar que as listas de eleitores já estavam previamente elaboradas, abrindo-se o sistema de gerenciamento para os eleitores que desejarem alterar sua senha, independentemente de tê-lo feito previamente, incluindo, ainda, correções encontradas e registradas no dia da votação.

Após a homologação do resultado do segundo turno (se houver), a $\mathcal{A}_C$ procederá com o fechamento do processo, autuando as peças que ainda faltem ($Fech.$), que será encaminhado ao Conselho Superior, para a última e definitiva homologação (H_{final}), que enviará posteriormente o processo ao Ministério da Educação para que a nomeação do candidato eleito ao cargo de reitor seja realizada.

5.2 Sistema Eleitoral Proposto

Para auxiliar a execução do protocolo eleitoral apresentado na Seção 5.1, propõe-se um sistema de informação que execute as funções de gerenciamento, de coleta e de apuração dos votos. O sistema eleitoral é dividido em dois componentes: o sistema de gerenciamento eleitoral e a urna eletrônica.

5.2.1 Sistema de Gerenciamento Eleitoral

O sistema de gerenciamento eleitoral é uma aplicação *web* que executa as funções gerenciais do processo eleitoral. É responsável pela manutenção do rol de eleitores ($\mathcal{E}$) e pelo cadastro de candidatos ($\mathcal{C}$) e de fiscais ($\mathcal{F}$). Também é incumbido da inseminação dos dados

de eleitores e candidatos nas urnas eletrônicas de cada seção eleitoral e pela publicação dos respectivos boletins de urna após a votação.

Para fins de organização das unidades eleitorais, acomodando a estrutura *multicampi* e segmentada, consideram-se as seguintes estruturas, emprestadas e estendidas do modelo eleitoral convencional:

Distrito Eleitoral: área de abrangência de um *campus*, sob a jurisdição de uma $\mathcal{A}_L$, ou a reitoria, supervisionada pela $\mathcal{A}_C$. Inclui a sede da unidade e quaisquer unidades conveniadas ou polos de EaD sob sua responsabilidade.

Zona Eleitoral: cada distrito eleitoral é dividido em três zonas, representando os segmentos docente, discente e técnico-administrativo da comunidade acadêmica.

Seção Eleitoral: local de votação, gerenciado por uma mesa receptora ($\mathcal{M}$), onde os eleitores cadastrados dirigir-se-ão para registrar seu voto. Cada seção pertence a uma zona específica do distrito eleitoral, com o propósito de permitir a parametrização da eleição para o cálculo do percentual final de votos.

A divisão apresentada tem como objetivo dar maior flexibilidade na configuração das eleições. Por exemplo, uma consulta típica à comunidade tem candidatos a reitor que devem aparecer entre as opções de todos os distritos que compõem o IF. Ao mesmo tempo, cada *campus* tem seus próprios candidatos a diretor-geral, que não devem aparecer fora do distrito eleitoral adequado. O sistema de gerenciamento deve permitir a coexistência de candidatos globais (para todos os distritos simultaneamente), distritais (por *campus*) e por zona eleitoral (por segmento). Este último caso abrange eleições para conselhos e comissões, nas quais cada segmento vota em seus próprios pares.

Os primeiros requisitos do sistema são, portanto, a criação e a configuração de uma eleição. Nestes requisitos, são cadastrados os distritos e as zonas eleitorais, determinando se haverá candidatos globais, distritais ou por segmento. Deve também permitir a parametrização da eleição, por exemplo, com aplicação de coeficientes como os encontrados na Equação 3.1, por zona eleitoral. Considerando-se as múltiplas autoridades eleitorais, deve haver delegação de privilégios na aplicação para que cada $\mathcal{A}_L$ gerencie seu próprio distrito, enquanto a $\mathcal{A}_C$ gerencia o distrito da reitoria e as candidaturas globais. O cadastro da eleição também inclui o cadastro dos candidatos, atribuição de seu número na urna, entre 2 e 10 dígitos, geralmente na faixa dos inteiros de 32 *bits*, sem sinal. Faixas maiores dependem da linguagem e do tipo de *hardware* usado na urna eletrônica, sendo recomendável a manutenção do limite proposto.

O sistema deve também permitir o gerenciamento do cadastro eleitoral ($\mathcal{E}$), associando-o a suas respectivas zonas eleitorais. Considerando que cada segmento deve possuir um sistema de numeração diferente, como matrícula SIAPE para servidores e número de registro acadêmico

para estudantes, o mapeamento deve ser realizado por CPF (Cadastro de Pessoa Física). Se for detectada a duplicação do cadastro em zonas diferentes, o sistema deve alertar o operador, para que seja feita a alocação em uma única zona eleitoral, conforme regras estabelecidas no Regimento Eleitoral Geral. Por exemplo, um Técnico Administrativo em Educação pode estar matriculado em um curso da própria instituição, sendo comum a determinação de que vote apenas no segmento dos servidores técnico-administrativos, onde tem maior peso individual. Esta medida deve garantir a elegibilidade e unicidade do voto do eleitor.

Para facilitar o cadastramento inicial, deve ser provido um mecanismo de importação de dados em formato aberto. Desta forma, os dados dos eleitores podem ser exportados de outros sistemas utilizados pela instituição e serem incluídos em lote no sistema eleitoral, evitando-se a digitação manual. Os critérios para inclusão nas seções devem ser parâmetros do sistema, como unidade de lotação do servidor, segmento em que tenha maior contribuição individual para servidores, entre outros. Para os alunos, além da unidade em que o aluno esteja matriculado, o agrupamento pode ser feito por curso, nível de ensino ou até mesmo por ordem alfabética, preenchendo sucessivamente as seções até o número máximo de eleitores que for parametrizado.

O cadastro eleitoral também deve permitir que os eleitores, nos períodos determinados e antes da inseminação dos dados nos terminais das urnas eletrônicas, atualizem sua senha de votação. O sistema deve utilizar um protocolo *challenge-response*, no qual o eleitor e_i autentica-se, informando um conjunto de dados não públicos (por exemplo, o número completo do CPF, a data de nascimento e o primeiro nome da mãe), sendo gerado um *token* que é enviado para seu *e-mail* cadastrado, em um *link* válido por um determinado período de tempo (configurável), que e_i usará para definir uma senha a ser usada no terminal do mesário para sua autenticação. Na abertura do período de atualização das senhas, o sistema deve ser capaz de enviar mensagem a todos os eleitores, notificando-os e detalhando os procedimentos e a que autoridade eleitoral devem se reportar em caso de dúvidas.

Como em qualquer processo eleitoral, há a possibilidade de os candidatos e/ou seus correligionários desviarem-se da conduta esperada no Regimento Eleitoral. Nesse caso, sanções devem ser aplicadas com o intuito de disciplinar o processo. O cadastro das denúncias, defesa da parte acusada e decisão são imprescindíveis no processo.

Devem ser cadastradas, no sistema, as urnas eletrônicas, seus respectivos números de série, chaves criptográficas, distrito, zona e seção. Estes dados, em conjunto com a chave pública da eleição e as listas $\mathcal{C}$ e $\mathcal{E}$ do distrito e da seção, devem ser exportados em formato JSON (*JavaScript Object Notation*) assinado digitalmente (*JSON Web Signature*), conforme especificação de Jones; Bradley e Sakimura (62). Estes arquivos serão utilizados no processo de inseminação (carga de dados) dos terminais eletrônicos usados no dia da votação. Serão identificadas as urnas em que a votação antecipada for habilitada, para que sejam preparadas para os procedimentos eleitorais.

Após a eleição, em cada seção eleitoral, o m_p deve enviar os dados provisórios de totalização, extraídos do $\mathcal{BU}$. Estes dados constituem o *bulletin board* ($\mathcal{BB}$) da eleição, permitindo acompanhamento da comunidade via *internet*, e serão marcados como temporários, até o carregamento do arquivo digitalmente assinado do $\mathcal{BU}$, oficializando-o. Portanto, além dos usuários membros das comissões eleitorais, devem ser cadastrados e autorizados, nesta função, cada um dos presidentes das mesas receptoras ($\mathcal{M}$). A comunidade, de posse dos $\mathcal{BU}$ afixados na entrada da seção, poderá validar e certificar-se do carregamento correto dos dados, tanto por parte do m_p quanto do $\mathcal{BU}$ digital. Por fim, após o processo de auditoria por amostragem, apresentado na Seção 5.1, os resultados da seção ainda podem ser corrigidos, em conformidade com o voto impresso conferido pelo eleitor.

O terminal do mesário também exportará a lista de eleitores presentes, que será importada para assinalar, no $\mathcal{BB}$, quais membros de $\mathcal{E}$ que compareceram. Esta funcionalidade permite à comunidade verificar se não houve eleitores fantasmas ou engravidamento de urna por parte dos mesários, na mesma interface utilizada para conferência do rol de eleitores.

Todos os cadastros devem ser facilitados por importação usando formato de dados abertos, como arquivos separados por vírgulas (CSV — *comma-separated values*), gerados a partir dos sistemas de informação da instituição. Todas as operações de cadastro devem ser permitidas apenas dentro de uma rede protegida, com acesso por rede privada virtual (VPN), aos usuários das $\mathcal{A}_L$ e da $\mathcal{A}_C$ (ou da $\mathcal{A}_E$, quando necessário), conforme descrito na Seção 5.2.4.

Para fins de transparência ativa e auditabilidade por parte da comunidade, todos os dados do sistema são públicos (22) e devem ser acessados, independentemente de autenticação, por meio de um portal do sistema, isolado das funcionalidades de cadastramento. Nesta área pública, também são disponibilizados, automaticamente, os demais dados do $\mathcal{BB}$, como homologações de candidaturas, recursos e decisões, resultados parciais e finais, etc. É desejável que a lista de candidatos apresente os dados usados na inscrição, fotografia, minicurrículo, arquivos com proposta de governo e acesso à página ou ao *blog* oficiais da candidatura, dando ampla visibilidade e de maneira igualitária a todos.

5.2.2 A Urna Eletrônica

Em continuidade à apresentação do sistema eleitoral proposto neste trabalho, esta seção descreve o *hardware* que compõe a urna eletrônica. Assim como o modelo do TSE, a presente proposta divide-se em um terminal do eleitor, onde serão registrados os votos, e o terminal do mesário, responsável pela autenticação do eleitor e pela liberação da urna para um único voto. A diferença na concepção encontra-se em dois elementos-chave: 1) o terminal do eleitor possui uma impressora para registro impresso do voto (VVPAT); 2) o processamento do terminal do mesário é realizado no próprio equipamento, sem conexão física com o terminal do eleitor.

O terminal do mesário, *ad initio*, é de construção simples, composto por um teclado numérico com teclas de função para confirmação ou correção dos dados, um *display* de cristal líquido para exibir os caracteres das mensagens (ou seja, não necessita ter resolução gráfica, podendo ter 2 ou 4 linhas por 20 colunas) e uma interface para cartão de controle do terminal do eleitor. Este cartão pode ser um *smart card*, com gerenciamento interno de chaves, ou simplesmente um cartão RFID, com leitura e escrita por radiofrequência. Nesse último caso, a interface do cartão deverá ser protegida por uma gaiola de Faraday, com o propósito de evitar interferências externas durante a leitura e a escrita. É possível adicionar identificação biométrica do eleitor, utilizando um leitor de impressões digitais e ajustando o modelo de recrutamento, com pontos de coleta de dados biométricos. Caso esta falhe, por qualquer motivo, a senha cadastrada pelo eleitor é solicitada. O gerenciamento pode ser feito por um microcontrolador de baixo custo, como um Arduino[9], uma vez que não haverá processamento intenso nesta unidade. Caso haja interrupção no fornecimento elétrico da concessionária, deve dispor de uma bateria interna capaz de suportar, no mínimo, seis horas ininterruptas de operação, de acordo com o consumo calculado. Mecanismos para economia de energia, como desligamento do *display*, devem ser implementados. Uma interface para cartão SD, lacrada pela $\mathcal{A}_C$, serve de interface de carregamento de dados, antes da eleição, e para *download* da lista de eleitores presentes, após seu término.

Uma implementação alternativa do terminal de mesário envolve a utilização de um microcomputador, *tablet* ou *smartphone*, formatados ou redefinidos para as configurações de fábrica, conforme o caso, com uma aplicação que execute as funções descritas nesta seção, e acessórios complementares, como leitores biométrico e de cartões. Embora um *hardware* dedicado seja preferencial, mantido sob custódia da $\mathcal{A}_C$, o aproveitamento de recursos já existentes pode auxiliar na redução do custo da logística das eleições. Por exemplo, a mesa receptora levaria a cada seção eleitoral um terminal do eleitor, os leitores necessários e um CD-ROM com um sistema operacional contendo a aplicação para ativação da urna. Toda comunicação sem fio deve ser desabilitada do sistema, conforme sugerido por Norden (78).

O terminal do eleitor, por sua vez, requer atenção especial, uma vez que registrará a vontade do eleitor e deverá garantir que esta prevaleça todo o tempo. Por questões de familiaridade, opta-se por uma estrutura similar à da urna eletrônica brasileira, em termos de formato e interface, com algumas adaptações. Além da tela de cristal líquido, que exibirá a interface com o eleitor, o teclado numérico e as teclas para confirmar e corrigir (a exclusão da tecla para voto em branco será abordada em sequência), adiciona-se uma janela transparente, de acrílico ou vidro, com cerca de 15 cm de comprimento e com largura suficiente para acomodar o papel utilizado. Na parte superior desta janela, posiciona-se uma impressora, que emitirá o voto impresso para conferência do eleitor, sem que este tenha contato físico com ele. A parte inferior da janela fica conectada a um servomotor, que posicionará a saída do papel, que descerá, por efeito da

[9] http://arduino.cc

gravidade, sobre roletes para recolhimento do material a uma caixa opaca e lacrada dentro do gabinete do terminal ou para um conjunto de guilhotinas, que fragmentarão o papel, recolhendo-o a uma caixa separada, destruindo o material repudiado pelo eleitor, que poderá ver, por uma pequena abertura transparente, o descarte da cédula.

Ao iniciar, o sistema operacional exibirá apenas a janela da aplicação eleitoral do terminal. Esta não terá nenhum meio de manipulação, tanto graficamente (barra de título com botões) quanto por teclado, que só tem as opções numéricas e os botões para confirmação e correção da entrada. O usuário não poderá manipular nenhum outro processo em execução no dispositivo. O projeto da aplicação também favorece esse modelo de interação e de ocultamento do sistema operacional subjacente, pois a descrição corresponde a uma máquina de estados finitos, de fácil implementação e validação. Outros autores também propõem a modelagem no formato de máquina de estados finitos, como Sturton *et al.* (105) e Tiella; Villafiorita e Tomasi (108).

Conforme apresentado na Seção 4.3, a Engenharia Semiótica da urna favorece uma interação dialógica com o eleitor e o conduz de forma mais precisa que as interfaces sensíveis ao toque utilizadas em muitas eleições americanas, cuja calibração pode alterar o voto sem percepção do eleitor (52, 78). A oferta de um sistema com uma interface familiar ao usuário favorece a usabilidade e esta já foi utilizada em vários formatos de votação, como eleições para a escolha de um candidato dentre vários (*1-de-n*), ou referendos para seleção entre sim e não.

Esta flexibilidade é extremamente desejada e recomendada por TGDC (107). Uma eleição para escolha de *1-de-n* é a mais simples ou comum, mas também não são raras as situações em que o eleitor pode escolher um subconjunto de opções dentre o universo de $\mathcal{C}$ (*m-de-n*). Por exemplo, para eleição de representantes do segmento para composição de um conselho da instituição, é possível que seja permitido ao eleitor votar em 2 ou 3 opções, dentre os diversos candidatos. Implementar com o modelo da urna eletrônica brasileira não é difícil, já que se torna necessário repetir a tela tantas vezes quantas forem as escolhas permitidas e validar a entrada para impedir que sejam repetidos os mesmos números. Em uma interface com tela sensível ao toque, na qual o usuário seleciona várias alternativas, há uma preocupação para que não ocorra o *overvoting* (seleção superior ao permitido) ou *undervoting* (quantitativo inferior), sendo monitoradas as seleções feitas. No modelo proposto, em que será exibida uma tela para que o eleitor digite o número de cada candidato separadamente, não é possível ele votar além do número de opções que lhe sejam ofertadas, eliminando o primeiro problema. O segundo, em termos brasileiros, não constitui um problema, já que se encontra consagrado o uso e o direito ao voto em branco, no qual o eleitor abstém-se de indicar um candidato. Além disso, inerentemente é implementado o modelo *write-in*, no qual o eleitor escreve em qual candidato deseja votar, no caso, através do número atribuído, que nem sempre é implementado em sistemas baseados em PCOS.

Em relação ao voto em branco, a proposta exclui a tecla existente na urna eletrônica brasileira. Em termos práticos, na própria legislação eleitoral, não há distinção entre voto branco

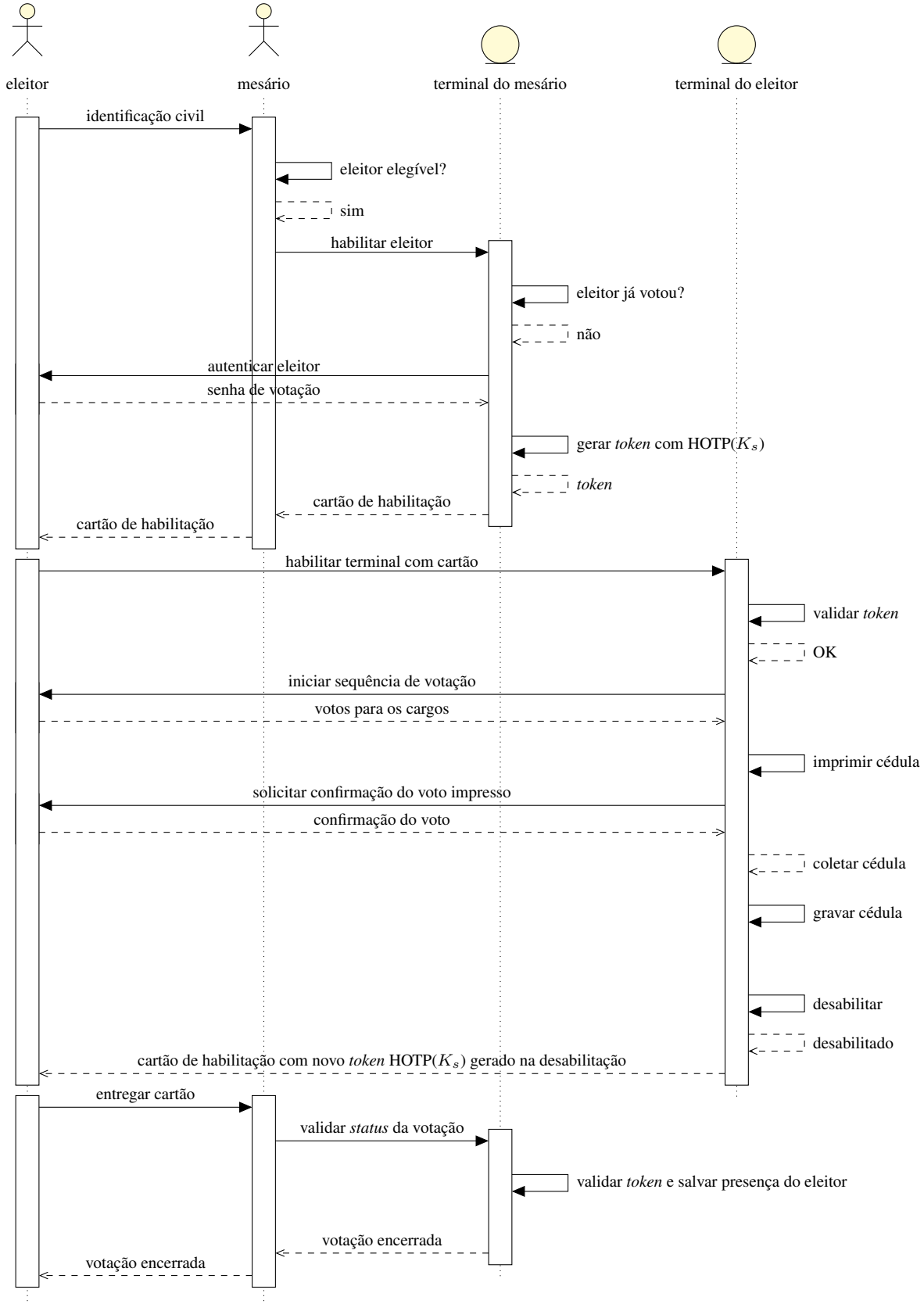
ou nulo, ambos são inválidos e não são contabilizados para qualquer candidato. Na urna eletrônica brasileira, o eleitor pode votar nulo digitando um número inexistente ou em branco, pressionando a tecla para este fim, registrando sua abstenção naquele cargo. Neste trabalho, propõe-se que qualquer valor digitado pelo usuário, que não corresponda a um candidato válido, seja atribuído à classe "voto branco/nulo" e seja convertido (e informado ao eleitor) para que tenha todos os dígitos iguais a 0 (zero). Esta medida busca mitigar o risco do ataque italiano para coerção dos eleitores. Esta medida torna obsoleta a tecla para voto em branco e simplifica o processo de apuração dos votos, uma vez que a votação é facultativa e não compulsória, como nas eleições regidas pelo TSE.

Em linhas gerais, pode-se estabelecer o processo de votação, sob a perspectiva do eleitor, da forma como se segue. Este, após ser habilitado no terminal do mesário, mediante identificação civil e autenticação com sua senha de votação, recebe um cartão e se dirige ao terminal próprio para votar. Ao introduzir o cartão no leitor (que possui as mesmas características descritas para o terminal do mesário), o sistema passa do estado de espera para o de votação. Um sensor mecânico detecta a presença do cartão e aciona uma trava, impedindo sua retirada antes do término do processo, evitando tentativas de reuso da habilitação. A urna passa à sequência de votação, apresentando sucessivamente as telas para os cargos cadastrados. O eleitor digita o número do candidato desejado, observando, na tela, se a foto apresentada corresponde a sua opção. Se não estiver correta, pressiona a tecla para corrigir, limpando os campos da tela e permitindo a redigitação. Se o eleitor estiver satisfeito com a seleção, pressiona a tecla de confirmação, passando para o próximo cargo, até que todos estejam finalizados. Em qualquer cargo, o eleitor poderá digitar um valor inexistente, sendo alertado pelo sistema de que será registrado um voto branco/nulo e que o valor digitado será convertido para zeros na cédula. Após o último cargo, o sistema mostrará uma tela com um resumo das opções do eleitor, solicitando que confira a impressão ao lado e confirme ou rejeite o voto (pressionando, respectivamente, a tecla de confirmação ou de correção). Se o voto for confirmado, será recolhido para uma urna interna e opaca, para fins de auditoria. Se for rejeitado pelo eleitor (pressionamento da tecla de correção), a cédula será destruída, e o processo de votação reiniciará a partir do primeiro cargo. A sequência encontra-se representada na Figura 11, na qual, para fins de simplificação, não são exibidos os fluxos alternativos.

Quando o eleitor finalizar seu voto com sucesso, o cartão receberá um código informando apenas que o voto foi finalizado satisfatoriamente, para atualização do registro no terminal do mesário, conforme exibido na Figura 11. Nele, nenhuma informação acerca do voto deve ser registrada, nem qualquer informação que o associe ao eleitor, apenas um código de habilitação e uma senha de uso único do padrão HOTP (*HMAC-based One-Time Password*), conforme especificação de M'Raihi *et al.* (76).

O emprego da senha de uso único evita que o mesmo cartão seja utilizado para habilitar duas vezes o mesmo terminal, considerando que, a cada execução, os terminais incrementam

Figura 11 – Processo de votação



Fonte: elaborado pelo autor.

seu contador e geram um novo valor, enviado para a outra ponta por meio do cartão. Como cada sequência de senhas depende de uma chave definida pelas partes (K_s), antes do início da votação, considerando que cada cartão tem seu próprio número de série, um ataque externo será mais difícil, e os dispositivos podem recusar cartões inválidos.

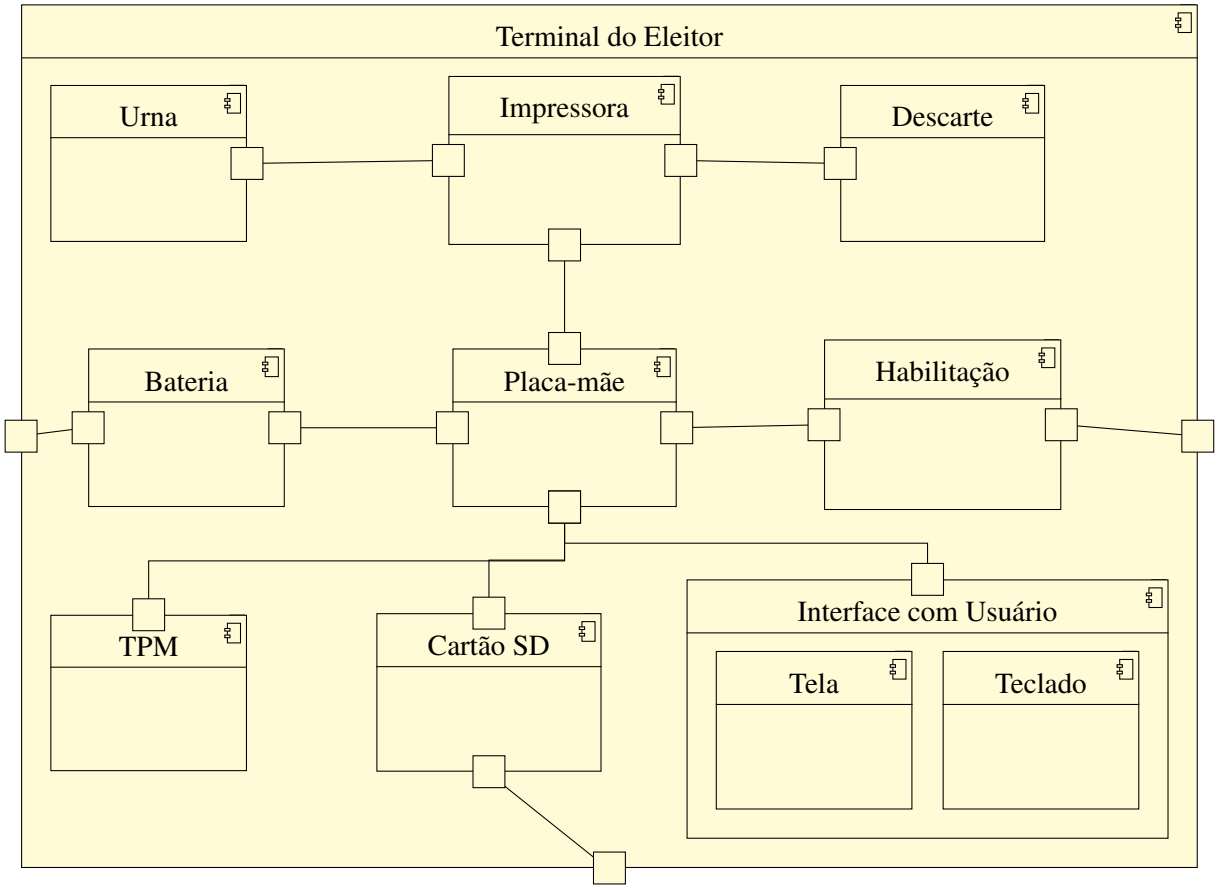
Há efeitos colaterais benéficos desta estratégia e da ausência de conexão física entre os terminais, tendo em vista que o enlace entre eles foi criticado, por Maneschy e Jakobskind (71), por vincular a identificação do eleitor ao terminal de votação, permitindo associá-lo ao voto. Como não há vínculo físico e a habilitação é feita por cartão, o mesmo terminal de mesário pode ser usado para gerenciar mais de um terminal de eleitor. Desta forma, seções com grande número de eleitores podem ter votação em paralelo, com o mesmo conjunto de mesários. Além disso, como o registro dos eleitores está no terminal de mesário, em caso de necessidade, a urna pode ser substituída sem atrasos decorrentes da transferência dos votos e da lista de eleitores de um dispositivo para outro, que é uma operação lenta, conforme apontada por Brunazo Filho e Gazziro (32). Basta habilitar outro cartão entre a nova urna e o terminal de mesário e continuar a votação normalmente. Se o problema ocorrer no terminal do mesário, faz-se a substituição do terminal, carregando o cartão com o rol de eleitores e fazendo o pareamento da chave com o terminal do eleitor.

Um sinal sonoro deve ser emitido para sinalizar o término bem-sucedido de uma votação, assim como no modelo brasileiro. O eleitor retirará o cartão e o levará à mesa receptora, onde o *status* será lido e registrado na lista eletrônica de presença, e poderá assinar a lista física e receber seus documentos de volta, retirando-se da seção. É possível que o eleitor abandone a votação com o cartão ainda inserido na máquina, e, ao contrário da urna brasileira, o mesário não tem como enviar um comando para cancelamento do eleitor a partir de seu terminal.

Para contornar este inconveniente, após um período configurável de inatividade de, no mínimo, 60 segundos, a urna iniciará um *timer* para finalização, também ajustável, ao término do qual o eleitor será invalidado, o cartão registrará abandono da votação como *status*, será liberada a trava e qualquer voto impresso será destruído, como se fosse rejeitado pelo eleitor. Para evitar que um eleitor seja cancelado enquanto estiver votando mais devagar, em função de alguma necessidade especial, o terminal emitirá um bip a cada 20 segundos e mostrará, em destaque, mas de forma não intrusiva, que venha a dificultar o processo de votação, que o eleitor deve pressionar alguma tecla numérica, para que a contagem seja parada, e continue votando normalmente. Os mesários, ouvindo o sinal da urna, poderão orientar o eleitor verbalmente, sem aproximar-se da cabine de votação.

A construção do terminal do eleitor pode ser feita na própria instituição. Por exemplo, todo o gabinete pode ser feito em uma marcenaria, com material leve e resistente. Recomenda-se que as laterais do equipamento possuam abas retráteis, que podem servir como bloqueio visual e constituir uma cabine de votação com privacidade. Internamente, o terminal do eleitor é representado na Figura 12 e é constituído por:

Figura 12 – Diagrama de componentes do terminal do eleitor proposto



Fonte: elaborado pelo autor.

Placa-mãe: elemento principal do processamento, contendo placa-mãe, processador e demais conexões de interface. Pode ser implementada com dispositivos de baixo custo e tamanho compacto, como as placas Beaglebone, Raspberry Pi ou Intel Galileo. O processador deve ter, preferencialmente, um número de série de fábrica, que possa ser lido somente pelo sistema operacional, que servirá como número de série da urna. Na sua ausência, algum dispositivo de numeração em *hardware* deve ser utilizado, como, por exemplo, o *chip* DS2401 da Maxim.

Módulo de segurança: responsável pelo armazenamento e controle das chaves criptográficas e inicialização segura do sistema operacional (*secure boot*). Pode ser implementado usando um *chip* TPM (*Trusted Platform Module*) ou um *smart card*, deve ser resistente à adulteração e manter, de forma segura, as chaves criptográficas usadas no sistema.

Bateria selada: utilizada para manter o sistema em funcionamento em caso de falta da alimentação elétrica vinda da rede da concessionária. Conectada a um circuito que mantém sua carga, enquanto a rede externa estiver disponível, entra em ação para sustentar o funcionamento do equipamento quando houver uma interrupção do fornecimento. Deve

ser dimensionada para sustentar o equipamento por, no mínimo, 6 horas ininterruptas, aliada a mecanismos de conservação do consumo em modo de espera.

Impressora: imprime as cédulas e os $\mathcal{BU}$ previstos no protocolo. Pode ser implementada como uma impressora térmica não fiscal, com guilhotina para corte completo do papel, para depósito definitivo na urna ou seu descarte. Dependendo da disponibilidade e do tamanho do gabinete da urna, também pode ser usada uma impressora a jato de tinta, com tamanhos reduzidos de papel, como os formatos A6 (105 mm $\times$ 148 mm) e A7 (74 mm $\times$ 105 mm). Nenhuma cédula deve ser divida em mais de um segmento de papel e, no caso dos boletins de urna, cada página deve ser numerada, constando o número total de páginas em cada folha (caso sejam usados papéis não contínuos).

Urna lacrada: local em que serão armazenados os votos conferidos e confirmados pelos eleitores, sem acesso externo.

Receptáculo para descarte: local para armazenamento das cédulas rejeitadas pelo eleitor, após passarem por lâminas de refilamento que destruam seu conteúdo.

Leitor de cartão de habilitação: interface para receber um cartão RFID ou *smart card* com os códigos de ativação de eleitor, onde será também escrito o *status* daquela sessão de votação (sucesso ou abandono do eleitor). Deve ser blindado contra interferências externas e possuir uma trava que impeça a retirada do cartão pelo eleitor, sem que tenha finalizado sua votação. Um sensor mecânico no fundo do dispositivo detectará a inserção do cartão, acionará a trava, liberará o sistema para leitura da autorização e ativará os dispositivos que foram desativados para economia de energia, como *display* e impressora.

Módulo de gravação de cartão SD: usado para receber os arquivos assinados digitalmente com a lista de candidatos e onde serão gravados os arquivos com todos os votos, com registro (*log*) de operação e os $\mathcal{BU}$ inicial e final. Seu acesso externo será impedido por tampa com lacre ou selo de segurança, bem como quaisquer interfaces que não sejam de uso do eleitor no processo normal de votação. Não deve ser confundido com o leitor de cartão SD em que o sistema operacional fica armazenado, de acordo com a plataforma utilizada, no qual ficarão apenas o sistema operacional e uma cópia reserva dos dados, para fins de redundância.

Interface com o usuário: composta por uma tela de cristal líquido e um teclado matricial, representa a comunicação entre o eleitor e o sistema de votação. A tela deve ser capaz de exibir gráficos, como a foto do candidato, para conferência do eleitor, nos moldes das eleições atuais.

No modelo proposto, a mesma impressora é utilizada para impressão dos votos e dos $\mathcal{BU}$, com o intuito de reduzir os custos de produção. No entanto, os $\mathcal{BU}$ não devem ser armazenados

dentro da urna e, conforme o protocolo determina, devem ser assinados por $\mathcal{M}$ e $\mathcal{F}$ presentes. Para este propósito, a janela de observação deve ser implementada de tal forma que, ao início e ao término das votações, os mesários possam abri-la e retirar o $\mathcal{BU}$ impresso. Uma trava mecânica, preferencialmente com chave, deve impedir a abertura durante o ciclo de votação. Um sensor de fechamento detectará toda abertura, registrará em *log* e sinalizará ao sistema que não deve ser impresso um voto enquanto a abertura não for fechada novamente. Essa medida também evitará eventual atolamento do papel, no qual uma intervenção humana seja necessária, em que o mesário instruirá o eleitor como proceder, sem violar o sigilo do voto. Na posição aberta, somente os roletes que conduzem às lâminas de corte deverão ficar acessíveis, permitindo o cancelamento do material danificado e a retomada do processo. Isso significa que, mesmo que um eleitor tenha confirmado o voto, ocorrendo a abertura da janela de exibição, este será cancelado e só será reimpresso e confirmado pelo eleitor por uma segunda vez após o restabelecimento da configuração original.

Outros sensores também devem estar presentes no equipamento, em pontos estratégicos, com o propósito de garantir seu correto funcionamento. Detectores de presença de papel para impressão e de atolamento dele na saída garantem o reconhecimento de situações em que se faça necessária a intervenção humana. Sensores de abertura de áreas sensíveis, como os acessos aos cartões de memória selados, impedem o acesso e a adulteração do registro de dados durante o funcionamento do equipamento. Sensores de temperatura e de umidade visam à verificação das condições de funcionamento adequadas, e detectores de movimento registram a manipulação do equipamento durante o voto. Estes dispositivos devem ser estrategicamente posicionados e dependem da construção do próprio gabinete que acomodará o *hardware*. Todos devem sinalizar à aplicação as alterações em seu estado, permitindo o registro desses eventos para eventuais auditorias.

Além dos sensores, fazem parte dos dispositivos de segurança, de prevenção e de detecção de adulteração os lacres e os selos. Estes devem ser numerados, permitir a identificação de violação (destruindo-se ou deixando marcas em sua retirada) e ser o menos suscetíveis possível à adulteração ou à manipulação indetectável. Conforme descrito por Appel (6), muitos lacres e/ou selos são frágeis e podem ser violados ou adulterados sem detecção. O autor destaca que o uso desses dispositivos de segurança sem uma política de selagem clara e verificável e sem o treinamento dos que farão a inspeção torna-os inócuos. O Regimento Eleitoral Geral deve estabelecer os padrões mínimos de qualidade e a política de selagem a ser utilizada, em conformidade com a estrutura física dos equipamentos.

Outro mecanismo de segurança, com o intuito de prevenir a adulteração das cédulas, deve estar presente nestas. Além das opções escolhidas pelo eleitor, a cédula impressa deve conter dados da urna (número de série, zona, seção e distrito eleitorais) e um código de barras em 2D (*QR-code*) com os mesmos dados, acrescidos da assinatura digital do voto, feita com a chave da urna, para leitura automatizada, no formato JSON assinado. Assim, qualquer aplicativo, de posse

das chaves públicas, poderá validar o conteúdo da cédula e sua autenticidade, além de permitir uma apuração eletrônica, reduzindo os riscos de alteração maliciosa dos mapas de apuração. Um aplicativo para celular pode ser disponibilizado para que qualquer fiscal, durante a apuração, possa certificar-se da validade da cédula apresentada.

Em relação à criptografia, pouco é requerido além da assinatura digital das cédulas e dos arquivos gerados pela urna eletrônica e pelo sistema de gerenciamento eleitoral, para que ambos possam autenticar a origem dos dados. Como votos impressos e eletrônicos são armazenados internamente, sem transmissão via rede, não precisam ser armazenados de forma criptografada dentro da urna. No entanto, para evitar adulteração por meio de acesso direto aos dados, como apresentado na urna eletrônica indiana (113), cada voto deve ser registrado com o respectivo código de autenticação de mensagem baseado em *hash* seguro — HMAC (66), com chave compartilhada entre a urna e a autoridade eleitoral. Qualquer alteração do conteúdo é detectada pelo HMAC, desde que o atacante não tenha acesso às chaves, que, por segurança, propõe-se que estejam armazenadas em dispositivo criptográfico que faça seu gerenciamento (módulo TPM ou *smart card*).

Tendo em vista que os algoritmos de criptografia e de *hash*, bem como os tipos de chaves, dependerão do *hardware* utilizado para apoiá-los, o presente texto não especificará nenhum deles detalhadamente. As recomendações recaem sobre os elementos que afetam diretamente a segurança destes algoritmos, como o uso de uma fonte de entropia segura para semear o gerador de números aleatórios (preferencialmente em *hardware*) e o uso de geradores de números aleatórios de qualidade criptográfica. Para os algoritmos, devem ser escolhidos aqueles que permitam um comprimento de chave seguro, conforme a natureza de cada um, e, no caso de *hash*, uso exclusivo de algoritmos resistentes a colisão, que sejam mais seguros. Devem ser evitados os algoritmos e comprimentos de chave já descritos na literatura como obsoletos ou que tenham passado por criptoanálise bem-sucedida. Conforme apontado por Aranha *et al.* (7, 8), Brunazo Filho *et al.* (30) e Brunazo Filho e Gazziro (32), a não observância destes cuidados, algumas vezes tão óbvios e conhecidos pela comunidade de segurança computacional, permite que a urna eletrônica brasileira tenha algumas vulnerabilidades que poderiam ser evitadas.

Ainda com vistas ao sigilo do eleitor, observando os problemas encontrados na urna brasileira e apontados por Aranha *et al.* (7, 8), propõe-se que os votos sejam armazenados fora da ordem de votação, ou seja, embaralhados. Para este fim, no momento de carregamento dos dados na urna, o sistema deverá gerar uma base de dados com um número de cédulas em branco que seja, no mínimo, igual ao dobro dos eleitores. Em cada registro, uma *flag* marcará o uso ou não daquele registro. Cada voto será armazenado em formato JSON plano, seguido de seu código de autenticação (HMAC). Prevendo o uso de algoritmos criptográficos não probabilísticos, em cada registro haverá um número sequencial (da ordem de criação, e não de votação), que será armazenado no registro JSON do voto na forma de *hash* seguro, permitindo que cada voto tenha um código de autenticação diferente de outros com os mesmos valores. Ao habilitar o terminal

para o eleitor, uma lista de todos os registros desocupados será recuperada da base de dados e embaralhada, usando um gerador de números aleatórios, sendo um desses registros sorteado para uso. Depois que o eleitor confirmar o voto impresso, o registro será armazenado na base de dados e em sua réplica de segurança e, depois de confirmado o sucesso da operação, o terminal será desabilitado.

O uso de gerador de números aleatórios seguro tem como meta impedir que a ordem dos votos seja recuperada, violando o seu sigilo. Nenhum registro de tempo deve ser armazenado nos dados do voto, e a urna somente registrará em seus *logs* o carimbo de tempo em que o dispositivo foi habilitado e quando foi finalizado.

No modelo apresentado, com o uso de placas, tais como Raspberry Pi ou similares, um sistema operacional deve ser instalado para prover o funcionamento geral do terminal do eleitor. É possível argumentar que o uso de um sistema operacional aumenta o número de linhas de código que compõem a TCB (*Trusted Code Base*), em detrimento à implementação em microcontrolador que executaria o código diretamente, sem necessidade de um sistema operacional completo, como, por exemplo, os trabalhos de Garera e Rubin (51) e Sturton *et al.* (105). TCB, no jargão de segurança computacional, corresponde à totalidade dos mecanismos de proteção dentro de um sistema computacional, incluindo *hardware*, *software* e *firmware*, cuja combinação é responsável por garantir uma política de segurança (40). Portanto, o sistema operacional, ao implementar os mecanismos de segurança de acesso a arquivos e fornecer as bibliotecas criptográficas, compiladores e interpretadores, passa a compor uma base de código para a qual assume-se confiabilidade incondicional.

Por outro lado, pode-se considerar que implementar pessoalmente cada algoritmo criptográfico pode levar à introdução de vulnerabilidades que permitam sua criptoanálise, sendo mais conveniente usar uma implementação mais testada e conhecida, presente no sistema operacional. Confia-se em uma TCB mais testada e conferida, assumindo-se os riscos desta escolha como um compromisso entre a segurança e a conveniência. Além disso, o sistema operacional oferece diversas funcionalidades que acabariam sendo desenvolvidas no sistema, como leitura de tela para deficientes visuais, acesso a arquivos, gerenciamento de bases de dados, etc. O desenvolvimento interno não garante ausência de *bugs* ou de vulnerabilidades.

Pode-se, no entanto, mitigar os efeitos desta escolha. Por exemplo, o sistema operacional subjacente à aplicação eleitoral pode ser fortalecido em termos de segurança. As mídias podem ser criptografadas, com o objetivo de manter seu sigilo e segurança, com as chaves gerenciadas pelo TPM do sistema (7, 8). Com o uso de Linux, os parâmetros de montagem destas mídias e das partições para armazenamento temporário devem excluir a possibilidade de executar arquivos, criar arquivos de dispositivos ou com privilégios de administrador (*root setuid*), através dos quais poderia ser inserido algum tipo de *malware* ou haver a violação da segurança do sistema. As partições de sistema, contendo programas e arquivos de configuração, devem ser montadas em modo somente-leitura. As interfaces de rede, especialmente as *wireless*, devem ser desabilitadas.

Para ilustrar a viabilidade da proposta, foram cotados os valores dos componentes eletrônicos essenciais de ambos os terminais. A cotação foi realizada em diversos portais de fornecedores nacionais e internacionais, à época da elaboração do presente trabalho, sem contar os valores dos impostos e do frete das mercadorias. Todos os valores foram expressos em dólares americanos, visando minimizar as diferenças da flutuação cambial no período da cotação. A Tabela 8 apresenta o custo dos componentes para a construção do terminal do eleitor, e a Tabela 9, do terminal do mesário. Ressalta-se que não foram incluídos os valores dos gabinetes, teclados e demais insumos eventualmente necessários, uma vez que a intenção é ilustrar as estimativas para aquisição dos componentes principais. Destaca-se também que os custos referem-se ao menor lote fornecido pelo vendedor, podendo ter valores menores quando os itens são solicitados em maior quantidade, para produção em escala.

Tabela 8 – Componentes para construção do terminal do eleitor

Componente	**Valor (US $)**
Impressora térmica Masung EP800-TMP, 80mm, *auto-cutter*	200,00
Raspberry Pi 3, 1 GB RAM, *quad core*, 1200MHz	35,00
Display 7” LCD PengJi IPS PJT500C01H29-300P40N	10,00
Real Time Clock DS3231	2,20
AVR TPM Module AT97SC3204	10,00
Leitor/Gravador de cartão inteligente e RFID Syncotek SK-288	76,00
Módulo SD Card	2,00
Total:	335,20

Fonte: dados pesquisados pelo autor.

Tabela 9 – Componentes para construção do terminal do mesário

Componente	**Valor (US $)**
Arduino Uno R3	5,00
Display 4x20 Huayuan	5,00
Real Time Clock DS3231	2,20
AVR TPM Module AT97SC3204	10,00
Leitor/Gravador de cartão inteligente e RFID Syncotek SK-288	76,00
Módulo SD Card	2,00
Total:	100,20

Fonte: dados pesquisados pelo autor.

5.2.3 Auditoria Amostral dos Votos Impressos

Conforme apresentado, o protocolo eleitoral baseia-se numa sequência de ações coordenadas que visam dar transparência aos pleitos realizados, contemplando desde as fases iniciais, com o cadastro dos eleitores, até a publicação dos resultados. Propõe-se um sistema de gerenciamento

que auxilie na execução dessas atividades (Seção 5.2.1), e as urnas eletrônicas, do tipo VVPAT, com conferência do voto pelo eleitor (Seção 5.2.2).

De acordo com o apresentado no protocolo, uma etapa importante do processo é a auditoria, por meio da recontagem dos votos impressos de um grupo aleatoriamente selecionado de urnas. Segundo Hall *et al.* (55), auditorias limitadoras de risco pós-eleição restringem as chances de homologar um resultado se este não for o previsto em uma contagem completa dos votos. Têm como objetivo encontrar e corrigir resultados eleitorais incorretos, permitindo escalar a amostra à medida que sejam detectadas falhas que possam comprometer o resultado final, chegando até mesmo a uma contagem completa dos votos.

Embora o trabalho de Hall *et al.* (55) estabeleça critérios para cálculo do risco de o resultado estar incorreto, levando a uma contagem completa, os autores reconhecem que as fórmulas propostas e constantes são arbitrárias. Com fundamento nos relatos de condados e suas propostas de legislação (55), propõe-se, neste trabalho, um modelo mais estatístico para definir a quantidade de recontagem e os critérios para expansão da amostragem, até se chegar a uma recontagem completa dos votos impressos.

Considerando-se que os votos são uma população estatisticamente finita, de tal forma que não seja consideravelmente superior ao tamanho das amostras, adota-se o cálculo destas últimas com base na estimativa da proporção populacional. O cálculo do tamanho da amostra (n) é dado pela Equação 5.1 (110), tendo N como o tamanho da população (número de votos registrados pelos eleitores), $Z_{\alpha/2}$ como o intervalo de confiança, e a taxa de erro amostral desejada e p, q sendo a proporção populacional de indivíduos que estão, respectivamente, incluídos e excluídos da categoria em análise ($q = 1-p$). Como não existem estudos da homogeneidade dos indivíduos da população para determinar p e q, será assumido o valor recomendado estatisticamente de 50% para cada um (i. e., 0,5). Os valores de $Z_{\alpha/2}$ para intervalo de confiança (I. C.) de 95%, 97% e 99% são, respectivamente, 1,96, 2,17 e 2,575. A Tabela 10 correlaciona os valores propostos de acordo com a margem de vitória (diferença entre o candidato eleito e o segundo colocado), representada por m.

$$n = \frac{N \times Z_{\alpha/2}^2 \times p \times q}{(N-1) \times e^2 + Z_{\alpha/2}^2 \times p \times q} \tag{5.1}$$

Tabela 10 – Valores de erro amostral e intervalo de confiança sugeridos para margens de vitória

Margem (m)	e	**I.C.**	$Z_{\alpha/2}$
$m < 1\%$	2%	99%	$2,575$
$1\% \leq m < 2\%$	3%	97%	$2,17$
$m \geq 2\%$	5%	95%	$1,96$

Fonte: elaborado pelo autor.

Para demonstração, deve-se supor uma eleição em que 8000 eleitores tenham comparecido, lançando, portanto, N=8000 votos, e que o primeiro colocado tenha tido uma margem de vitória $m = 3\%$ a mais que o segundo colocado. De acordo com a Tabela 10, adota-se uma margem de erro amostral de 5%, com 95% de intervalo de confiança, que equivale a $Z_{\alpha/2} = 1,96$. Substituindo esses valores na Equação 5.1, a amostra **mínima** de votos que devem ser conferidos é de $n \approxeq 367$ cédulas impressas. Este total será tomado de um conjunto de urnas sorteado, após a realização da eleição, que seja igual ou superior ao total de votos e que represente as três zonas eleitorais. Por exemplo, podem ser sorteadas três urnas contendo 100 votos de docentes, 75 votos de técnicos administrativos e 300 votos de discentes, totalizando 475 votos. Quanto menor a margem de vitória, menor o erro amostral e maior o intervalo de confiança para verificação. Se, no mesmo exemplo, a margem m caísse para $0,75\%$, seriam auditados, no mínimo, 2731 votos. Este valor, comparado ao total de votos, ainda é inferior a uma recontagem completa, validando a solução tecnológica.

Considerando-se que o voto impresso é conferido e confirmado pelo eleitor, espera-se que a urna eletrônica emita um $\mathcal{BU}$ com os mesmos valores apurados manualmente. Por este motivo, todos os votos das urnas abertas devem ser auditados, não somente a amostra mínima calculada. Caso haja discrepância, aumenta-se o intervalo de confiança e reduz-se o erro amostral, passando para o próximo nível da Tabela 10. Se o nível ampliado não apresentar discrepâncias, procede-se com a correção dos resultados apurados fisicamente e encerra-se a auditoria. Se surgirem novos erros, passa-se para o nível seguinte, se houver, ou realiza-se uma recontagem completa, quando esgotados os limites propostos.

Retomando-se o primeiro exemplo, se for encontrada uma diferença entre o registro eletrônico e o físico, expande-se o intervalo de confiança para 97% e a margem de erro para $e = 3\%$. Se nesta segunda rodada forem constatados novos erros, faz-se a nova expansão, visando ao I.C. de 99% e $e = 2\%$. Se for obtida nova disparidade, expande-se finalmente para a recontagem completa de todos os votos, descartando-se os registros eletrônicos.

Com uma proposta de sistema independente de *software*, com a educação do eleitor para que realmente faça a conferência dos votos, espera-se que as recontagens completas sejam extremamente raras. Para auxiliar no processo de recontagem e reduzir erros introduzidos por falha humana, intencionais ou não, pode-se usar uma aplicação desenvolvida para leitura e validação do *QR-code* das cédulas, mostrando os resultados em um telão, para acompanhamento dos fiscais e dos candidatos, conforme previamente apresentado. O escrutinador poderá "cantar" o voto em voz alta, passando-o por uma câmera, que fará a leitura do código de barras para uma aplicação que validará a assinatura digital e decodificará seu conteúdo, publicamente.

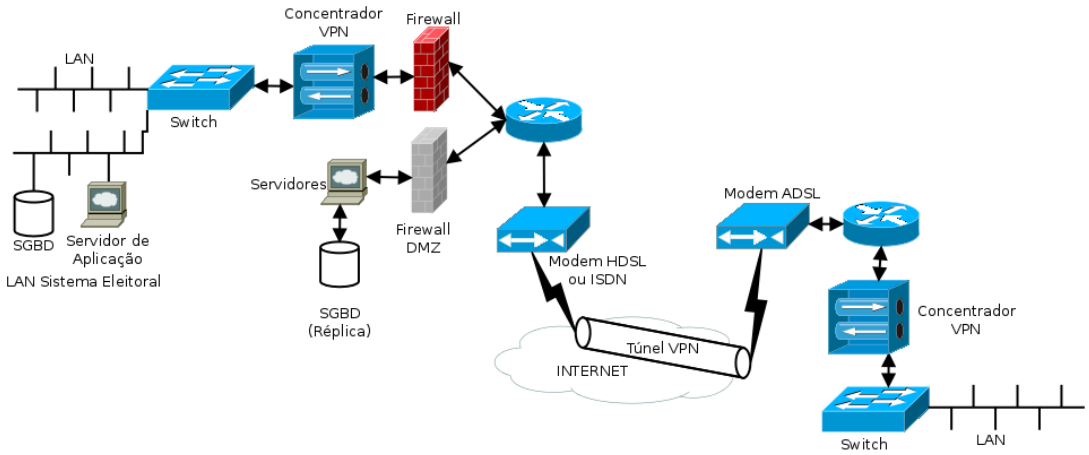
Devem ser incluídas, obrigatoriamente, todas as urnas que tenham comprovado comportamento anômalo, registrando em papel valor divergente da intenção de voto do eleitor, conforme apresentado na Seção 5.3. Nenhuma urna deve ser sorteada para auditoria antes ou durante o processo eleitoral, com o propósito de evitar que sequências de teclas escondidas no

software sinalizem que ela deve comportar-se adequadamente. Também é imprescindível que, uma vez iniciada a contagem de uma urna, todo o seu conteúdo seja auditado, sem interrupções ou intervalos, evitando a exposição do material sem acompanhamento e fiscalização, facilitando a inclusão e/ou supressão de votos e colocando em risco a confiabilidade do processo.

5.2.4 Infraestrutura de TI Necessária

A Figura 13 sumariza a proposta de infraestrutura deste trabalho, facilitando o entendimento da solução. Inicialmente, convém destacar que o tráfego de dados, das Comissões Eleitorais Locais para a Comissão Eleitoral Central, é pequeno, constituindo-se basicamente dos boletins de urna, coletados após o encerramento da votação. Desta forma, locais com acesso limitado para *upload* não são prejudicados. Assume-se que a estrutura de processamento será sediada na reitoria do IF. O tipo de rede de acesso é totalmente transparente para o usuário, não havendo necessidade de contratação de linha privativa durante o período eleitoral para o funcionamento do sistema, o que tornaria a solução mais onerosa. Foram consideradas as infraestruturas de TI típicas dos IF, conforme apresentado na Seção 3.4.

Figura 13 – Infraestrutura proposta com VPN



Fonte: elaborado pelo autor.

Além disso, a implantação do sistema requer uma rede local (LAN) para o sistema eleitoral, que será usada pelas Comissões Locais para se conectarem através da VPN. Nesta LAN estará o servidor com o sistema eleitoral (servidor de aplicação), no qual serão realizados os cadastros de eleitores e candidatos, bem como o processamento dos dados originários das urnas utilizadas nas seções eleitorais. Esta LAN deve estar em um segmento distinto do restante da rede local, através de segmentação física ou, quando esta não for possível, pelo uso de VLAN (Virtual LAN), para que não ocorra interferência, interceptação ou injeção de tráfego na LAN do sistema eleitoral.

Para a publicidade das informações, permitindo uma ampla auditoria, é necessário que haja um portal no qual estes dados sejam acessíveis ao público. Desta forma, na zona

desmilitarizada (DMZ) deve ser instalado um servidor *web* para prover acesso a estas páginas, que serão montadas dinamicamente por acesso a uma réplica da base de dados principal. É importante que a base original esteja na LAN privativa, utilizando replicação do tipo *push*, ou seja, todas as escritas são feitas na base de dados mestre, privada, e replicadas na base escrava, acessível pela aplicação *web*. Assim, em caso de qualquer comprometimento externo, a réplica não afetará a base original. Entretanto, o servidor de banco de dados utilizado não deverá ter acesso público, mesmo situando-se na DMZ. Esta restrição deve ser garantida nas regras do *firewall* de borda, que gerencia o acesso para a rede interna.

Para a manutenção do rol eleitoral, no entanto, deve ser disponibilizado acesso para que o eleitor possa cadastrar sua senha de votação, a partir do portal público. Este recurso pode ser implementado por meio da execução de *web services* no sistema eleitoral original, que permitam o acesso somente à atualização do registro do eleitor. Caso contrário, seria necessário estabelecer um ponto de atendimento em cada distrito eleitoral, com o propósito de realizar as atualizações dos dados pela autoridade eleitoral.

Observa-se ainda, na Figura 13, que foi representada apenas a conexão entre reitoria, à esquerda, e um *campus* com poucos recursos, através de rede de acesso ADSL, com o intuito de demonstrar que não são exigidos equipamentos dispendiosos para sua execução. Além disso, o concentrador VPN, como dito anteriormente, pode ser um módulo do *firewall* dedicado ou até mesmo um PC com uma implementação do IPsec para fazer a "discagem" e o estabelecimento do túnel criptográfico, como previamente estabelecido.

No momento em que a Comissão Eleitoral Local for utilizar os sistemas do servidor de aplicação central, é estabelecido um túnel criptográfico, empregando chaves previamente estabelecidas na configuração do IPsec, em conformidade com a especificação da arquitetura. A partir deste momento, o usuário terá acesso à rede privada da reitoria, como se estivesse presente na própria LAN, acessando todos os recursos, especialmente o servidor de aplicação.

Além da segurança da conexão, é oportuno destacar que o gerenciamento centralizado de um único servidor de aplicação facilita a execução da política de segurança do processo, reduzindo o número de pontos de vulnerabilidade. Para ter acesso ao sistema, além das credenciais de usuário, é necessário o uso de um equipamento que possua as chaves criptográficas da VPN, dificultando o acesso não autorizado e as tentativas de comprometimento do processo.

O uso de VPN permite que o sistema eleitoral seja executado em um servidor de aplicação central, facilitando o gerenciamento. Além disso, a solução utiliza padrões públicos disponíveis para VPN, dispensando *hardware* dedicado e soluções proprietárias e onerosas. Ao mesmo tempo, permite que as informações públicas sejam acessadas, sem comprometimento ou necessidade de acesso à aplicação principal. Os mecanismos de replicação e de gerenciamento da base de dados, por não estarem diretamente ligados à infraestrutura de TI, não fazem parte deste texto.

A segurança da infraestrutura proposta reside, principalmente, no gerenciamento das chaves e na configuração segura dos equipamentos. O ponto mais forte, como já salientado, é a possibilidade de aproveitar a estrutura atual, sem necessidade de aporte de capital na aquisição de novos equipamentos.

5.3 Análise da Segurança da Proposta

As Seções 5.1 e 5.2 apresentaram a proposta do protocolo eleitoral e detalhes do sistema de informação que lhe dará suporte, incluindo as urnas eletrônicas. Na presente seção, são analisados os requisitos de segurança, previamente apresentados na Seção 4.4, e como a proposta busca atendê-los.

O requisito de **auditabilidade** é garantido pela proposta, ao determinar que todos os dados sejam públicos, para conferência da comunidade. Desde a elaboração das listas de eleitores, todos os dados podem passar por escrutínio público em busca de erros e inconsistências. O sistema de gestão eleitoral e as urnas eletrônicas possuem seu próprio registro de *logs*, implementando medidas que impeçam a adulteração indetectável. Ainda neste requisito, a trilha de auditoria do voto impresso não é apenas gerada, sendo previstos, no protocolo, os procedimentos para sua correta utilização.

A **autenticação** do eleitor foi endereçada na proposta em dois momentos distintos. No primeiro, ao publicar o rol de eleitores ($\mathcal{E}$), permite-se que cada eleitor e_i cadastre uma senha para uso no momento da votação. Nesta etapa, utiliza-se um protocolo *challenge-response* para autenticação em duas fases, em que o eleitor deve comprovar conhecimento dos dados pessoais e a posse do endereço eletrônico para o qual será enviado o *token* de autenticação. No segundo momento, no próprio dia da votação, esta senha é utilizada por e_i para obter a liberação do terminal do eleitor. Destaca-se que, nesta ocasião, a autenticação é feita em duas ou três fases. A primeira é a identificação civil, utilizando documento oficial com foto. A segunda, com a senha cadastrada na atualização de $\mathcal{E}$, e a terceira, opcional, por meio de biometria em concomitância com a senha.

A **certificabilidade** está presente na especificação do *hardware* e *software* propostos. Os diversos requisitos funcionais podem ser mapeados em um *checklist* para inspeção do sistema eleitoral implementado, mensurando-se sua aderência à especificação, permitindo que sejam certificados e homologados para uso. Muitos dos requisitos são observáveis, como o registro impresso do voto, a publicação completa das listas, dentre outros, permitindo que membros da comunidade sem conhecimento técnico possam acompanhar o processo de certificação sem serem enganados por linguagem técnica.

Quanto à **completude**, considera-se que tenha sido satisfatoriamente atendida, tendo em vista que o registro dos votos é feito mediante confirmação do eleitor, tanto em via eletrônica quanto física. O registro eletrônico prevê redundância no armazenamento, utilizando mídias

diferentes, e possui também a forma consolidada do $\mathcal{BU}$. Em caso de falhas, as cópias redundantes podem ser recuperadas e analisadas. O registro impresso também constitui forma de redundância, independentemente de *software*, podendo estabelecer, de forma fidedigna, a intenção do eleitor.

Um requisito que merece atenção refere-se à **confiabilidade/robustez** do sistema, que demanda que este funcione sem comprometimento do voto, independentemente de falhas do sistema ou da coalizão de agentes maliciosos. Quanto ao comprometimento do voto, reitera-se que há redundância lógica e física dos votos do eleitor. Com a separação entre os terminais e o processamento realizado em cada um, é possível, como já apresentado, adicionar ou substituir um terminal de eleitor sem a necessidade de transferência de dados, bastando estabelecer uma chave HOTP entre o terminal do mesário e o novo terminal do eleitor. Assim, acredita-se que o sistema tenha, em termos de *hardware* e *software*, um elevado nível de confiabilidade.

Quanto ao risco de coalizão, esta pode ocorrer em todas as etapas do processo. A publicidade dos dados e dos atos é um mecanismo de inibição das ações de má-fé da autoridade eleitoral, caso tente fraudar lista de eleitores aptos ou excluir um candidato do processo. Este último é impedido pela impressão do $\mathcal{BU}$ inicial contendo os nomes de todos os candidatos cadastrados no dispositivo, que poderá ser impugnado caso detecte-se a ausência de nomes no início da votação. A possibilidade de instalação deliberada de *malware* para alterar o voto registrado é combatida com o seu registro impresso, conferido pelo eleitor.

Neste último caso, uma ressalva deve ser registrada e acrescentada ao protocolo. Entre as razões apresentadas pelo TSE para a não utilização do voto impresso nas eleições brasileiras, encontra-se o risco de um eleitor impugnar a urna alegando que o voto impresso não corresponde aos candidatos que tenha escolhido (27). Na impossibilidade de conferência dos mesários sem violação do sigilo do voto, tal argumento justifica a ausência de registro físico conferível pelo eleitor, ao contrário das tendências mundiais. Para evitar este contratempo, delineia-se o seguinte procedimento, que pode ser adotado em qualquer seção eleitoral, na ocorrência de queixa do eleitor.

Assume-se que o eleitor e_i tenha realizado um número indefinido de tentativas e conferências do registro impresso, todas sem sucesso. Partindo-se do princípio de que a urna esteja com comportamento anômalo, introduzido por algum agente malicioso, e a presunção inicial de que o eleitor seja sincero, a mesa receptora e os fiscais iniciarão um processo de validação. Inicialmente, sem observar o registro atual feito por e_i, este será instruído por m_p a rejeitar o voto atual e iniciar um novo ciclo de votação, para proteger sua privacidade. Com uma câmera, necessária devido à destruição dos votos cancelados, que pode ser o próprio *smartphone* de um dos membros de $\mathcal{M}$ ou equipamento provido pela autoridade eleitoral, registram-se todas as ações de inspeção:

1. Identificação nominal de e_i, de m_p e de f_i, f_j, ..., f_n, que acompanharão o processo, com suas respectivas autorizações para registro em áudio e vídeo.

2. Uma sequência de 3 a 5 combinações de votos é acordada entre as partes identificadas, sem relacionar o voto de e_i.

3. O m_p dita a e_i cada voto, enquanto filma as ações, até a impressão do voto.

4. Registra-se no vídeo o valor impresso da cédula, comparando-o com o resumo na tela do terminal, para cada uma das sequências acordadas.

5. Cada voto é cancelado e registra-se sua destruição, pelo visor apropriado, comprovando-se que ele não entrará no processo de apuração.

6. A ocorrência é registrada na ata da seção, e o vídeo, entregue à autoridade eleitoral, para futuras providências.

Havendo inconsistência nos valores em pelo menos um dos testes, assume-se a veracidade da alegação do eleitor, com desativação da urna, que será substituída e marcada para auditoria compulsória no período de apuração. Esta auditoria deverá ocorrer não apenas na conferência entre os registros eletrônico e impresso dos votos, verificando se estão corretos, mas também nos *logs* e nos sistemas de arquivos, em busca de adulteração do sistema, realizada por equipe com conhecimento técnico apropriado e credenciada pela autoridade eleitoral. Se os registros forem idênticos e não havendo indícios que desabonem a medida, os votos previamente encontrados poderão ser contabilizados, assumindo-se que o *malware* iniciou suas atividades após um determinado número de eleitores, com o intuito de burlar processos de auditoria antes do período de votação. Se os registros forem inconsistentes, a urna terá seu conteúdo anulado e retirado da totalização.

Se os testes tiverem resultados consistentes, sem divergência entre o valor digitado e o impresso, assume-se a possibilidade de má-fé do eleitor, que será instruído a realizar normalmente sua votação. A autoridade eleitoral, de posse do material produzido, com anuência de todas as partes, tomará as medidas disciplinares previstas em lei (no caso de servidores) ou em regulamentos disciplinares próprios para o corpo discente, sem detrimento de ações cíveis e criminais cabíveis. A má-fé será confirmada pela auditoria compulsória do terminal, nos mesmos moldes previamente descritos, quando não encontrados indícios de adulteração do sistema. Estes procedimentos permitem verificar a veracidade das alegações, ao mesmo tempo em que desencorajam o comportamento malicioso do eleitor, que poderá se sujeitar a sanções administrativas e penais por seus atos.

Retornando aos demais requisitos, o **controle de acesso** determina que apenas a autoridade eleitoral poderá acessar certos processos e/ou dados no sistema eleitoral. Este requisito é implementado na forma do cadastro de usuários e pelo uso de rede privada virtual para acesso ao sistema de gerenciamento. Demais usuários acessam o sistema apenas por meio de portal público em uma réplica da base de dados original.

Segundo a literatura, para que seja atendido o requisito de **democracia**, devem ser atendidas a elegibilidade e a unicidade do voto do eleitor. Quanto à **elegibilidade**, a publicação das listas de votação para inspeção pública, o cadastro de uma senha eleitoral de uso exclusivo do eleitor e o próprio procedimento de identificação civil garantem que o eleitor só possa votar se estiver cadastrado no rol de eleitores de seu segmento. Na sequência do texto, a unicidade será demonstrada, comprovando que o sistema proposto atende os critérios de democracia.

O princípio da **equidade**, como requisito do sistema eleitoral, determina que a eleição não possa ser afetada por um conhecimento prévio da distribuição efetiva dos votos, influenciando a vontade do eleitor em direção ao candidato mais votado. Na presente proposta, nenhuma informação sobre os votos é liberada antes do término do período de votação. O número de eleitores que compareceram, por si só, é insuficiente para estabelecer proporções. A privacidade do voto impede que o voto real seja deduzido, mesmo por observadores externos, já que o eleitor pode registrar sua vontade de tal forma que somente ele é capaz de conhecê-la, não tendo meios para prová-la a terceiros.

Por outro lado, existem fatores para a equidade que são alheios ao sistema eleitoral. O comportamento da autoridade eleitoral e de órgãos externos, como sindicatos, diretórios estudantis, associações e autoridades externas, afetam o balanço da equanimidade, influenciando a vontade do eleitor fora do controle do sistema eleitoral. A única forma de mitigar essa desigualdade é através da proposta do Regimento Eleitoral Geral, que deve estabelecer critérios mínimos de isonomia no processo e sanções em caso de infração. Aos membros das comissões eleitorais deve ser vedada a manifestação individual e pública em favor ou em detrimento de qualquer candidato, de forma escrita, verbal ou *on-line*. O eleitor não pode ver a autoridade eleitoral como detentora de conhecimentos que não foram a público e que abonem ou desabonem algum indivíduo, sendo fundamental a isenção desta para evitar desvios no processo. As demais organizações devem assumir o papel de fiscalização ou auditoria externa, portanto, seus membros não devem se pronunciar em nome da organização, pois isso pode comprometer a percepção de isenção do ente auditor. Neste trabalho, entende-se que a fiscalização não deve recair somente sobre os fiscais designados pelo candidato, uma vez que estes não podem cobrir todo o processo. Reposicionar tais instâncias, no papel de garantir a transparência das ações dos atores do processo, é mais valioso no contexto do que saber que o sindicato x apoia o candidato c_i ou c_j. Note-se que há uma clara divisão entre as entidades e os indivíduos que as compõem. Estes podem ter suas inclinações próprias, mas, ao agir em nome de uma entidade, deve haver isenção.

Quanto ao requisito de **livre arbítrio**, todo o processo eleitoral é desenhado com a premissa do exercício facultativo do direito ao voto. Nenhum eleitor é obrigado a comparecer, embora deva ser conscientizado da importância do voto para o futuro da instituição. Ao optar por exercê-lo, o fará em uma cabine isolada, individualmente, sem pressão e sem condições de comprovar a qualquer fonte de coerção qual foi o voto registrado. A publicação, em portal, dos dados dos candidatos, propostas e demais informações relevantes, além das atividades das

campanhas dos candidatos, auxiliam-no a tomar uma decisão informada e por sua livre escolha, garantindo o atendimento desse requisito.

A **integridade ou acurácia** visa garantir que o voto registrado pelo eleitor seja o mesmo incluído na tabulação dos resultados, com exatidão. O uso de códigos de autenticação de mensagem, no registro do voto (HMAC), e as assinaturas digitais nos arquivos trocados entre os componentes buscam atestar a integridade dos dados no formato digital e a detecção de adulterações. O voto impresso e **conferido pelo eleitor**, aliado aos procedimentos de auditoria, visa salvaguardar que, mesmo que os dados sejam alterados de forma imperceptível, a vontade dele prevalecerá. Para que uma alteração seja bem-sucedida, um atacante teria que assegurar a adulteração dos registros eletrônicos antes do início do processo (instalando um *malware*, por exemplo) ou após a votação. Também deveria ser capaz de gerar os votos impressos com as mesmas características e com a assinatura digital de cada urna, substituindo-os depois da votação, antes do início das auditorias. Em todos os casos, necessitaria obter acesso ao conjunto de chaves, armazenado em *hardware* criptográfico, para gerar as assinaturas e os códigos de autenticação de mensagem, que *ad initio* assume-se ser inviável em termos tecnológicos, já que o módulo TPM não deve permitir esse acesso. É necessário também acesso físico às urnas para modificação dos votos, geração da impressão fraudulenta para substituição, enfim, um conjunto de atividades que são difíceis de serem executadas de forma rápida e indetectável sem apoio interno da autoridade eleitoral, cujos procedimentos são monitorados por toda a comunidade acadêmica.

Para prover **isenção de disputas**, o protocolo prevê a divulgação de todas as informações necessárias ao acompanhamento do processo. A comunidade poderá verificar e corrigir, em períodos estabelecidos, a lista de eleitores. Os procedimentos previstos para auditoria dos votos impressos baseiam-se em evidências físicas e conferíveis sem necessidade de conhecimentos especiais. O comportamento do sistema pode ser verificado pelo eleitor, ao certificar-se de que a impressão do voto corresponde a sua seleção prévia. Assim, todas as disputas podem ser solucionadas de forma confiável e auditável, dando transparência ao processo.

Um dos requisitos mais apontados na literatura refere-se ao conceito de **privacidade, anonimato ou sigilo**, que tem como objetivo assegurar que não existam mecanismos de associação do voto ao eleitor. A primeira medida para garanti-lo encontra-se na separação das funções e do processamento dos terminais do mesário e do eleitor, de tal forma que um não contenha os dados presentes no outro. Esta separação física impede uma ligação entre os dados das duas unidades de forma direta. Para evitar associação indireta, determina-se o uso de fontes de entropia e de geradores de números aleatórios seguros para que o voto seja registrado em uma posição aleatória da base de dados, que não possa ser recomposta na sequência real de comparecimento dos eleitores e que nenhum voto inclua carimbos de tempo que permitam o cruzamento com registros de eventos. Estes últimos, no terminal do eleitor, só devem conter a informação da liberação do terminal e do encerramento da votação, sem o valor do voto. Assim sendo, o cruzamento dos carimbos de tempo do terminal do mesário com o registro do

comparecimento do eleitor apenas comprova que, naquele momento, ele utilizou o terminal, mas não é possível associá-lo ao voto. O registro eletrônico do voto sem criptografia não viola a privacidade, uma vez que nenhum agente tem acesso à mídia, nem o seu conteúdo é transmitido por rede para qualquer destino.

Em relação ao voto impresso, todos os cuidados para manutenção do sigilo foram tomados. Primeiro, os votos são emitidos e, no caso de bobinas de papel para impressora térmica, são cortados por uma guilhotina para serem depositados na urna lacrada, que só será aberta no período de auditoria. Desta forma, não se pode afirmar com precisão a sequência do armazenamento, já que o manuseio, o descarregamento do papel para contagem e o próprio depósito feito por gravidade auxiliam o ocultamento da ordem. Podem ainda ser adicionados ao recipiente que guarda os votos impressos um mecanismo de rotação que altere a disposição das cédulas e a posição do receptáculo periodicamente, apenas construindo este último em formato cilíndrico e provido de uma tampa com rolamentos que permitam que gire sem romper o lacre ou desconectá-lo da entrada do papel.

Ao eleitor não é permitido o manuseio do voto impresso, que será exibido somente por um visor transparente. Desta forma, ele não poderá fazer marcações que comprovem, em tempo de auditoria, que aquele voto lhe pertence, como nas eleições com cédulas impressas. A ausência de manuseio físico também impede que a impressão digital do eleitor fique marcada no papel, podendo ser analisada com conhecimentos rudimentares de Química e comparação de registros dos eleitores.

Com o objetivo de prover os mecanismos de **proteção contra ameaças externas**, o presente trabalho propõe que o sistema operacional inclua ferramentas de detecção de intrusão e de *malware*, bem como uma série, não exaustiva, de configurações no acesso aos arquivos e às mídias para minimizar os riscos de adulteração do conteúdo. Também segue a orientação de Norden (78) para que todas as interfaces de rede *wireless* sejam previamente desabilitadas nos terminais das seções eleitorais. O acesso ao sistema de gerenciamento é realizado através de rede privativa virtual e todos os dados ofertados ao público são armazenados em réplicas das bases de dados originais do sistema, fora da VPN. Na infraestrutura de TI, propõe-se o uso de *firewall* e demais recursos que minimizem os riscos. Entretanto, este é um dos requisitos que não dependem exclusivamente de soluções tecnológicas implementadas, que podem ser inutilizadas por comportamento inseguro dos usuários. A conscientização para uso seguro de soluções computacionais, com o objetivo de manter a segurança do usuário, está fora do escopo do presente trabalho, embora possa impactá-lo negativamente, caso senhas de sistemas e chaves de acesso a VPN sejam obtidas por indivíduos mal intencionados. Pouco também se pode fazer em relação a ataques de *insiders*, com legítimo acesso ao sistema, como os membros da autoridade eleitoral. A principal salvaguarda de ataques externos é o registro impresso do voto, desde que o eleitor faça uma verificação cuidadosa de seu conteúdo antes de confirmá-lo e o

processo de auditoria evite a adulteração ou contagem incorreta desse material, assegurando a completa independência de *software*.

Conforme descrito no requisito de **rastreabilidade**, o sistema deve prover meios para que o eleitor possa ter certeza de que seu voto foi registrado corretamente. Este requisito é garantido pela geração do voto impresso, conferido pelo eleitor, que pode ser recontado tantas vezes quantas forem necessárias para certificar que o resultado do pleito está correto. A inclusão de assinatura digital, em código de barras 2D, utilizando chave guardada em dispositivo criptográfico dedicado dificulta a possibilidade de terceiros adulterarem os votos impressos, se não tiverem acesso à chave específica da urna.

O requisito de **segurança de transmissão de dados** ocupa-se da garantia de que a confidencialidade dos eleitores seja preservada durante a transferência de dados. Entre os terminais da seção eleitoral, não há comunicação da identificação do eleitor, apenas dos códigos de liberação de terminal e do *status* final daquela votação (sucesso ou abandono). Entre os terminais e o sistema de gerenciamento, durante o período de votação, não há nenhuma conexão, e os dispositivos permanecem com interfaces de rede, caso existam, desabilitadas. O conteúdo das mídias, que será informado no sistema eleitoral, constitui-se basicamente do boletim de urna, com os totais de votos recebidos por candidato, sem associá-los aos eleitores. Da mesma forma, a lista de presença eletrônica do terminal do mesário fornece informações ao sistema de gerenciamento eleitoral sobre a presença ou abstenção do eleitor e, no caso da primeira, se ele registrou o voto com sucesso ou abandonou o processo sem fazê-lo. Além disso, todos os arquivos transferidos entre sistemas são assinados digitalmente e validados antes da inclusão na base de dados, podendo ser convalidados por evidências físicas (votos e listas de presença impressos).

Para que o eleitor não seja influenciado a vender o seu voto em troca de qualquer tipo de vantagem ou benefício, a literatura recomenda votação **sem comprovantes** ou com **incoercibilidade**. Ambos os conceitos são mapeados na impossibilidade de o eleitor prover evidência física (recibo ou comprovante) da forma em que votou, para apresentação a terceiros. Sem a capacidade de comprovar o voto, desestimulam-se a compra e a venda de sufrágio, pois não há garantias da contraprestação do acordo por parte do eleitor. Ao impedir que este possa manusear o voto, assinalando-o de alguma forma, ele fica privado de mecanismos para comprovar, durante a apuração, que cumpriu sua parte no conchavo, mesmo que tal marcação invalide o voto, caso seja detectada. Ao eleitor também deve ser requerido que se dirija ao terminal de votação sem portar dispositivos que registrem o voto, como celulares, câmeras e similares. Todavia, esta ação é externa à solução e, conforme apontado por Benaloh (14), praticamente inócua, à medida que dispositivos móveis e ubíquos surgem a cada dia, como os dispositivos *wearables*, não obstrutivos, tornam-se disponíveis no mercado. Dentro do limite tecnológico da solução, este requisito é atendido, mas no que tange ao eleitor, uma ação conjunta e atenta dos mesários e

dos fiscais é a única solução disponível com baixos custos, já que a instalação de detectores para escanear os eleitores em cada seção eleitoral torna-se dispendiosa.

Para garantir a **solidez**, da forma definida na literatura, só se registra o voto confirmado pelo eleitor após recolhimento da via impressa. O registro eletrônico traz, embutidos, mecanismos para detectar sua violação, como códigos de verificação, impedindo que uma adulteração deliberada dos registros passe despercebida. Os votos impressos, que não sejam validados pelo eleitor, são imediatamente destruídos, não sendo recolhidos para contagem, evitando sua inclusão na apuração, seja de forma intencional ou por desatenção. O registro redundante permite convalidar e recuperar os valores corretos, registrados pelo eleitor, garantindo a solidez dos resultados.

Conforme descrito no requisito de democracia, é necessário garantir também a **unicidade, exatidão ou cédula não reutilizável**. No modelo proposto, após a autenticação do eleitor para o critério de elegibilidade, o terminal do mesário emitirá um código de liberação do terminal do eleitor, o qual inclui uma senha de uso único (HOTP) com o intuito de impedir que a mesma autorização seja utilizada mais de uma vez (ataque de repetição). O leitor do cartão deve possuir também uma trava física, que só libere sua retirada após a concretização do voto ou o total abandono do eleitor, invalidando o código emitido. Cada senha HOTP é gerada por uma chave compartilhada entre os terminais, e sua aleatoriedade impede a determinação do valor seguinte ou a sua validação em um terminal diferente daquele a que foi destinada. Também se prevê, na elaboração das listas de eleitores, a detecção destes em zonas eleitorais diferentes, ou seja, membros de dois ou mais segmentos simultaneamente. Neste caso, o sistema deve alocá-los em apenas uma zona eleitoral, e a validação pública permite detectar seu comportamento correto. Desta forma, garante-se que cada eleitor é habilitado para registrar uma única cédula por eleição, desde que seja elegível para tal ato.

Em termos de **verificabilidade**, pode-se observar o atendimento da verificabilidade individual, na qual o eleitor confere o registro impresso de seu voto, e da forma universal, uma vez que toda a comunidade pode verificar os resultados do pleito. Esta verificabilidade universal inicia-se com a emissão dos $\mathcal{BU}$, afixados nas entradas das seções eleitorais após o término da votação. Continua na sua replicação, no $\mathcal{BB}$ do portal do sistema de gerenciamento, em que todos podem conferir se os valores atribuídos à seção correspondem ao verificado na porta. Por fim, concretiza-se nos procedimentos de auditoria, em que os votos impressos podem atestar o comportamento adequado do sistema ou, em caso de detecção de qualquer inacurácia, restaurar o resultado verdadeiro por meio da recontagem completa destes registros. Ao término da votação, os arquivos com os votos individuais (equivalentes ao RDV da urna brasileira) são carregados para o sistema de gerenciamento, que os torna públicos, permitindo que o total seja comparado com o registro individual, por seção eleitoral.

Na Seção 4.2, foram apresentadas algumas das fraudes conhecidas. Embora uma lista exaustiva seja praticamente de concepção inviável, pode-se analisar como as propostas deste trabalho ajudam a mitigar sua ocorrência.

Inicialmente, a fraude do eleitor fantasma só subsiste se houver possibilidade de adulteração do cadastro eleitoral. A publicação das listas antes do período de votação contribui para minimizar sua incidência. Ao perceber um nome em uma lista em que não deveria estar, qualquer indivíduo poderá solicitar sua retirada, visando à correção dos arrolamentos. Da mesma forma, o eleitor pode verificar se está na lista e questionar sua ausência, que o tornaria inelegível para exercer o direito ao voto. A detecção de duplicidade em segmentos também coíbe a execução desta fraude, já que o eleitor não poderá registrar mais de um voto e beneficiar-se deste fato. Para eficácia da proposta, é necessário um trabalho de conscientização e de valorização desta verificação das listas, especialmente em segmentos compostos por muitos eleitores, como o discente, em que se torna difícil conhecer a validade da pertinência de cada um, exceto para aqueles estudantes mais próximos. Em segmentos menores, é mais fácil perceber a presença de nomes espúrios. Para auxiliar o processo de validação, podem-se incluir dados como curso e turma dos discentes, organizando-os nestas unidades, com o registro individual da seção em que o voto será exercido, em vez da listagem por seção eleitoral, que também é publicada e fica disponível para assinatura durante a votação. Dados similares, como departamentos, setores, etc., podem ser associados aos eleitores que pertencem ao quadro de servidores, facilitando a localização e verificação dos nomes. A escolha entre os formatos de listagem pode ficar a critério do consulente, como parâmetro da interface, que pode mudar de listagem alfabética para os demais formatos em tempo de execução.

A fraude de clonagem de urna eletrônica pode ser minimizada pela adoção de números de série em *hardware*, não modificáveis por *software*. Cada vez que os dados são gerados, com registro impresso ou digital, associa-se o número de série de cada equipamento, que também deve estar estampado em seu gabinete. Atas de seção eleitoral e $\mathcal{BU}$ devem incluir estes números, uma vez que são assinados pelos mesários e fiscais presentes, dificultando a troca posterior do equipamento, além de permitir a qualquer indivíduo, durante a votação, verificar se o equipamento em que vai votar corresponde ao que foi informado pela autoridade eleitoral. Para este propósito, a listagem das seções eleitorais deve incluir o número identificador do equipamento alocado, e qualquer alteração, como os casos de substituição previstos no protocolo, precisa ser devidamente registrada em ata e convalidada pelos fiscais.

As fraudes do voto de cabresto e de compra de votos, em seu cerne, dependem da habilidade de coerção do atacante. Medidas como a separação física dos terminais, publicação do código-fonte do sistema eleitoral para escrutínio público, ausência de comprovantes do voto ou da sua manipulação física, que permitam associar o eleitor a um voto específico, auxiliam na redução da eficácia destas fraudes. Quanto mais seguro o eleitor se sentir em relação ao sigilo efetivo do voto, menor o poder de coerção do atacante. Sem mecanismos para comprovar o voto,

o eleitor também fica sem moeda de troca para vendê-lo e obter vantagens, reduzindo a incidência deste tipo de fraude. O que geralmente distingue uma fraude da outra é que a primeira baseia-se, principalmente, no medo e na perseguição, e a segunda, na obtenção de vantagens percebidas pelo eleitor. A forma mais eficaz de combatê-las, entretanto, é atacando suas fundações, por meio da educação e da conduta ética.

Um detalhe importante da implementação proposta refere-se ao mapeamento dos votos brancos e nulos para valores com os dígitos iguais a zero. Esta medida dificulta as fraudes citadas, pois o agente da coerção ou da compra de votos, mesmo tendo determinado um valor que o eleitor deveria digitar em um dos cargos que não lhe interesse o resultado, não poderia fazê-lo. Mesmo que o eleitor digite o número solicitado, ao serem publicados os registros de votos de cada seção, o fraudador não poderá encontrá-lo, pois todos foram mapeados para o mesmo valor.

O engravidamento de urna é uma fraude que pode ocorrer em qualquer modalidade desta, lançando-se votos de eleitores ausentes. Seu combate ocorre por meio da autenticação do eleitor. A proposta apresentada é eficaz, uma vez que o eleitor só se habilita para votar após digitar uma senha que tenha cadastrado previamente. Como se deve prever que nem todos farão o cadastramento da senha, um valor individual pode ser gerado a partir de informações não públicas, como parte do número do CPF ou da data de nascimento, por exemplo. Por não público entende-se que estes dados não devem estar na lista de eleitores nem serem facilmente consultados pelos mesários em sistemas da instituição aos quais tenham acesso. Esta abordagem é mais eficaz que a utilizada na urna brasileira, que libera o acesso por meio do número do título de eleitor (presente na lista da seção). Alguns equipamentos mais recentes incluíram teste biométrico, com leitura da impressão digital, que se torna inócuo, uma vez que, em caso de falha, o presidente da mesa receptora pode habilitar o eleitor manualmente. Esta habilitação oportuniza o engravidamento da urna, pois é independente do eleitor e pode ocorrer por conluio dos mesários e aquiescência (ou ausência) dos fiscais.

Ao transferir para o eleitor o controle completo do tempo de votação, impede-se o golpe do eleitor anulado, da forma como foi descrito. O mesário não tem mais o poder de utilizar seu terminal para impedir que um eleitor conclua a votação. O terminal do eleitor controlará o tempo de uso, utilizando um *timer* para impedir que uma votação permaneça aberta caso o eleitor abandone a votação. Em situações em que o eleitor precise, de forma legítima, de maior tempo para votar, ele poderá estendê-lo até que conclua com êxito seu intento. Aos mesários são permitidos apenas a orientação verbal e o acompanhamento das dificuldades do eleitor, se necessário. O uso de trava no leitor do cartão de habilitação também impede que um eleitor seja desabilitado no meio do processo, retirando-se o cartão da unidade.

Uma fraude que pode surgir por ação deliberada e dolosa da autoridade eleitoral é o denominado golpe do candidato nulo. Nele, os dados de um candidato não são introduzidos em um ou mais terminais de votação, mapeando-o para voto nulo. A impressão do $\mathcal{BU}$ inicial (conhecido no TSE como zerésima) é uma medida efetiva de combate, desde que haja fiscalização

ativa. Se um nome não consta no boletim inicial, o dispositivo deve ser impugnado e substituído antes do processo de votação se iniciar. Este propósito do $\mathcal{BU}$ inicial é muito superior à alegada verificação de que todos estão com os votos zerados (origem do epíteto "zerésima"), que pode ser facilmente produzido via *software*, sem meios de validação externa.

A adulteração dos programas da urna eletrônica é uma fraude contra os equipamentos de votação, na qual um programa malicioso é introduzido para alterar o comportamento correto do dispositivo. Na presente proposta, esta fraude é mitigada pelos requisitos de proteção contra ameaças externas, integridade ou acurácia e confiabilidade/robustez, previamente discutidos. Aplicando-se ainda os princípios de independência de *software*, esta fraude também torna-se inócua, desde que o registro físico do voto seja válido e conferido pelo eleitor.

A única fraude mencionada, que ocorre no tempo de totalização, é a adulteração dos mapas de votação. Ela pode acontecer caso a mesa escrutinadora, deixada sem fiscalização, altere os mapas de votos na expectativa de que não seja feita uma recontagem. Além do risco de o eleitor impugnar a urna sob alegação do registro incorreto do voto, previamente endereçado nesta seção, o TSE alega que o registro impresso permite o retorno desse tipo de fraude (27). Esta, no entanto, pode suceder até mesmo na urna eletrônica brasileira, se o boletim de urna for emitido com valores adulterados ou for substituído após a eleição, não dependendo de fatores humanos. Para evitar, na fase de auditoria, que mapas fraudulentos sejam criados, este trabalho propõe o uso de leitura eletrônica das cédulas, acompanhada pelo anúncio verbal do escrutinador (ato corriqueiramente denominado "cantar o voto"). Todas as cédulas são emitidas com um código de barras 2D (*QR-code*) com os valores do voto e da assinatura digital da urna, com o propósito de autenticar sua emissão. Estes dados são também emitidos em texto claro, de tal forma que os fiscais igualmente podem validar o registro usando uma aplicação por meio da câmera de um celular (auditoria do sistema de leitura eletrônica) e por inspeção visual.

5.4 Reflexões Finais

O presente capítulo apresentou o protocolo eleitoral proposto, os requisitos dos sistemas em *hardware* e *software*, de infraestrutura para sua implantação, bem como os procedimentos de auditoria. Por fim, fez uma análise dos requisitos não funcionais de segurança, previamente apresentados na revisão de literatura (Seção 4.4), e das fraudes eleitorais endereçadas (Seção 4.2), à luz da proposta.

Pôde-se observar que os requisitos de segurança, dentro dos limites tecnológicos da solução, foram satisfatoriamente atendidos. As fraudes, quando não possível ter mitigação completa, i. e., serem totalmente evitadas, tiveram seus riscos ou fatores desencadeantes minimizados. Portanto, em termos de segurança computacional, pode-se afirmar que foi apresentada solução satisfatória para a execução do processo eleitoral.

Foi também proposto um modelo estatístico para auditoria por apuração amostral. Embora projetado para evitar uma recontagem de todos os votos, permite detectar falhas e ampliar a amostra, caso necessário, podendo chegar a uma recontagem completa, se houver indícios que demonstrem sua inevitabilidade. O registro impresso do voto, quando devidamente conferido pelo eleitor, é a chave para o sucesso do protocolo e para garantir que, mesmo que o *software* apresente falhas, o processo possa chegar a termo satisfatoriamente.

Por fim, o êxito da proposta também depende do estabelecimento de um Regimento Eleitoral Geral, aprovado pelo órgão colegiado máximo da instituição, que regulamente todas as atividades. Deve contemplar os procedimentos, os direitos e as obrigações de cada um dos atores do processo, além de estabelecer as sanções em casos de abusos ou descumprimento das normas.

6 Conclusões

O presente trabalho apresenta uma proposta de sistema de votação eletrônica para instituições federais de educação superior. Após ampla revisão bibliográfica e documental, analisando a legislação pertinente à matéria, foi apresentado um protocolo que atende de forma satisfatória os requisitos legais e de segurança, como contribuição primária.

O trabalho estruturou-se em três objetivos específicos. O primeiro compreendia estudar os processos eleitorais existentes em uma instituição de ensino, suas características e regulamentações. Este objetivo foi parcialmente alcançado, conforme apresentado, pois não foi concedida vista aos processos eleitorais, solicitada através da Lei de Acesso à Informação. A análise dos procedimentos foi restrita à legislação que rege os processos de consulta à comunidade, sem investigação de uma instância específica para comparar as linhas de tempo das atividades e os tipos de situações que todos os atores expõem em recursos, violações de conduta e dúvidas comuns. Este fato foi abordado na Seção 6.1.

O segundo e o terceiro objetivos deste trabalho incorporavam a identificação do protocolo, atores e demais informações necessárias para propor um sistema de informação que ofereça suporte ao protocolo em proposição. Estes objetivos foram plenamente alcançados, sendo apresentado um protocolo que compreende todas as atividades de um processo eleitoral complexo e com severa restrição de tempo para conclusão. Foram apresentados os requisitos funcionais e não funcionais necessários à implementação desse sistema, tanto para gerenciamento quanto para a votação propriamente dita, com foco sempre voltado à segurança e à auditabilidade. Propôs-se ainda a elaboração de um Regimento Eleitoral Geral que atenda às especificidades de cada instituição, respeitando-se sua autonomia administrativa e sua própria cultura. Esse regimento também contribui com a redução do tempo dispendido em sua construção, durante o processo de consulta à comunidade, e repetido a cada quatro anos, dentro do exíguo prazo para realizar toda a eleição. A elaboração prévia permite uma ampla discussão com a comunidade acadêmica e, consequentemente, maior legitimidade e qualidade da regulamentação.

A adoção da presente proposta implica não apenas na criação de regulamentações, mas na capacitação de todos os atores envolvidos. O sistema de gerenciamento e os próprios terminais são elementos que devem ser operados com destreza para que não sejam inseridas informações que venham a comprometer o bom andamento do pleito. Não basta apenas a disponibilização de manuais técnicos das aplicações, as comissões eleitorais e os mesários precisam ser treinados na realização de suas atividades. Isso implica em uma preparação das equipes de Tecnologia da Informação da instituição para que possam prestar treinamento e auxílio em todas as fases do processo. Quanto à logística, existem poucas alterações em relação ao processo em papel, no que se refere à mobilização e distribuição de material e de recursos humanos.

6.1 Limitações da Pesquisa

O presente trabalho produziu, como artefato, um protocolo eleitoral para as instituições de educação superior, conforme previamente estabelecido neste capítulo. Uma de suas limitações constitui-se, no momento, no fato de não haver uma instanciação do protocolo para sua validação. Foram observadas as restrições de tempo impostas pela legislação vigente para estabelecer um modelo flexível e exequível dentro destas restrições, sendo necessário validá-las em uma eleição real, submetida a um calendário acadêmico com todas as suas especificidades.

Inicialmente, propunha-se a análise documental de processos eleitorais previamente executados em um IF, com o intuito de levantar dados que corroborassem com a construção dessa linha de tempo. Entretanto, conforme já apresentado, a instituição usada como referência não forneceu as cópias solicitadas, impedindo que as linhas de tempo reais fossem estabelecidas e usadas como um critério de aperfeiçoamento do modelo. O acesso foi postergado com inúmeras justificativas e, ao final, a promessa de envio não chegou a acontecer.

Todavia, essa postergação ao acesso, que se prolongou até o recurso em segunda instância e não se concretizou, indica uma necessidade de maior transparência nos processos administrativos. A principal alegação referia-se à dificuldade de manusear um processo com mais de vinte mil páginas. Como contribuição secundária, propõe-se que seja adotado um sistema de gerenciamento de autos para este fim específico e de outros processos que tramitam nos órgãos públicos. Há uma iniciativa do Tribunal Regional Federal da 4ª Região (TRF4), denominada *SEI!*[10] (Sistema Eletrônico de Informações), com todas as funcionalidades para tramitação de processos e documentos em meio digital, já adotada inclusive pelo Ministério da Educação. Este sistema, caso empregado, permitiria o acesso a qualquer processo que tenha tramitado por meio dele com plena segurança e transparência. Por ser desenvolvido por órgão público, está disponível no Portal de *Software* Público Brasileiro e pode ser obtido gratuitamente por meio de convênio com o TRF4. Atividades como envio de fichas de inscrição, interposição de recursos, publicação de decisões, atas, etc. podem ser feitas pelo sistema, utilizando assinaturas digitais, desonerando o sistema de gerenciamento eleitoral dessa responsabilidade.

6.2 Trabalhos Futuros

Como trabalhos futuros, vislumbra-se a implementação em *hardware* e *software* da solução proposta. Além dos aspectos de segurança, deseja-se que a solução seja economicamente viável, para que se torne exequível. Foram apresentadas as estimativas de custos dos principais componentes para prototipação, que demonstram a viabilidade da proposta.

Também é possível perceber que, adaptados os pontos necessários, o presente trabalho pode permitir uma verificabilidade fim a fim pelo eleitor, através da emissão de comprovantes

[10] SEI!: https://softwarepublico.gov.br/social/sei. O nome é grafado com ponto de exclamação no original.

para auditoria da apuração propriamente dita. Também é possível adaptar os requisitos para que, com maior ou menor esforço, a solução se ajuste a outros tipos de processos eleitorais.

Considerando as limitações apresentadas na Seção 6.1, contempla-se também a possibilidade de ampliar o sistema de gerenciamento eleitoral para que este possa gerar os documentos no SEI!, agregando suas funcionalidades. Desta forma, os sistemas seriam integrados, e a geração dos artefatos do processo eleitoral ocorreria sem retrabalho por parte da autoridade eleitoral.

Referências

1 ADESHINA, S. A.; OJO, A. Towards Improved Adoption of e-Voting: Analysis of the Case of Nigeria. In: INTERNATIONAL CONFERENCE ON THEORY AND PRACTICE OF ELECTRONIC GOVERNANCE (ICEGOV 2014), 8th, Guimarães, Portugal. **Proceedings...** New York, NY, USA: ACM, 2014. (ICEGOV '14, 8th), p. 403–412. DOI: 10.1145/2691195.2691255.

2 ADIDA, B.; RIVEST, R. L. Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting. In: ACM WORKSHOP ON PRIVACY IN ELECTRONIC SOCIETY, 5th, Alexandria, VA, USA. **Proceedings...** New York, NY, USA: ACM, 2006. (WPES '06, 5th), p. 29–39. DOI: 10.1145/1179601.1179607.

3 ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no Desenvolvimento de Software**: Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Rio de Janeiro: Editora Campus, 2002.

4 ALVAREZ, R. M.; HALL, T. E.; SINCLAIR, B. Whose absentee votes are returned and counted: The variety and use of absentee ballots in California. **Electoral Studies**, v. 27, n. 4, p. 673–683, 2008. DOI: 10.1016/j.electstud.2008.05.007.

5 ANDERSSON, L.; MADSEN, T. **Provider Provisioned Virtual Private Network (VPN) Terminology**. RFC-4026. [S.l.]: IETF, 2005. Disponível em: <https://tools.ietf.org/html/rfc4026>. Acesso em: 15 mar. 2016.

6 APPEL, A. W. Security Seals on Voting Machines: A Case Study. **ACM Transactions on Information and System Security (TISSEC)**, v. 14, n. 2, 18:1–18:29, 2011. DOI: 10.1145/2019599.2019603.

7 ARANHA, D. F.; KARAM, M. M.; MIRANDA, A.; SCAREL, F. (In)segurança do voto eletrônico no Brasil. Edição: Maria Teresa Aina Sadek. **Cadernos Adenauer 1/2014: Justiça Eleitoral**, Fundação Konrad Adenauer, v. 1, p. 117–133, 2014. Disponível em: <http://www.kas.de/wf/doc/13775-1442-5-30.pdf>. Acesso em: 4 maio 2016.

8 ARANHA, D. F.; KARAM, M. M.; MIRANDA, A. d.; SCAREL, F. **Vulnerabilidades no *software* da urna eletrônica brasileira**. Relatório da 2ª Ed. dos Testes Públicos de Segurança do Sistema Eletrônico de Votação do Tribunal Superior Eleitoral. [S.l.], 2013. 40 p. Disponível em: <http://w3.lasca.ic.unicamp.br/media/publications/relatorio-urna.pdf>. Acesso em: 15 ago. 2016.

9 ARAÚJO, R.; CUSTÓDIO, R. F.; VAN DE GRAAF, J. A verifiable voting protocol based on Farnel (extended abstract). In: **Towards Trusthworthy Elections**: New Directions in Electronic Voting. Edição: D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. A. Ryan, J. Benaloh, M. Kutylowski e B. Adida. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. LNCS 6000, p. 274–288. DOI: 10.1007/978-3-642-12980-3_17.

10 ARAÚJO, V. M. R. H. de. Sistemas de informação: nova abordagem teórico-conceitual. **Ciência da Informação**, v. 24, n. 1, 1995. Disponível em: <http://revista.ibict.br/ciinf/article/view/610>. Acesso em: 20 out. 2015.

11 BASKAR, A.; RAMANUJAM, R.; SURESH, S. P. Knowledge-based modelling of voting protocols. In: CONFERENCE ON THEORETICAL ASPECTS OF RATIONALITY AND KNOWLEDGE, 11th, Brussels, Belgium. **Proceedings...** New York, NY, USA: ACM, 2007. (TARK '07, 11th), p. 62–71. DOI: 10.1145/1324249.1324261.

12 BAX, M. P. Design Science: Filosofia da Pesquisa em Ciência da Informação e Tecnologia. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO — ENANCIB 2014, XV, Belo Horizonte. **Anais...** Belo Horizonte: XV ENANCIB, 2014. p. 3883–3903. Disponível em: <http://www.bax.com.br/publications/artigos/design-science-filosofia-da-pesquisa-em-ciencia-da-informacao-e-tecnologia/view>. Acesso em: 10 dez. 2015.

13 BELL, S.; BENALOH, J.; BYRNE, M. D.; DEBEAUVOIR, D.; EAKIN, B.; FISHER, G.; KORTUM, P.; MCBURNETT, N.; MONTOYA, J.; PARKER, M.; PEREIRA, O.; STARK, P. B.; WALLACH, D. S.; WINN, M. STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. In: ELECTRONIC VOTING TECHNOLOGY WORKSHOP / WORKSHOP ON TRUSTWORTHY ELECTIONS, 2013, Washington, DC, USA. **Proceedings...** Washington, DC, USA: USENIX Association, 2013. (EVT/WOTE '13, 2013). Disponível em: <https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell>. Acesso em: 5 abr. 2015.

14 BENALOH, J. Rethinking Voter Coercion: The Realities Imposed by Technology. In: ELECTRONIC VOTING TECHNOLOGY WORKSHOP / WORKSHOP ON TRUSTWORTHY LECTIONS, EVT/WOTE '13, 2013, Washington, DC, USA. **Proceedings...** Washington, DC, USA: USENIX Association, 2013. Disponível em: <https://www.usenix.org/conference/evtwote13/workshop-program/presentation/benaloh>. Acesso em: 31 mar. 2015.

15 BENALOH, J.; BYRNE, M.; KORTUM, P. T.; MCBURNETT, N.; PEREIRA, O.; STARK, P. B.; WALLACH, D. S. STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System. **CoRR**, 2012. Disponível em: <http://arxiv.org/abs/1211.1904>. Acesso em: 31 mar. 2015.

16 BENALOH, J.; JONES, D.; LAZARUS, E. L.; LINDEMAN, M.; STARK, P. B. SOBA: Secrecy-preserving Observable Ballot-level Audit. In: ELECTRONIC VOTING TECHNOLOGY WORKSHOP / WORKSHOP ON TRUSTWORTHY ELECTIONS, 2011, San Francisco, CA, USA. **Proceedings...** San Francisco: USENIX Association, 2011. (EVT/WOTE '11, 2011). Disponível em: <https://www.usenix.org/conference/evtwote-11/soba-secrecy-preserving-observable-ballot-level-audit>. Acesso em: 5 abr. 2015.

17 BEN-NUN, J.; FAHRI, N.; LLEWELLYN, M.; RIVA, B.; ROSEN, A.; TA-SHMA, A.; WIKSTRÖM, D. A New Implementation of a Dual (Paper and Cryptographic) Voting System. In: INTERNATIONAL CONFERENCE ON ELECTRONIC VOTING 2012, 5th, Bregenz, Austria. **Proceedings...** Bregenz, Austria: Gesellschaft für Informatik, 2012. v. 205. (LNI, 5th), p. 315–329. Disponível em: <http://subs.emis.de/LNI/Proceedings/Proceedings205/article6748.html>. Acesso em: 5 abr. 2015.

18 BERNHARD, D.; CORTIER, V.; PEREIRA, O.; WARINSCHI, B. Measuring vote privacy, revisited. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 2012, Raleigh, North Carolina, USA. **Proceedings...** New York, NY, USA: ACM, 2012. (CCS '12, 2012), p. 941–952. DOI: 10.1145/2382196.2382295.

19 BIAGIONI, E.; DONG, Y.; PETERSON, W.; SUGIHARA, K. Practical distributed voter-verifiable secret ballot system. In: ACM SYMPOSIUM ON APPLIED COMPUTING, 2009, Honolulu, Hawaii, USA. **Proceedings...** New York, NY, USA: ACM, 2009. (SAC '09, 2009), p. 16–21. DOI: 10.1145/1529282.1529286.

20 BOGDAN, M. P. Electoral fraud: Few thoughts and insights about the phenomenon. **Cogito — Multidisciplinary Research Journal**, Bucharest, v. V, n. 01, p. 94–108, 2013. Disponível em: <http://cogito.ucdc.ro/n5/cogito-engleza29-03-2013-vol5-nr.1.pdf>. Acesso em: 5 abr. 2015.

21 BRASIL. **Decreto nº 6.986, de 20 de outubro de 2009**. Brasília: Imprensa Nacional, 2009. D.O.U., 20/09/2009, Ed. Extra, Seção 1, pp. 1–2. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/Decreto/D6986.htm>. Acesso em: 20 mar. 2016.

22 _____. **Decreto nº 7.724, de 16 de maio 2012**. Brasília: Imprensa Nacional, 2012. D.O.U., 16/05/2012, Ed. Extra, Seção 1, pp. 1–6. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm>. Acesso em: 20 mar. 2016.

23 _____. **Lei nº 11.892, de 29 de dezembro de 2008**. Brasília: Imprensa Nacional, 2008. D.O.U., 30/12/2008, Seção 1, pp. 1–3. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm>. Acesso em: 20 mar. 2016.

24 _____. **Lei nº 12.527, de 18 de novembro 2011**. Brasília: Imprensa Nacional, 2011. D.O.U., 18/11/2011, Ed. Extra, Seção 1, pp. 1–4. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 20 mar. 2016.

25 _____. **Lei nº 12.778, de 28 de dezembro de 2012**. Brasília: Imprensa Nacional, 2012. D.O.U., 31/12/2012, Seção 1, pp. 30–97. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12778.htm>. Acesso em: 20 mar. 2016.

26 _____. **Portaria nº 246, de 15 de abril de 2016**. Brasília: Imprensa Nacional, 2016. D.O.U., 18/04/2016, Seção 1, pp. 37–43.

27 _____. Tribunal Superior Eleitoral (TSE). **Por dentro da urna**. 2. ed., rev. e atual. Brasília: Tribunal Superior Eleitoral, 2010. 22 p. Disponível em: <http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/57_porDentroDaUrna1.2.pdf>. Acesso em: 4 mar. 2015.

28 _____. Tribunal Superior Eleitoral (TSE). **Resolução nº 22.685, de 13 de dezembro de 2007**. Brasília: Imprensa Nacional, 2007. p. 21–22. D.J.U., 07/02/2008, Seção 1.

29 _____. Tribunal Superior Eleitoral (TSE). **Sistema Eletrônico de Votação**: Perguntas Mais Frequentes. Brasília: Tribunal Superior Eleitoral, 2014. 24 p. Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tse-perguntas-mais-frequentes-sistema-eletronico-de-votacao>. Acesso em: 31 mar. 2015.

30 BRUNAZO FILHO, A.; CARVALHO, M. A. M.; TEIXEIRA, M. C.; SIMPLICIO JR., M. A.; FERNANDES, C. T. Auditoria Especial no Sistema Eleitoral 2014. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, XV, Florianópolis. **Anais...** Florianópolis: SBC, 2015. p. 511–522. Disponível em: <http://siaiap34.univali.br/sbseg2015/anais/WTE/artigoWTE01.pdf>. Acesso em: 5 ago. 2016.

31 BRUNAZO FILHO, A.; CORTIZ, M. A. **Fraudes e defesas no voto eletrônico**. São Paulo: All Print Editora, 2006. 96 p. Disponível em: <http://brunazo.eng.br/voto-e/livros/F&D-texto.pdf>. Acesso em: 31 mar. 2015.

32 BRUNAZO FILHO, A.; GAZZIRO, M. A. Critérios para Avaliação de Sistemas Eleitorais Digitais. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, XIV, Belo Horizonte, p. 599–610. Disponível em: <http://www.lbd.dcc.ufmg.br/bdbcomp/servlet/Trabalho?id=22339>. Acesso em: 5 abr. 2016.

33 BUDURUSHI, J.; JÖRIS, R.; VOLKAMER, M. Implementing and evaluating a software-independent voting system for polling station elections. **Journal of Information Security and Applications**, v. 19, n. 2, p. 105–114, 2014. DOI: 10.1016/j.jisa.2014.03.001.

34 CARBACK, R.; CHAUM, D.; CLARK, J.; CONWAY, J.; ESSEX, A.; HERRNSON, P. S.; MAYBERRY, T.; POPOVENIUC, S.; RIVEST, R. L.; SHEN, E.; SHERMAN, A. T.; VORA, P. L. Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy. In: USENIX CONFERENCE ON SECURITY, 19th, Washington. **Proceedings...** Washington, DC, USA: USENIX Association, 2010. (USENIX Security'10, 19th), p. 19–35. Disponível em: <http://dl.acm.org/citation.cfm?id=1929820.1929846>. Acesso em: 31 mar. 2015.

35 CARROLL, T. E.; GROSU, D. A secure and anonymous voter-controlled election scheme. **Journal of Network and Computer Applications**, v. 32, n. 3, p. 599–606, 2009. DOI: 10.1016/j.jnca.2008.07.010.

36 CHAUM, D. Secret-Ballot Receipts: True Voter-Verifiable Elections. **IEEE Security Privacy**, v. 2, n. 1, p. 38–47, 2004. DOI: 10.1109/MSECP.2004.1264852.

37 CHAUM, D.; FLORESCU, A.; NANDI, M.; POPOVENIUC, S.; RUBIO, J.; VORA, P. L.; ZAGÓRSKI, F. Paperless Independently-Verifiable Voting. In: **Revised Selected Papers**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. LNCS 7187, p. 140–157. (Lecture Notes in Computer Science, 2011). DOI: 10.1007/978-3-642-32747-6_9.

38 CHAUM, D.; RYAN, P. Y.; SCHNEIDER, S. A practical voter-verifiable election scheme. In: COMPUTER SECURITY – ESORICS 2005: EUROPEAN SYMPOSIUM ON RESEARCH IN COMPUTER SECURITY, 10th, Milan, Italy. **Proceedings**. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2005. 3679 LNCS, p. 118–139. DOI: 10.1007/11555827_8.

39 CHAVES, S. A. de; MELLO, E. R. de. O uso de um sistema de votação on-line para escolha do conselho universitário. In: XIV SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, XIV, Belo Horizonte. **Anais...** Belo Horizonte: Sociedade Brasileira de Computação, 2014. p. 634–645. Disponível em: <http://www.lbd.dcc.ufmg.br/bdbcomp/servlet/Trabalho?id=22366>. Acesso em: 5 abr. 2015.

40 COMMITTEE ON NATIONAL SECURITY SYSTEMS (CNSS). **National Information Assurance (IA) Glossary**. [S.l.]: CNSS, 2009. 103 p. Disponível em: <https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf>. Acesso em: 25 jul. 2016.

41 CRAIG, J. S.; PIERRE, J. N.; TOWNSEND, M.; HART, G. W.; COX, D. R. Toward a System of Checks and Balances for Electronic Voting Machines. In: INFORMATION SECURITY CURRICULUM DEVELOPMENT CONFERENCE, 2009, Kennesaw, Georgia. **Proceedings...** New York, NY, USA: ACM, 2009. (InfoSecCD '09, 2009), p. 142–147. DOI: 10.1145/1940976.1941004.

42 CROSS II, E. V.; MCMILLIAN, Y.; GUPTA, P.; WILLIAMS, P.; NOBLES, K.; GILBERT, J. E. Prime III: a user centered voting system. In: CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, '07, San Jose, CA, USA. **CHI '07 Extended Abstracts...** New York, NY, USA: ACM, 2007. v. 2, p. 2351–2356. DOI: 10.1145/1240866.1241006.

43 CUNHA, S. S. da; MARCACINI, A. T. R.; CORTIZ, M. A.; FERNANDES, C. T.; STOLFI, J.; REZENDE, P. A. D. de; BRUNAZO FILHO, A.; MOURA, F. V. de; CARVALHO, M. A. M. de; TEIXEIRA, M. C. **Relatório sobre o Sistema Brasileiro de Votação Eletrônica**. Brasília, 2010. 105 p. Disponível em: <http://brunazo.eng.br/voto-e/textos/CMind-1-Brasil-2010.pdf>. Acesso em: 31 mar. 2015.

44 DEMIREL, D.; HENNING, M.; RYAN, P. Y. A.; SCHNEIDER, S.; VOLKAMER, M. Feasibility analysis of Prêt à Voter for German federal elections. In: E-VOTING AND IDENTITY, 3rd, Tallinn, Estonia. **Revised Selected Papers**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. LNCS 7187. (Lecture Notes in Computer Science, 3rd), p. 158–173. DOI: 10.1007/978-3-642-32747-6_10.

45 DILL, D. L.; CASTRO, D. Point/Counterpoint: The U.S. Should Ban Paperless Electronic Voting Machines. **Communications of the ACM**, v. 51, n. 10, p. 29–33, 2008. DOI: 10.1145/1400181.1400192.

46 ESSEX, A.; HENGARTNER, U. Hover: Trustworthy elections with Hash-Only Verification. **IEEE Security and Privacy**, v. 10, n. 5, p. 18–24, 2012. DOI: 10.1109/MSP.2012.63.

47 EVANS, D.; PAUL, N. Election Security: Perception and Reality. **IEEE Security and Privacy**, IEEE Computer Society, v. 2, n. 1, p. 24–31, 2004. DOI: 10.1109/MSECP.2004.1264850.

48 FERNANDES, L. d. S. **Manifestações de territorialidade e seus impactos em um processo de integração no setor público**. 2012. Dissertação (Mestrado em Administração) – FUMEC, Belo Horizonte. Disponível em: <http://www.fumec.br/anexos/cursos/mestrado/dissertacoes/completa/leise-de-souza-fernandes.pdf>. Acesso em: 20 ago. 2016.

49 FERNANDEZ, E. B.; LA RED, D. L.; PELÁEZ, J. I. A conceptual approach to secure electronic elections based on patterns. **Government Information Quarterly**, v. 30, n. 1, p. 64–73, 2013. DOI: 10.1016/j.giq.2012.08.001.

50 GALLO, R.; KAWAKAMI, H.; DAHAB, R.; AZEVEDO, R.; LIMA, S.; ARAUJO, G. T-DRE: a hardware trusted computing base for direct recording electronic vote machines. In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 26th, Austin, Texas, USA. **Proceedings...** New York, NY, USA: ACM, 2010. (ACSAC '10, 26th), p. 191–198. DOI: 10.1145/1920261.1920291.

51 GARERA, S.; RUBIN, A. D. An Independent Audit Framework for Software Dependent Voting Systems. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY — CCS, 2007, Alexandria, Virginia, USA. **Proceedings...** New York, NY, USA: ACM, 2007. (CCS '07, 2007), p. 256–265. DOI: 10.1145/1315245.1315278.

52 GILBERT, J. E.; MARTIN, A. M.; ROGERS, G.; MCCLENDON, J.; EKANDEM, J. Hey, that's not who I voted for!: a study on touchscreen ballot design. **Interactions**, ACM, New York, NY, USA, v. 19, n. 6, p. 34–39, 2012. DOI: 10.1145/2377783.2377792.

53 GLEESON, B.; LIN, A.; HEINANEN, J.; ARMITAGE, G.; MALIS, A. **A Framework for IP Based Virtual Private Networks**. RFC-2764. [S.l.]: IETF, 2000. Disponível em: <https://tools.ietf.org/html/rfc2764>. Acesso em: 15 mar. 2016.

54 HAAS, B. Engineering Better Voting Systems. In: DOCENG'06 — ACM SYMPOSIUM ON DOCUMENT ENGINEERING, 2006, Amsterdam, The Netherlands. **Proceedings...** New York, NY, USA: ACM, 2006. v. 2006, p. 56–58. DOI: 10.1145/1166160.1166178.

55 HALL, J. L.; MIRATRIX, L. W.; STARK, P. B.; BRIONES, M.; GINNOLD, E.; OAKLEY, F.; PEADEN, M.; PELLERIN, G.; STANIONIS, T.; WEBBER, T. Implementing Risk-Limiting Post-Election Audits in California. In: ELECTRONIC VOTING TECHNOLOGY WORKSHOP / WORKSHOP ON TRUSTWORTHY ELECTIONS, 2009, Montreal, Canada. **Proceedings...** Montreal, Canada: USENIX Association, 2009. (EVT / WOTE '09, 2009), p. 1–22. arXiv: arXiv:0905.4691v4.

56 HAO, F.; KREEGER, M. N. Every Vote Counts: Ensuring Integrity in Large-Scale DRE-based Electronic Voting. **IACR Cryptology ePrint Archive**, v. 2010, 2010. Disponível em: <http://eprint.iacr.org/2010/452>. Acesso em: 31 mar. 2015.

57 HAO, F.; KREEGER, M. N.; RANDELL, B.; CLARKE, D.; SHAHANDASHTI, S. F.; LEE, P. H.-J. Every Vote Counts: Ensuring Integrity in Large-Scale Electronic Voting. In: ELECTRONIC VOTING TECHNOLOGY WORKSHOP / WORKSHOP ON TRUSTWORTHY ELECTIONS, 2014, San Diego, CA, USA. **Proceedings...** San Diego, CA, USA: USENIX Association, 2014. (EVT / WOTE '14, 2014). Disponível em: <https://www.usenix.org/conference/evtwote14/workshop-program/presentation/hao>. Acesso em: 15 abr. 2016.

58 HOKE, C. Internet Voting: Structural Governance Principles for Election Cyber Security in Democratic Nations. In: WORKSHOP ON GOVERNANCE OF TECHNOLOGY, INFORMATION AND POLICIES — GTIP '10, 2010, Austin, Texas, USA. **Proceedings...** New York, NY, USA: ACM, 2010. (GTIP '10, 2010), p. 61–70. DOI: 10.1145/1920320.1920329.

59 HOSP, B.; VORA, P. L. An information-theoretic model of voting systems. **Mathematical and Computer Modelling**, v. 48, 9–10, p. 1628–1645, 2008. DOI: 10.1016/j.mcm.2008.05.040.

60 JARDÍ-CEDÓ, R.; PUJOL-AHULLÓ, J.; CASTELLÀ-ROCA, J.; VIEJO, A. Study on poll-site voting and verification systems. **Computers and Security**, v. 31, n. 8, p. 989–1010, 2012. DOI: 10.1016/j.cose.2012.08.001.

61 JEFFERSON, D.; RUBIN, A. D.; SIMONS, B.; WAGNER, D. Analyzing Internet Voting Security. **Communications of the ACM**, v. 47, n. 10, p. 59–64, 2004. DOI: 10.1145/1022594.1022624.

62 JONES, M.; BRADLEY, J.; SAKIMURA, N. **JSON Web Signature (JWS)**. RFC-7515. [S.l.]: IETF, 2015. Disponível em: <https://tools.ietf.org/html/rfc7515>. Acesso em: 15 mar. 2016.

63 KACZMAREK, T.; WITTROCK, J.; CARBACK, R.; FLORESCU, A.; RUBIO, J.; RUNYAN, N.; VORA, P. L.; ZAGÓRSKI, F. Dispute resolution in accessible voting systems: The design and use of audiotegrity. In: INTERNATIONAL CONFERENCE VOTE-ID 2013, 4th, Guildford, UK. **E-Voting and Identify**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. 7985 LNCS, p. 127–141. DOI: 10.1007/978-3-642-39185-9_8.

64 KELLY, S.; RAMAMOORTHI, S. **Requirements for IPsec Remote Access Scenarios**. RFC-3457. [S.l.]: IETF, 2003. Disponível em: <https://tools.ietf.org/html/rfc3457>. Acesso em: 15 mar. 2016.

65 KENT, S.; SEO, K. **Security Architecture for the Internet Protocol**. RFC-4301. [S.l.]: IETF, 2005. Disponível em: <https://tools.ietf.org/html/rfc4301>. Acesso em: 15 mar. 2016.

66 KRAWCZYK, H.; BELLARE, M.; CANETTI, R. **HMAC: Keyed-Hashing for Message Authentication**. RFC-2104. [S.l.]: IETF, 1997. Disponível em: <https://tools.ietf.org/html/rfc2104>. Acesso em: 15 mar. 2016.

67 KRZYWIECKI, Ł.; KUTYŁOWSKI, M. Lagrangian E-voting: Verifiability on demand and strong privacy. In: INTERNATIONAL CONFERENCE TRUST 2010, 3rd, Berlin, Germany. **Trust and Trustworthy Computing**. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2010. LNCS 6101. (TRUST'10, 3rd), p. 109–123. DOI: 10.1007/978-3-642-13869-0_8.

68 LEE, Y.; PARK, S.; MAMBO, M.; KIM, S.; WON, D. Towards trustworthy e-voting using paper receipts. **Computer Standards and Interfaces**, v. 32, n. 5-6, p. 305–311, 2010. DOI: 10.1016/j.csi.2010.03.001.

69 LEITE, J. C.; SOUZA, C. S. de. Uma linguagem de especificação para a engenharia semiótica de interfaces de usuário. In: WORKSHOP SOBRE FATORES HUMANOS EM SISTEMAS COMPUTACIONAIS — IHC, II, Campinas. **Atas**. Campinas: Unicamp, 1999. Disponível em: <http://www.unicamp.br/~ihc99/Ihc99/AtasIHC99/art23.pdf>. Acesso em: 27 jul. 2015.

70 LI, X.; CARLISLE, M.; KWAN, A. C.; LEUNG, L.; ENEMUO, A.; ANSHEL, M. An elementary electronic voting protocol using RFID. In: IEEE WORKSHOP ON INFORMATION ASSURANCE, 2007, West Point, NY, USA. **Proceedings...** West Point, NY: IEEE, 2007. p. 234–238. DOI: 10.1109/IAW.2007.381938.

71 MANESCHY, O.; JAKOBSKIND, M. A. (Coord.). **Burla Eletrônica**. Rio de Janeiro: Fundação Alberto Pasqualini, 2002. 176 p. Disponível em: <http://brunazo.eng.br/voto-e/arquivos/BurlaEletronica.pdf>. Acesso em: 15 mar. 2015.

72 MOHEN, J.; GLIDDEN, J. The case for internet voting. **Communications of the ACM**, v. 44, n. 1, 72–ff. 2001. DOI: 10.1145/357489.357511.

73 MORAN, T.; NAOR, M. Split-Ballot Voting: Everlasting Privacy with Distributed Trust. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY — CCS '07, 14th, Alexandria, Virginia, USA. **Proceedings...** New York, NY, USA: ACM, 2007. (CCS '07, 14th), p. 246–255. DOI: 10.1145/1315245.1315277.

74 _____. Split-ballot Voting: Everlasting Privacy with Distributed Trust. **ACM Transactions on Information and System Security**, ACM, v. 13, n. 2, 16:1–16:43, 2010. DOI: 10.1145/1698750.1698756.

75 MOREIRA, A.; MAIA, L. C. G. Tecnologias da informação, mudança e administração pública. **DataGramaZero**, v. 14, n. 2, 2013. Disponível em: <http://www.luizmaia.com.br/docs/tecnologias_da_informacao_mudanca_e_administracao_publica.pdf>. Acesso em: 21 jul. 2016.

76 M'RAIHI, D.; BELLARE, M.; HOORNAERT, F.; NACCACHE, D.; RANEN, O. **HOTP: An HMAC-Based One-Time Password Algorithm**. RFC-4226. [S.l.]: IETF, 2005. Disponível em: <https://tools.ietf.org/html/rfc4226>. Acesso em: 15 mar. 2016.

77 NADAF, R. M. Modelo Brasileiro de Votação Mecatrônica Independente de Software ou Votação Mecatrônica. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, XIV, Belo Horizonte, p. 622–633. Disponível em: <http://www.lbd.dcc.ufmg.br/bdbcomp/servlet/Trabalho?id=22363>. Acesso em: 5 abr. 2015.

78 NORDEN, L. D. (Ed.). **The machinery of democracy**: Protecting elections in an electronic world. New York, NY, USA, 2006. Disponível em: <https://www.brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf>. Acesso em: 20 maio 2016.

79 OKOLI, C.; SCHABRAM, K. A Guide to Conducting a Systematic Literature Review of Information Systems Research. **Sprouts: Working Papers on Information Systems**, v. 10, n. 26, 2010. Disponível em: <http://sprouts.aisnet.org/10-26>. Acesso em: 20 out. 2015.

80 ONSHUS, B. K. R. **Secure and Verifiable Electronic Elections at NTNU**. 2006. 134 p. Master Thesis – Norwegian University of Science e Technology Department. Disponível em: <http://brage.bibsys.no/xmlui/handle/11250/262018>. Acesso em: 2 abr. 2015.

81 PALAZZOLO, D.; MOSCARDELLI, V. G.; PATRICK, M.; RUBIN, D. Election reform after HAVA: Voter verification in congress and the states. **Publius**, v. 38, n. 3, p. 515–537, 2008. DOI: 10.1093/publius/pjn013.

82 PASQUINUCCI, A. Web voting, security and cryptography. **Computer Fraud & Security**, v. 2007, n. 3, p. 5–8, 2007. DOI: 10.1016/S1361-3723(07)70033-7.

83 PATEL, B.; ABOBA, B.; DIXON, W.; ZORN, G.; BOOTH, S. **Securing L2TP using IPsec**. RFC-3193. [S.l.]: IETF, 2001. Disponível em: <https://tools.ietf.org/html/rfc3193>. Acesso em: 15 mar. 2016.

84 PAWLAK, Z. Information systems theoretical foundations. **Information Systems**, v. 6, n. 3, p. 205–218, 1981. DOI: 10.1016/0306-4379(81)90023-5.

85 PEACOCK, T.; RYAN, P. Y. A.; SCHNEIDER, S.; XIA, Z. Verifiable Voting Systems. In: **Computer and Information Security Handbook**. Edição: John R. Vacca. 2. ed. Boston: Morgan Kaufmann, 2013. cap. 69, p. 1103–1125. DOI: 10.1016/B978-0-12-394397-2.00069-6.

86 PEFFERS, K.; TUUNANEN, T.; GENGLER, C. E.; ROSSI, M.; HUI, W.; VIRTANEN, V.; BRAGGE, J. The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. In: INTERNATIONAL CONFERENCE ON DESIGN SCIENCE IN INFORMATION SYSTEMS AND TECHNOLOGY (DESRIST), 1st, Claremont, CA, USA, p. 83–106. Disponível em: <http://www.wrsc.org/sites/default/files/documents/000designscresearchproc_desrist_2006.pdf>. Acesso em: 20 dez. 2014.

87 POPOVENIUC, S.; CARBACK, R. ClearVote: An End-to-End Voting System that Distributes Privacy Between Printers. In: ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY — WPES 2010, 9th, Chicago, Illinois, USA. **Proceedings...** New York, NY, USA: ACM, 2010. (WPES '10, 9th), p. 119–122. DOI: 10.1145/1866919.1866937.

88 POST, G. V. Using re-voting to reduce the threat of coercion in elections. **Electronic Government**, v. 7, n. 2, p. 168–182, 2010. DOI: 10.1504/EG.2010.030926.

89 PROSSER, A. Transparency in eVoting: Lessons learnt. **Transforming Government: People, Process and Policy**, v. 8, n. 2, p. 171–184, 2014. DOI: 10.1108/TG-09-2013-0032.

90 RIO GRANDE DO SUL. Tribunal Regional Eleitoral. **Voto Eletrônico**: Edição Comemorativa: 10 Anos da Urna Eletrônica; 20 Anos do Recadastramento Eleitoral. 1. ed. Porto Alegre: Tribunal Regional Eleitoral do RS/Centro de Memória da Justiça Eleitoral, 2006. 102 p. Disponível em: <http://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/Voto_Eletronico.pdf>. Acesso em: 15 mar. 2015.

91 RIVEST, R. L. On the notion of 'software independence' in voting systems. **Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences**, v. 366, n. 1881, p. 3759–3767, 2008. DOI: 10.1098/rsta.2008.0149.

92 RYAN, P. Y. A. Prêt à Voter with Paillier encryption. **Mathematical and Computer Modelling**, v. 48, n. 9-10, p. 1646–1662, 2008. DOI: 10.1016/j.mcm.2008.05.015.

93 RYAN, P. Y. A. A Variant of the Chaum Voter-Verifiable Scheme. In: WORKSHOP ON ISSUES IN THE THEORY OF SECURITY — WITS, 2005, Long Beach, CA, USA. **Proceedings...** New York, NY, USA: ACM, 2005. (WITS '05, 2005), p. 81–88. DOI: 10.1145/1045405.1045414.

94 RYAN, P. Y. A.; BISMARK, D.; HEATHER, J.; SCHNEIDER, S.; XIA, Z. Prêt à voter: A voter-verifiable voting system. **IEEE Transactions on Information Forensics and Security**, v. 4, n. 4, p. 662–673, 2009. DOI: 10.1109/TIFS.2009.2033233.

95 SAAD, A.; ROSELI, M. I. M.; ZULLKEPLY, M. S. A Smart e-Voting System Using RFID Authentication Method for a Campus Electoral. In: INTERNATIONAL CONFERENCE ON UBIQUITOUS INFORMATION MANAGEMENT AND COMMUNICATION, 8th, Siem Reap, Cambodia. **Proceedings...** New York, NY, USA: ACM, 2014. (ICUIMC '14, 8th), 31:1–31:7. DOI: 10.1145/2557977.2557985.

96 SALTMAN, R. G. Computerized Voting. Edição: Marshall C. Yovits. **Advances in Computers**, Elsevier, v. 32, n. 100, p. 255–305, 1991. DOI: 10.1016/S0065-2458(08)60249-1.

97 SANTAELLA, L. **O que é semiótica?** São Paulo: Brasiliense, 1983. (Coleção Primeiros Passos).

98 _____. **Semiótica Aplicada**. reimpr. da 1. ed. de 2002. São Paulo: Pioneira Thompson Learning, 2004.

99 SELKER, T. Fixing the vote. **Scientific American**, v. 291, n. 4, p. 90–97, 2004. DOI: 10.1038/scientificamerican1004-90.

100 SIMON, H. A. **The Sciences of the Artificial**. 3. ed. Cambridge: MIT Press, 1996.

101 SPYCHER, O.; HAENNI, R. A novel protocol to allow revocation of votes in a hybrid voting system. In: INFORMATION SECURITY FOR SOUTH AFRICA CONFERENCE — ISSA, 2010, Sandton, Johannesburg. **Proceedings...** Sandton, Johannesburg: IEEE, 2010. p. 1–8. DOI: 10.1109/ISSA.2010.5588262.

102 SRISURESH, P. **Secure Remote Access with L2TP**. RFC-2888. [S.l.]: IETF, 2000. Disponível em: <https://tools.ietf.org/html/rfc2888>. Acesso em: 15 mar. 2016.

103 STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. 5. ed. Rio de Janeiro: Campus, 2005.

104 STENBRO, M. **A survey of modern electronic voting technologies**. 2010. 162 p. Master Thesis – Norwegian University of Science e Technology. Disponível em: <http://brage.bibsys.no/xmlui/handle/11250/262287>. Acesso em: 2 abr. 2015.

105 STURTON, C.; JHA, S.; SESHIA, S. A.; WAGNER, D. On voting machine design for verification and testability. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY — CCS '09, 16th, Chicago, Illinois, USA. **Proceedings...** Chicago, Illinois, USA: ACM, 2009. (CCS '09, 16th), p. 463–476. DOI: 10.1145/1653662.1653719.

106 SWIERENGA, S. J.; ZANTJER, R. S.; JACKSON, J. E.; ISMIRLE, J.; BLOSSER, S. R.; PIERCE, G. L. Security implications for personal assistive technology in voting. In: HUMAN ASPECTS OF INFORMATION SECURITY, PRIVACY, AND TRUST, 3rd, Los Angeles, CA, USA. **Proceedings...** Cham: Springer International Publishing, 2015. LNCS 9190, p. 582–591. DOI: 10.1007/978-3-319-20376-8_52.

107 TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE (TGDC). **Voluntary Voting System Guidelines**: Voting System Performance Guidelines. v. 1. [S.l.]: U.S. Election Assistance Commission, 2015. 194 p. Disponível em: <https://eac926.ae-admin.com/assets/1/Documents/VVSG.1.1.VOL.1.FINAL.pdf>. Acesso em: 6 maio 2016.

108 TIELLA, R.; VILLAFIORITA, A.; TOMASI, S. FSMC+, a tool for the generation of Java code from statecharts. In: INTERNATIONAL SYMPOSIUM ON PRINCIPLES AND PRACTICE OF PROGRAMMING IN JAVA, 5th, Lisboa, Portugal. **Proceedings...** New York, NY, USA: ACM, 2007. (PPPJ '07, 5th), p. 93–102. DOI: 10.1145/1294325.1294338.

109 TOWNSLEY, W.; VALENCIA, A.; RUBENS, A.; PALL, G.; ZORN, G.; PALTER, B. **Layer Two Tunneling Protocol "L2TP"**. RFC-2661. [S.l.]: IETF, 1999. Disponível em: <https://tools.ietf.org/html/rfc2661>. Acesso em: 15 mar. 2016.

110 TRIOLA, M. F. **Introdução à Estatística**. Tradução: Vera Regina Lima de Farias e Flores. 10. ed. (reimpr.) Rio de Janeiro: LTC, 2012. 696 p.

111 VAN DE GRAAF, J.; CUSTÓDIO, R. F. **Tecnologia Eleitoral e a Urna Eletrônica**: Relatório SBC 2002. [S.l.], 2002. 38 p. Disponível em: <http://www.brunazo.eng.br/voto-e/textos/relatoriosbc.pdf>. Acesso em: 15 ago. 2016.

112 VOLKAMER, M.; SPYCHER, O.; DUBUIS, E. Measures to Establish Trust in Internet Voting. In: INTERNATIONAL CONFERENCE ON THEORY AND PRACTICE OF ELECTRONIC GOVERNANCE, 5th, Tallinn, Estonia. **Proceedings...** New York, NY, USA: ACM, 2011. (ICEGOV '11, 5th), p. 1–10. DOI: 10.1145/2072069.2072071.

113 WOLCHOK, S.; WUSTROW, E.; HALDERMAN, J. A.; PRASAD, H. K.; KANKIPATI, A.; SAKHAMURI, S. K.; YAGATI, V.; GONGGRIJP, R. Security Analysis of India's Electronic Voting Machines. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 17th, Chicago, Illinois, USA. **Proceedings...** New York, NY, USA: ACM, 2010. (CCS '10, 17th), p. 1–14. DOI: 10.1145/1866307.1866309.

114 YASINSAC, A. Precision in elections: Extracting a precise result from an inherently imprecise process. **International Journal of Critical Infrastructure Protection**, v. 5, n. 3-4, p. 135–136, 2012. DOI: 10.1016/j.ijcip.2012.09.002.

115 _____. **Software Independence**. [S.l.: s.n.], 2007. Disponível em: <http://www.cs.fsu.edu/~yasinsac/SoftwareIndependence.pdf>. Acesso em: 5 abr. 2015.

116 ZWIERKO, A.; KOTULSKI, Z. A Light-Weight e-Voting System with Distributed Trust. **Electronic Notes in Theoretical Computer Science**, v. 168, SPEC. ISS., p. 109–126, 2007. DOI: 10.1016/j.entcs.2006.12.004.