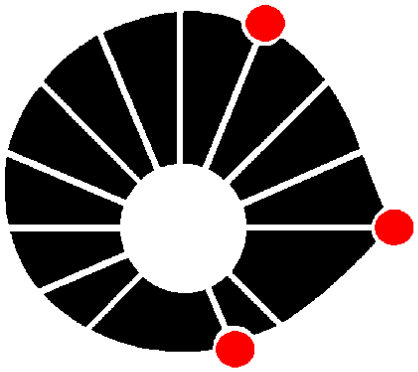

Avaliação do Sistema Informatizado de Eleições

(Urna Eletrônica)

UNICAMP
Maio 2002

Índice

1 INTRODUÇÃO 1

1.1 Apresentação 1
1.2 Objetivo e escopo 2
1.3 Coleta de informações 3
1.4 Documentos, programas e dados fornecidos pelo TSE 3
1.5 Ambiente de trabalho e recursos 5
1.6 Organização deste documento 5

2 METODOLOGIA DE AVALIAÇÃO 7

2.1 Estudo do processo eleitoral 7
2.2 Análise do fluxo de informação e dos procedimentos do SIE 7
2.3 Análise do projeto de hardware e firmware da urna 8
2.4 Análise do software da urna 8
2.5 Análise do processo de transporte e totalização 8
2.6 Análise dos ambientes e ferramentas auxiliares 8
2.7 Análise dos procedimentos de inseminação 9
2.8 Teste e análise de operação 9
2.9 Análise da topologia e da segurança da rede do TSE 9
2.10 Análise das técnicas criptográficas empregadas no SIE 10

3 VISÃO GERAL DO SISTEMA INFORMATIZADO DE ELEIÇÕES 11

3.1 Componentes principais do SIE 11
3.1.1 A urna eletrônica 11
3.1.2 Transportador e totalizador dos dados 14
3.1.3 Sistemas de suporte ao processo eleitoral 15
3.1.4 Subsistemas auxiliares 15
3.2 O desenvolvimento e a distribuição do software da urna 16
3.3 O fluxo do software e dados no SIE 19

4 AVALIAÇÃO DO SISTEMA INFORMATIZADO DE ELEIÇÕES 22

4.1 Introdução 22
4.2 O hardware da urna 22
4.3 O desenvolvimento do código-fonte 24
4.4 O processo de compilação do código-fonte 25
4.5 Os mecanismos de verificação de integridade de arquivos 26
4.6 O sistema operacional residente na urna 27
4.7 O empacotamento e a transferência do software da UE 27
4.8 O Subsistema de Instalação e Segurança (SIS) 28
4.9 A geração de mídia e a inseminação da UE 29
4.10 A preparação da urna para o segundo turno 30
4.11 Software do aplicativo 31
4.12 Uso de técnicas criptográficas 32
4.13 O boletim de urna e seu transporte 33
4.14 A totalização 34
4.15 A rede de computadores do TSE 35

5 RECOMENDAÇÕES 37

5.1 Desenvolvimento dos aplicativos de votação baseados em blocos estáveis e permanentes para todas as eleições 38

5.2 Formalização do ciclo de desenvolvimento do software 39
5.3 Avaliação do código-fonte do núcleo do aplicativo e seus componentes acessórios por especialistas em informática independentes do TSE 39
5.4 Compilação e determinação de resumos criptográficos dos arquivos em sessão pública 40
5.5 Verificação, por representantes partidários, dos resumos criptográficos dos arquivos instalados nas urnas inseminadas....41
5.6 Revisão do procedimento de preparação da urna para o segundo turno....42
5.7 Impressão do boletim de urna antes do ciframento dos resultados da votação....42
5.8 Substituição do uso de ciframento por assinaturas digitais como forma de autenticação dos Boletins de Urnas 42
6 CONCLUSÕES 45

1 INTRODUÇÃO

1.1 Apresentação

Este documento é o Relatório Final de avaliação do Sistema Informatizado de Eleições (SIE) do Tribunal Superior Eleitoral e consiste de um sumário das principais atividades realizadas, da avaliação dos componentes do SIE e de recomendações para o aprimoramento da segurança e confiabilidade do sistema, especialmente no que se refere ao sigilo do voto e ao respeito à expressão do voto do eleitor.

As avaliações, recomendações e conclusões apresentadas são fruto de: leitura e interpretação minuciosa dos programas-fonte; simulação de eleições tanto nas urnas eletrônicas como em computadores comuns (PCs) usando os programas da urna; compilação dos programas completos e de partes deles para testar funções específicas; análise detalhada das estruturas de dados usadas pelos programas e seus conteúdos antes, durante e após uma votação; interrupção forçada e reinício do programa de votação na urna sob diversas circunstâncias e em momentos variados do processo; análise detalhada de todos os arquivos presentes nos cartões de memória *flash* e disquetes da urna eletrônica antes, durante e após uma votação.

O trabalho de avaliação baseou-se também em informações referentes às eleições de 2000, no Edital de Licitação da Urna Eletrônica de 2002, em documentos e artigos especializadas em eleições e sistemas de votação eletrônica e em artigos acadêmicos publicados em anais de conferências em áreas correlatas.

As atividades são referentes ao Contrato TSE nº 54/2001 de prestação de serviços técnicos especializados, celebrado entre o Tribunal Superior Eleitoral e a Fundação de Desenvolvimento da UNICAMP - FUNCAMP com a interveniência da Universidade Estadual de Campinas - UNICAMP, assinado em 30/11/2001. A execução das atividades contratadas foi autorizada pelo Ofício 4672/2001 - SI/DG de 07/12/2001.

Composição da Comissão de Avaliação

A composição da Comissão de Avaliação encarregada da prestação dos serviços técnicos especializados, conforme comunicado ao TSE no Ofício GR 478/2001 de 13/12/2001, é a seguinte:

Prof. Dr. Clésio Luis Tozzi (Faculdade de Engenharia Elétrica e de Computação – FEEC/UNICAMP) – Coordenador

Prof. Dr. Tomasz Kowaltowski (Instituto de Computação – IC/UNICAMP) – Coordenador Adjunto

Prof. Dr. Jacques Wainer (Instituto de Computação – IC/UNICAMP)

Prof. Dr. José Raimundo de Oliveira (Faculdade de Engenharia Elétrica e de Computação – FEEC/UNICAMP)

Prof. Dr. Marco Aurélio Amaral Henriques (Faculdade de Engenharia Elétrica e de Computação – FEEC/UNICAMP)

Prof. Dr. Mario Jino (Faculdade de Engenharia Elétrica e de Computação – FEEC/UNICAMP)

Prof. Dr. Paulo Lício de Geus (Instituto de Computação – IC/UNICAMP)

Prof. Dr. Ricardo Dahab (Instituto de Computação – IC/UNICAMP)

1.2 Objetivo e escopo

O objetivo do trabalho aqui relatado foi a análise do Sistema Informatizado de Eleições visando detectar a existência de eventuais vulnerabilidades, avaliar o seu impacto e recomendar medidas para eliminá-las ou atenuá-las. Em especial, a análise visou as vulnerabilidades que pudessem comprometer os requisitos fundamentais de um sistema informatizado de eleições, ou seja, o sigilo do voto e o respeito à expressão do voto do eleitor. Adicionalmente, buscou-se avaliar a auditabilidade das funções e da operação do sistema.

Deve-se salientar que o trabalho realizado não constituiu uma auditoria do Sistema Informatizado de Eleições e, sim, uma avaliação do sistema utilizado nas eleições de 2000 e a proposição de medidas para a sua melhoria.

A análise enfocou os programas executados nas Urnas Eletrônicas e outros computadores do TSE e TREs para a captação, transmissão e totalização dos votos, os procedimentos para o desenvolvimento desses programas e o seu ambiente de operação. Foram abordados com maior ênfase os aspectos diretamente relacionados com a urna eletrônica, ponto principal do processo eleitoral implementado pelo Sistema Informatizado de Eleições.

1.3 Coleta de informações

A Comissão de Avaliação baseou o seu trabalho em informações (documentos, programas e dados) referentes às eleições de 2000 e bem como no Edital de Licitação da Urna Eletrônica de 2002, fornecidos pelo TSE. Subsídios adicionais foram colhidos em outras fontes especializadas em eleições e sistemas de votação eletrônica. Foram analisados documentos disponibilizados por entidades tais como *The Institute of Electrical and Electronics Engineers* (IEEE - USA), *Federal Election Comission* (USA), *California Institute of Technology* (CALTECH), *Massachusetts Institute of Technology* (MIT), Fórum de Debate Sobre o Voto Eletrônico (http://www.votoseguro.org), entre outros. Também foram analisados artigos acadêmicos publicados em anais de conferências em áreas correlatas.

Tais informações foram complementadas em várias reuniões entre membros da comissão de avaliação, técnicos e consultores do TSE e técnicos de empresas terceirizadas pela Secretaria de Informática do TSE para o desenvolvimento de software. Durante vários dias membros da comissão permaneceram no TSE acompanhando seus procedimentos internos e coletando dados adicionais. Esclarecimentos diversos sobre o SIE foram prestados por técnicos do TSE durante a visita de instalação do Subsistema de Instalação e Segurança (SIS) e do sistema de geração de mídia para a urna eletrônica. Um dos membros da comissão visitou o CEPESC (Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações) para conhecer os algoritmos e protocolos criptográficos utilizados para ciframento do boletim de urna. Membros da comissão estiveram em reunião com técnicos da empresa Módulo Security Solutions, quando foi possível discutir o funcionamento e características internas do Subsistema de Instalação e Segurança (SIS) bem como o processo de empacotamento e desempacotamento de software realizado neste ambiente. Membros da comissão estiveram em Brasília para obter esclarecimentos adicionais sobre o processo de totalização dos votos.

Além disso, membros da comissão de avaliação participaram de vários eventos relacionados ao SIE: reunião com os técnicos do TSE em 10/08/2001 para discussão inicial sobre o SIE; apresentação detalhada do SIE pelos técnicos do TSE na UNICAMP em 17/08/2001; encontro de Secretários de Informática da Justiça Eleitoral, em Brasília, de 24 a 26/10/2001 e de 10 a 12/04/2002.

1.4 Documentos, programas e dados fornecidos pelo TSE

Para subsidiar o trabalho da comissão de avaliação, o TSE forneceu a documentação, os programas e os dados descritos a seguir:

- CD contendo os arquivos-fonte do software e firmware da urna;

- mapas descritivos da arquitetura de todo o Sistema Informatizado das Eleições bem como mapas de *workflow* do sistema e o diagrama da topologia da rede do TSE;
- fluxograma dos procedimentos relativos ao empacotamento de software e outras informações para fins de distribuição e posterior recuperação dentro do Subsistema de Instalação e Segurança (SIS);
- Código Eleitoral Anotado e Legislação Complementar - 4a. Edição TSE 2001;
- Guia de Programação para Linguagem C – VirtuOS;
- VirtuOS - Users and Reference Guide;
- base de dados para testes do Gerador de Mídias;
- documentação da eleição de 2000, cujos itens estão listados a seguir:
  - Instruções para Mesários;
  - Instruções das Eleições Vols. I, II e III (Resoluções);
  - Sistema Eletrônico de Apuração (Descrição);
  - Diagrama do Fluxo de Informações e Ambiente Operacional;
  - Orientação para Juízes e Promotores;
  - cópia do PA TSE 10.158/2000 - Apresentação aos Partidos Políticos;
  - vinte e oito CDs com dados e Sistema Estatístico dos *logs* das UEs;
  - um CD com programas-fonte dos Sistemas Eleitorais e Especificações;
  - uma pasta com a Referência dos Arquivos do CD acima;
  - documentação do CEPESC sobre a Criptografia;
  - Descritivo do SIS - Subsistema de Instalação e Segurança;
  - informação das Plataformas e Versões de Software Básico Utilizados na Eleição;
  - Manual de hardware UE2000;
  - Manual de Operação e Instalação;
  - Manual de Produção;
  - Manual de Projeto;
  - Manual de Software Básico UE2000;
  - Manual de Software do GM;
  - Manual de Software do SE;
  - Manual de Software do SRUE;
  - Manual de Software do SVC;
  - Manual do Usuário do Gerador de Mídia;

- Manual do Usuário do SE;
- Manual do Usuário do SRUE;
- Manual do Usuário do SVC;
- Manual Técnico de Suporte;
- Manual Teste Fabril UE2000;
- Treinamento Gerador de Pacotes SIS3_0 (Manual);
- Treinamento Multiplicadores SIS3_0 (Manual);
- Treinamento Suporte SIS3_0 (Manual).

1.5 Ambiente de trabalho e recursos

Um laboratório para dar suporte ao trabalho de avaliação do SIE foi montado em uma sala da Faculdade de Engenharia Elétrica e de Computação. Neste laboratório foram instalados os equipamentos utilizados para a reprodução dos ambientes necessários para simular as atividades ligadas ao SIE. O acesso a esta sala ficou restrito aos membros da comissão de avaliação.

Além disso, a comissão de avaliação contou com equipamento e material disponibilizado pelo TSE para o trabalho de análise, conforme listado a seguir:

- um computador com a configuração oficial de um gerador de mídia;
- três unidades de urnas eletrônicas, modelo UE2000;
- unidades de *flash card* divididas da seguinte forma:
  - três unidades de *flash card* interna (FI), instaladas internamente às urnas disponibilizadas;
  - seis unidades de *flash card* de 30 Mbytes ;
  - seis unidades de *flash card* de 15 Mbytes.
- um acionador de flash card para o barramento IDE.
- amostras de lacres das tampas da UE (no. 1422900 a 1422904 e 0134801 a 0134805).

1.6 Organização deste documento

O relatório inclui, além desta introdução, as seções cujos conteúdos são descritos a seguir.

Seção 2 – **Metodologia de Avaliação**: são descritas sucintamente as atividades técnicas realizadas na análise dos vários tópicos abordados na avaliação do Sistema Informatizado de Eleições: o processo eleitoral; o

fluxo de informação e os procedimentos do SIE; o projeto de hardware e firmware da urna; o software da urna; o processo de transporte e totalização; os ambientes e ferramentas auxiliares do SIE; os procedimentos de inseminação; a operação da urna; a topologia e a segurança da rede do TSE; e as técnicas criptográficas empregadas no SIE.

Seção 3 – **Visão Geral do Sistema Informatizado de Eleições**: contém uma descrição resumida do Sistema Informatizado de Eleições (SIE), não tendo como objetivo apresentar uma descrição completa e formal de todos os seus componentes e processos associados, mas apenas as informações essenciais para o seu entendimento.

Seção 4 – **Avaliação do Sistema Informatizado de Eleições**: são avaliados os pontos do hardware e do software do SIE que foram considerados mais relevantes para este trabalho e que merecem comentários específicos: o hardware da urna, o desenvolvimento do código-fonte, o processo de compilação do código-fonte, o sistema operacional residente na urna, o empacotamento e a transferência do software da urna, o subsistema de instalação e segurança, a geração e mídias e a inseminação da urna, a preparação da urna para o segundo turno, o software aplicativo, o uso de técnicas criptográficas, o boletim de urna e seu transporte, a totalização e a rede de computadores do TSE.

Seção 5 – **Recomendações**: é apresentado um conjunto de recomendações cujo objetivo é o aumento da segurança do Sistema Informatizado de Eleições, em especial de seu componente mais sensível que é a urna eletrônica e que tem seu processo de segurança altamente dificultado pela necessidade de preservação do sigilo do voto.

Seção 6 – **Conclusões:** são apresentadas as considerações finais desta avaliação, onde são ressaltados os principais resultados e recomendações do trabalho da comissão de avaliação do Sistema Informatizado de Eleições.

2 METODOLOGIA DE AVALIAÇÃO

Nesta seção são descritas sucintamente as atividades técnicas realizadas na análise dos vários tópicos abordados na avaliação do Sistema Informatizado de Eleições: o processo eleitoral; o fluxo de informação e os procedimentos do SIE; o projeto de hardware e firmware da urna; o software da urna; o processo de transporte e totalização; os ambientes e ferramentas auxiliares do SIE; os procedimentos de inseminação; a operação da urna; a topologia e a segurança da rede do TSE; e as técnicas criptográficas empregadas no SIE. O detalhamento das atividades técnicas foi relatado ao TSE.

2.1 Estudo do processo eleitoral

A primeira atividade de avaliação consistiu no estudo e entendimento de processos eleitorais em geral e de seus requisitos básicos.

Em seguida, foram analisados o processo eleitoral brasileiro, a organização da Justiça Eleitoral, as disposições legais e os aspectos logísticos relativos à realização de uma eleição em âmbito nacional. Este estudo foi baseado em informações bibliográficas e em documentação disponibilizada pelo TSE.

2.2 Análise do fluxo de informação e dos procedimentos do SIE

Este estudo visou a análise geral dos componentes do Sistema Informatizado de Eleições e dos procedimentos de desenvolvimento, compilação e empacotamento de software do SIE.

Esta análise baseou-se na documentação fornecida pelo TSE e em contatos diretos com membros da equipe de técnicos do TSE, em Brasília e no laboratório na UNICAMP.

2.3 Análise do projeto de hardware e firmware da urna

Esta análise foi baseada na documentação fornecida pelo TSE, no exame das três unidades de urnas disponibilizadas para os trabalhos de avaliação e nos contatos diretos com a equipe de técnicos do TSE.

2.4 Análise do software da urna

Sistema Operacional e suas extensões

Foi feita uma análise funcional do sistema operacional e dos programas que estendem suas funcionalidades. Foram realizadas análises detalhadas dos principais arquivos de lote de comandos (*batch*).

Código-fonte do aplicativo de votação

O código-fonte do aplicativo de votação das eleições de 2000 foi analisado com base nos arquivos fornecidos pelo TSE. Experimentos de compilação e execução de programas foram realizados; examinou-se também o efeito de modificações de trechos do código-fonte.

Código-fonte do voto cantado

O código-fonte do aplicativo de voto cantado das eleições de 2000 foi analisado com base nos arquivos fornecidos pelo TSE e testes foram feitos com sua versão executável.

2.5 Análise do processo de transporte e totalização

Os documentos disponibilizados pelo TSE foram estudados, inicialmente, para a análise do processo de transporte e totalização. Esta análise aprofundou-se com as visitas de membros da comissão de avaliação aos técnicos do TSE em Brasília.

A análise dos programas do sistema de transporte e totalização, com exceção das rotinas criptográficas, baseou-se nos arquivos-fonte disponibilizados pelo TSE.

2.6 Análise dos ambientes e ferramentas auxiliares

Ambientes e ferramentas auxiliares são aqueles que dão suporte às atividades associadas ao SIE. A análise de dois desses ambientes, considerados essenciais para a avaliação do processo, foi viabilizada pela sua instalação em computadores do laboratório montado na UNICAMP.

Subsistema de Instalação e Segurança (SIS)

A análise do SIS foi realizada com base em: documentação do fornecedor, disponibilizada pelo TSE; apresentação técnica especialmente realizada pelo fornecedor para membros da comissão de avaliação; operação de computador equipado com o SIS; e experimentos de acesso a informações protegidas.

Gerador de mídia

Esta análise foi realizada utilizando dois computadores com o aplicativo de geração de mídia instalado e dispondo de ambiente similar ao encontrado nos TREs. Um dos computadores, da mesma marca e modelo dos computadores utilizados pelos TREs, foi disponibilizado pelo TSE com o gerador de mídia previamente instalado. O outro computador, disponível no laboratório da UNICAMP, foi formatado e carregado com o sistema operacional NT, o ambiente SIS e o programa Gerador de Mídia.

A avaliação funcional foi realizada por meio da geração de disquetes e *flash cards* de carga (FCs) e de votação (FVs) e pelo exame de seus conteúdos.

2.7 Análise dos procedimentos de inseminação

Os programas utilizados para inseminação da urna foram analisados detalhadamente. Os mecanismos de verificação da integridade e autenticidade das *flash cards* de carga foram analisados e testados. Os disquetes e as *flash cards* interna e de carga tiveram seus conteúdos analisados a cada passo do processo de inseminação. O processo de preparação da urna para o segundo turno também foi analisado.

2.8 Teste e análise de operação

As urnas inseminadas com os programas e dados oficiais das eleições de 2000 foram analisadas sob as mesmas condições encontradas no dia da eleição (data da votação, horários de abertura e encerramento, emissão de zerésima e boletins de urna, geração de disquetes etc). As *flash cards* interna e de votação e o disquete tiveram seus conteúdos analisados antes, durante e após o período de votação.

2.9 Análise da topologia e da segurança da rede do TSE

A análise da rede do TSE foi realizada com base em documentos fornecidos pelo TSE e em visitas às instalações do TSE. Foram estudados a topologia de *firewall* utilizada e seus componentes (provedores de serviços públicos e funcionalidades de *firewall*). A rede privada do TSE, interligando o TSE, os TREs, zonas e pólos eleitorais, também foi analisada. Deu-se também

importância às configurações adotadas para os elementos de rede, especialmente o *firewall*, antes, durante e depois da eleição.

2.10 Análise das técnicas criptográficas empregadas no SIE

Esta análise cobriu: a utilização de resumos criptográficos para verificação de integridade e autenticidade de vários componentes do SIE; o ciframento dos pacotes de software e dados provenientes do TSE e destinados aos TREs; e o ciframento dos boletins de urna para o seu transporte aos centros de totalização. O objetivo desta análise foi a verificação da corretude dos vários protocolos criptográficos empregados e de sua adequabilidade aos requisitos de segurança do SIE.

A análise do protocolo de ciframento do boletim de urna baseou-se em uma apresentação feita por técnicos do CEPESC, na especificação de interface fornecida e nos códigos-fonte dos programas de totalização.

3 VISÃO GERAL DO SISTEMA INFORMATIZADO DE ELEIÇÕES

Esta seção contém uma descrição resumida do Sistema Informatizado de Eleições (SIE), não tendo como objetivo apresentar uma descrição completa e formal de todos os seus componentes e processos associados, mas apenas as informações essenciais para o seu entendimento.

3.1 Componentes principais do SIE

Esta subseção descreve os principais componentes do SIE: a urna eletrônica, o transportador, o totalizador e sistemas auxiliares.

3.1.1 A urna eletrônica

Há três versões de hardware para a urna eletrônica, os modelos UE96, UE98 e UE2000, que foram adquiridos nos anos de 1996, 1998 e 2000, respectivamente. Todos os modelos apresentam a mesma arquitetura básica, embora diferenças, decorrentes da evolução tecnológica, possam ser observadas no seu hardware.

Hardware

A urna compõe-se de dois módulos: o terminal do eleitor (a urna propriamente dita e que inclui toda a capacidade de processamento e armazenamento da informação) e o microterminal, utilizado pelos mesários.

Além dos dispositivos de entrada e saída visíveis para o eleitor, teclado e monitor de vídeo, a urna inclui também:

- uma impressora, usada para impressão dos boletins de urna e dos relatórios de testes e de carga de software;
- um acionador de disquete de 3,5 polegadas;
- dois *slots* para inserção de cartões de memória do tipo *flash*, que são denominados *flash* interna e *flash* externa;

- um conector para teclado padrão PS2 convencional, usado em procedimentos de teste e de manutenção da urna;
- dois conectores USB;
- um conector para fone de ouvido, para uso de eleitores com deficiência visual;
- um conector para conexão com outros terminais de eleitor (no microterminal);
- um conector para impressora (no microterminal).

Todos esses dispositivos de entrada e saída, com exceção do *flash card* interno, são acessíveis do exterior do terminal de votação. Todos os dispositivos com acesso externo, exceto o fone de ouvido, possuem tampas que são lacradas após o carregamento do software de votação e que permanecem lacradas até a conclusão da votação.

Após a votação de primeiro turno apenas o lacre do acionador de disquete é rompido para retirada do disquete com o resultado da votação. Os demais dispositivos permanecem lacrados.

O microterminal comunica-se com o terminal do eleitor por meio de um cabo serial ligado diretamente às placas internas. Todo o processamento das informações inseridas pelo mesário, como a identificação do eleitor e os comandos, é realizado no terminal do eleitor.

Cada conjunto (terminal do eleitor, microterminal) pode ser interligado a até dois outros terminais do eleitor. Nessa configuração um terminal atua como mestre do sistema e os outros dois como escravos. Os dados da votação (candidatos, partidos, eleitores) são armazenados no terminal mestre, que também é responsável pelo processo de totalização da seção eleitoral. Os terminais escravos realizam apenas as funções de entrada e saída (teclado e tela). Esta configuração é utilizada em seções com grande número de eleitores.

A urna eletrônica possui uma arquitetura similar à arquitetura de um computador IBM-PC. Seu projeto inclui, todavia, hardware não encontrado em um computador pessoal e que é necessário para controle e segurança da urna. Seu hardware inclui, por exemplo, sensores para verificação do estado da bateria interna, do estado da impressora etc, e um microcontrolador, utilizado para controle dos sensores e do teclado do terminal do eleitor. A comunicação desse microcontrolador com o processador é feita através de porta serial de uso compartilhado com o teclado padrão PS2.

Firmware

Também no firmware a urna eletrônica difere ligeiramente de um computador IBM-PC.

Algumas funções foram implementadas em firmware e armazenadas no que se denominou Extensão do BIOS. Essas modificações impedem, por

exemplo, a inicialização da urna eletrônica a partir do acionador de disquete independentemente da configuração da memória CMOS. Outras funções de segurança foram implementadas nessa extensão.

Ainda, memórias não voláteis (EEPROM) são utilizadas para armazenamento de informações próprias de cada urna (número de série) e informações necessárias para autenticação e criptografia.

Software

A urna eletrônica utiliza o sistema operacional VirtuOS. Este é um sistema operacional *multithreaded*, que possibilita o compartilhamento do processador por diferentes processos que são executados simultaneamente. Funções complementares, especialmente desenvolvidas para atender as características da urna eletrônica, foram agregadas ao sistema operacional. O conjunto das funções agregadas foi denominado Extensão do Sistema Operacional.

A aplicação em si é formada por um conjunto de programas destinados a teste da urna, simulações, treinamento e votação. Os programas da aplicação utilizados em uma eleição são idênticos para todas as urnas eletrônicas, independentemente do local da votação. A adequação da urna para uma seção específica é feita no processo de instalação do software (inseminação da urna) pelo carregamento dos dados relativos aos eleitores e candidatos aptos a votar e receber votos, respectivamente, naquela seção.

Dados da seção eleitoral

Como já observado acima, todas as urnas eletrônicas executam o mesmo programa de votação. Sua adequação a uma seção específica é decorrente dos dados carregados na urna durante o processo de inseminação.

Os dados necessários à preparação da urna eletrônica para uma seção eleitoral consistem basicamente de:

- designação do município, zona e seção eleitoral;
- tabelas de partidos e candidatos que disputam eleição no local da seção;
- tabela de eleitores da seção eleitoral;
- fotos dos candidatos.

Após o encerramento da votação dispõe-se na urna, além do boletim de urna (BU) com o resultado apurado na seção, de outros resultados que são armazenados em arquivos e remetidos juntamente com o boletim de urna para o centro totalizador. Entre estes arquivos estão o registro de eleitores ausentes, o registro de justificativas eleitorais e o arquivo de *log* (registro de todos os eventos associados à urna eletrônica, desde o momento de sua inseminação até o encerramento da votação).

Além dos dados acima referenciados, são mantidas no *flash card* interno (FI) e no *flash card* externo (FV) cópias das matrizes de totalização e de

estruturas de controle que são essenciais para a retomada do processo de votação, sem perda dos dados, na eventual ocorrência de falhas.

3.1.2 Transportador e totalizador dos dados

Dois sistemas são essenciais no processo de apuração da eleição: o transportador, que tem como função a leitura do disquete gerado na urna e sua transmissão para o centro de totalização e o totalizador, que tem como função a recepção dos dados enviados pelos transportadores, a extração do resultado de cada seção eleitoral e a totalização dos dados da eleição.

Transportador

O transportador consiste em um conjunto de aplicativos instalados em uma máquina sob a guarda do juiz eleitora, cujas funções principais são: a leitura dos disquetes provenientes das seções eleitorais; a cópia dos arquivos de dados contidos nos disquetes, entre eles o BU; o armazenamento dos arquivos extraídos dos disquetes; e o posterior envio dos mesmos ao computador de totalização.

O software do transportador é instalado em plataforma Windows NT, em máquinas que ficam normalmente no próprio local de apuração. A transmissão dos arquivos para o totalizador é feita em lotes, isto é, vários disquetes são lidos, seus conteúdos armazenados localmente e, posteriormente, transmitidos ao totalizador em um único bloco.

A transferência de dados entre o transportador e o totalizador é feita através de uma rede de computadores. A rede utilizada é privada e não tem conexão direta com redes públicas. A integridade física da rede é garantida pelo isolamento do local de apuração e pela restrição do acesso aos computadores de rede, permitido somente a pessoas autorizadas.

Totalizador

O totalizador é formado por um conjunto de aplicativos instalados em um computador com plataforma Unix (HP/UX) ou Windows NT, instalados nos TREs ou em zonas-mãe eleitorais. Sua função é processar os arquivos enviados pelo transportador e fazer a totalização dos resultados. Compõem o totalizador:

- rotinas criptográficas para o deciframento dos BUs;
- aplicativos para verificação de consistência e autenticidade dos BUs;
- aplicativos para leitura dos dados e acumulação dos votos;
- sistema gerenciador de banco de dados Oracle;
- aplicativos para divulgação dos resultados nos municípios.

Em caso de eleições municipais a totalização é feita nas zonas-mãe. Nas outras eleições a totalização é feita nos TREs.

No caso de eleições presidenciais são feitas totalizações parciais nos TREs. Estes dados parciais são regularmente transmitidos ao TSE, que computa o resultado nacional a partir das totalizações estaduais. O transporte dos dados dos TREs para o TSE é feito por uma rede privada de computadores. A atualização dos resultados é feita por transações em banco de dados.

A instalação e a operação do software do totalizador são feitas de forma controlada, com usuários cadastrados e a utilização de senhas e contra-senhas. A ativação dos programas é feita de forma oficial, com a presença do Juiz Eleitoral, que deve fornecer no ato a sua senha pessoal.

3.1.3 Sistemas de suporte ao processo eleitoral

Além do transportador e do totalizador, outros sistemas compõem o SIE. Estes sistemas são utilizados, por exemplo, para:

- controle da distribuição, armazenamento e acompanhamento das urnas eletrônicas,
- controle do cadastro de eleitores;
- controle do registro de candidatos;
- controle e acompanhamento da propaganda eleitoral.

Estes sistemas não foram objeto de análise neste trabalho.

3.1.4 Subsistemas auxiliares

Embora do ponto de vista estrito o Gerador de Mídia (GM) e o Subsistema de Instalação e Segurança (SIS) não se caracterizem como componentes do SIE, suas funcionalidades e características são apresentadas abaixo, dada a importância que estes dois sistemas apresentam para a distribuição do software utilizado no processo eleitoral.

Gerador de Mídia

O Gerador de Mídia pode ser considerado o ponto de convergência dos programas e dados originados no TSE e dos dados (candidaturas) gerados localmente nos TREs.

É no Gerador de Mídia que os dados das seções eleitorais (tabelas de eleitores, candidatos e partidos) e os programas são transferidos para o *flash card* de carga (FC) utilizada para a inseminação da urna eletrônica. Este aplicativo tem também como função a recuperação da tabela de correspondência que resulta do processo de inseminação e que fica armazenada no *flash card* de carga. Esta tabela associa a urna eletrônica (identificada pelo número de série gravado internamente em EEPROM) com a seção eleitoral cujos dados foram efetivamente transferidos para a urna no processo de inseminação. Estas informações são transferidas ao

totalizador e utilizadas, durante a totalização, para verificar a consistência dos dados.

O Gerador de Mídia tem ainda como função a gravação dos *flash cards* de votação e dos disquetes utilizados nas urnas durante a eleição.

Subsistema de Instalação e Segurança (SIS)

O Subsistema de Instalação e Segurança (SIS), desenvolvido pela empresa Módulo, é uma das ferramentas básicas de segurança do SIE e é empregado nos computadores do TSE, dos TREs e dos pólos de inseminação de UEs com o objetivo de controlar de forma mais rigorosa o acesso e as operações feitas pelos usuários desses computadores.

O SIS é uma camada de software que interage com o sistema operacional Windows NT. O SIS assiste os usuários na instalação e no uso dos vários softwares do SIE e controla o acesso aos recursos do sistema, pelo cruzamento de informações sobre o sistema instalado e das permissões e dos perfis de utilização previamente cadastrados.

Além do controle de acesso, o SIS possui outras funções importantes de segurança, como a verificação de contra-senhas e o registro de informações detalhadas sobre as operações realizadas pelos usuários, que são utilizadas para eventuais auditorias.

Por suas características, o SIS permite a criação de um ambiente de trabalho homogêneo e disciplinado em todos os computadores onde é instalado (TREs, pólos de inseminação etc), o que possibilita a uniformização dos procedimentos de geração dos *flash cards* de carga e o controle do processo de inseminação das urnas eletrônicas.

3.2 O desenvolvimento e a distribuição do software da urna

A implantação da votação eletrônica teve início em 1996 e completou-se em 2000 quando foi utilizada em todas as seções eleitorais do país.

A aquisição das cerca de 350.000 urnas necessárias para a cobertura de todas as seções eleitorais foi feita em etapas, com aquisições em 1996, 1998 e 2000. Uma nova aquisição de 50.000 urnas está sendo feita em 2002.

Embora a aquisição de novas urnas e o desenvolvimento (ou adequação) do software de aplicação para a eleição corrente pudessem ser tratados de forma independente, o TSE optou por tratá-los conjuntamente e ambos são objeto de uma única licitação. Desta forma, a empresa vencedora da licitação é responsável pela produção tanto do hardware como do software de aplicação, que será usado em todas as urnas eletrônicas (novas e antigas).

Assim, os procedimentos de um ano eleitoral iniciam-se com a preparação do edital de licitação para: aquisição do hardware, desenvolvimento do

software e contratação de serviços técnicos para a preparação e instalação das urnas.

Embora a empresa vencedora da licitação seja única, a licitação inclui diferentes produtos e, portanto, diferentes fluxos devem ser considerados para a entrega desses produtos. A Figura 3.1 ilustra este fato. A entrega das urnas e do software apresentam fluxos independentes. As urnas incluem apenas o BIOS e a extensão do BIOS quando de sua liberação na fábrica. Todos os demais softwares necessários para sua operação no dia da eleição serão incorporados posteriormente no processo de inseminação, o que é feito também para as urnas antigas.

Apresenta-se a seguir uma descrição resumida do processo de desenvolvimento do software de aplicação e do caminho percorrido por esse software até a sua instalação na urna eletrônica.

O desenvolvimento do software

O desenvolvimento do software de aplicação é feito a partir das especificações do edital de licitação. De forma geral seu desenvolvimento tem tomado como base um núcleo relativamente estável que vem sendo aperfeiçoado desde 1996 e que foi empregado nas eleições de 1996, 1998 e 2000.

O desenvolvimento dos programas é um processo iterativo, no qual o setor de informática do TSE recebe e testa as sucessivas versões dos programas desenvolvidos pela empresa contratada. A avaliação dos programas é feita por meio de simulações com massas de dados fictícios similares aos dados reais. A aprovação pela equipe do TSE resulta na versão final do programa que é encaminhada às fases seguintes do processo.

A compilação

A compilação da versão final do código-fonte é precedida de uma preparação pela equipe do TSE, quando são inseridas as chaves e as rotinas criptográficas.

Finalizada a preparação do código-fonte, é feita a compilação e a geração de códigos executáveis. Atendendo a requisitos legais, os códigos-fonte dos programas são colocados à disposição dos partidos políticos para análise. Encerrado o período de exposição, cópias dos programas-fonte e dos programas executáveis são feitas em mídia permanente (CDs) e lacradas em envelopes que recebem as assinaturas dos representantes de partidos políticos. Esses CDs ficam armazenados sob a guarda do TSE.

A compilação do código-fonte no TSE é feita em máquina isolada da rede, instalada numa sala com acesso restrito, e seu uso é registrado em *log*s. No ano de 2000, foi utilizado o compilador C da Borland, Versão 4.5.

Empacotamento e envio do software aos TREs

Encerrada a compilação dos programas, tem início a preparação dos pacotes que serão utilizados para envio dos programas aos TREs. Os pacotes incluem, além do programa aplicativo, todos os demais programas utilizados na urna eletrônica (sistema operacional, arquivos de dados, arquivos de lote etc) e os utilitários de apoio ao processo de inseminação da urna.

Estes pacotes são preparados em ambiente seguro e padronizado, criado pela utilização de Subsistema de Instalação e Segurança (SIS). Este sistema provê os mecanismos de comunicação segura entre o TSE e os TREs. A fase final de montagem do pacote, até o ano de 2000, foi feita por uma equipe de empresa terceirizada (Módulo) trabalhando nas instalações do TSE sob a supervisão de técnicos do TSE.

O pacote é finalmente cifrado e enviado aos TREs, através da rede de computadores do TSE ou por meio de CDs. Também é enviado a cada TRE o Cadastro Nacional de Eleitores.

O pacote de software e os dados do Cadastro Nacional de Eleitores recebidos nos TREs são desempacotados e disponibilizados em máquinas locais sob a gerência do Subsistema de Instalação e Segurança (SIS) e passam, então, a ser tratados pelo Gerador de Mídia como dados para a preparação dos *flash cards* de carga utilizadas na inseminação das urnas.

Os dados relativos às candidaturas locais são preparados nos TREs e também incorporados como dados no Gerador de Mídia.

A partir de cada TRE, o pacote de software e o cadastro de eleitores recebidos do TSE, juntamente com os dados das candidaturas locais, podem ser redistribuídos para os locais de inseminação das urnas, criando-se novas instâncias do Sistema Gerador de Mídia instalado no TRE e que ficam sob a supervisão do juiz eleitoral local.

A transferência do software para a urna eletrônica

A última etapa percorrida pelo software para chegar à urna eletrônica é feita por meio do *flash card* de carga utilizada para inseminação.

Os *flash cards* de carga são preparados no Gerador de Mídia. Sua preparação consiste no carregamento dos *flash cards* com cópias dos arquivos da aplicação, dos arquivos do sistema operacional, de arquivos de instalação e de arquivos de controle, todos recebidos do TSE. Cópias dos arquivos de candidaturas, gerados localmente nos TREs, e a parte do cadastro de eleitores, correspondente às seções que serão montadas pelo *flash card* de carga no processo de inseminação.

No processo de inseminação o *flash card* de carga é inserido no *slot* de *flash* externo e a urna é ligada. A inicialização da urna é feita a partir do *flash card* externo e é seguida da execução de programas que formatam o

flash card interno e copiam do *flash card* externo para o *flash card* interno os arquivos da aplicação, os arquivos do sistema operacional e os arquivos de controle. A urna é, então, desligada, o *flash card* de carga é retirado e é inserido em seu lugar o *flash card* de votação. O disquete de votação é inserido no acionador de disquete e a urna é religada. Procedimentos de verificação de integridade do hardware e do software são executados e, não sendo detectados erros, a urna é desligada, lacrada e está pronta para utilização no dia da votação.

3.3 O fluxo do software e dados no SIE

O diagrama das Figuras 3.1 a 3.3 mostra os principais eventos do SIE bem como o fluxo de informações dentro do sistema e complementa a exposição das Subseções 3.1 e 3.2. Neste diagrama foi dada ênfase aos eventos e informações diretamente associados à urna eletrônica e à totalização.

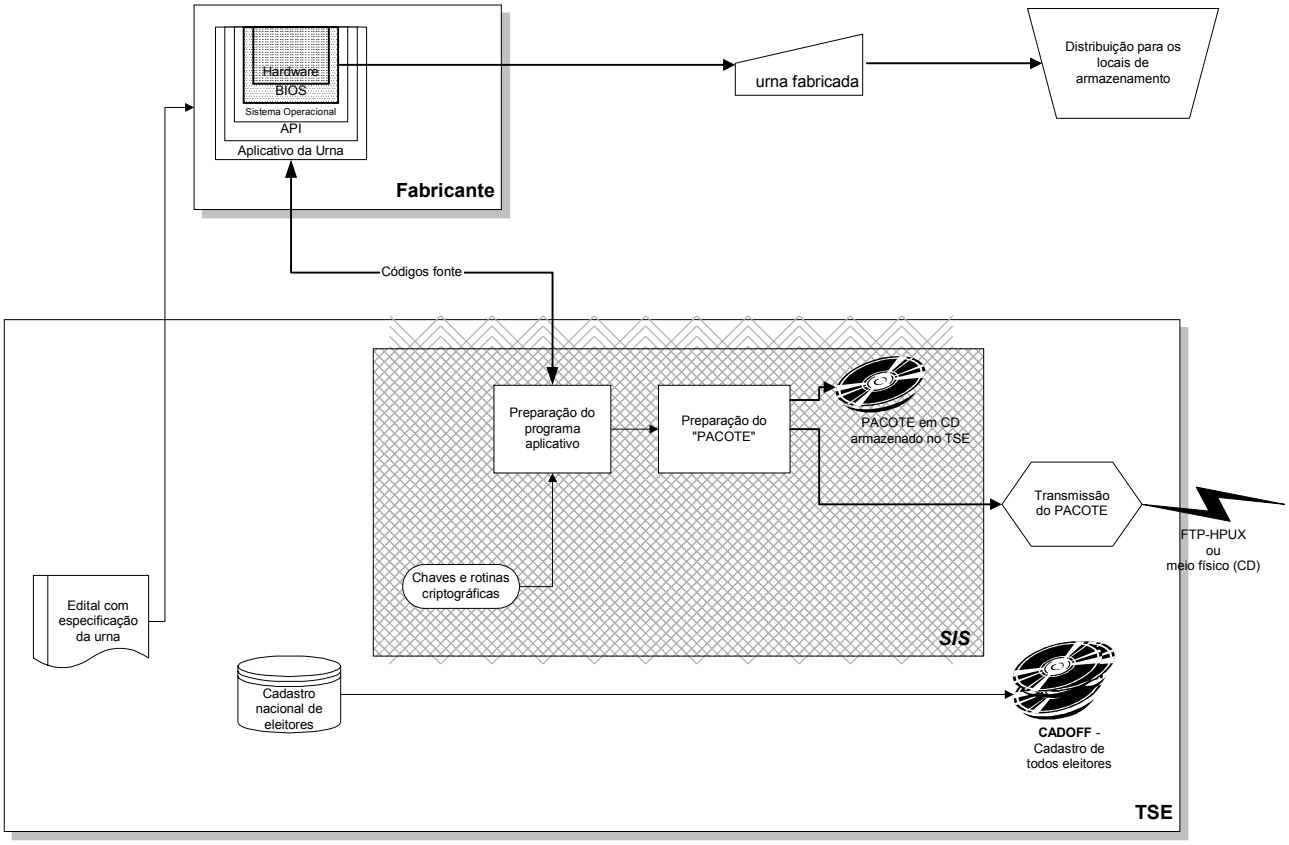

Figura 3.1: Etapas do desenvolvimento do software da urna.

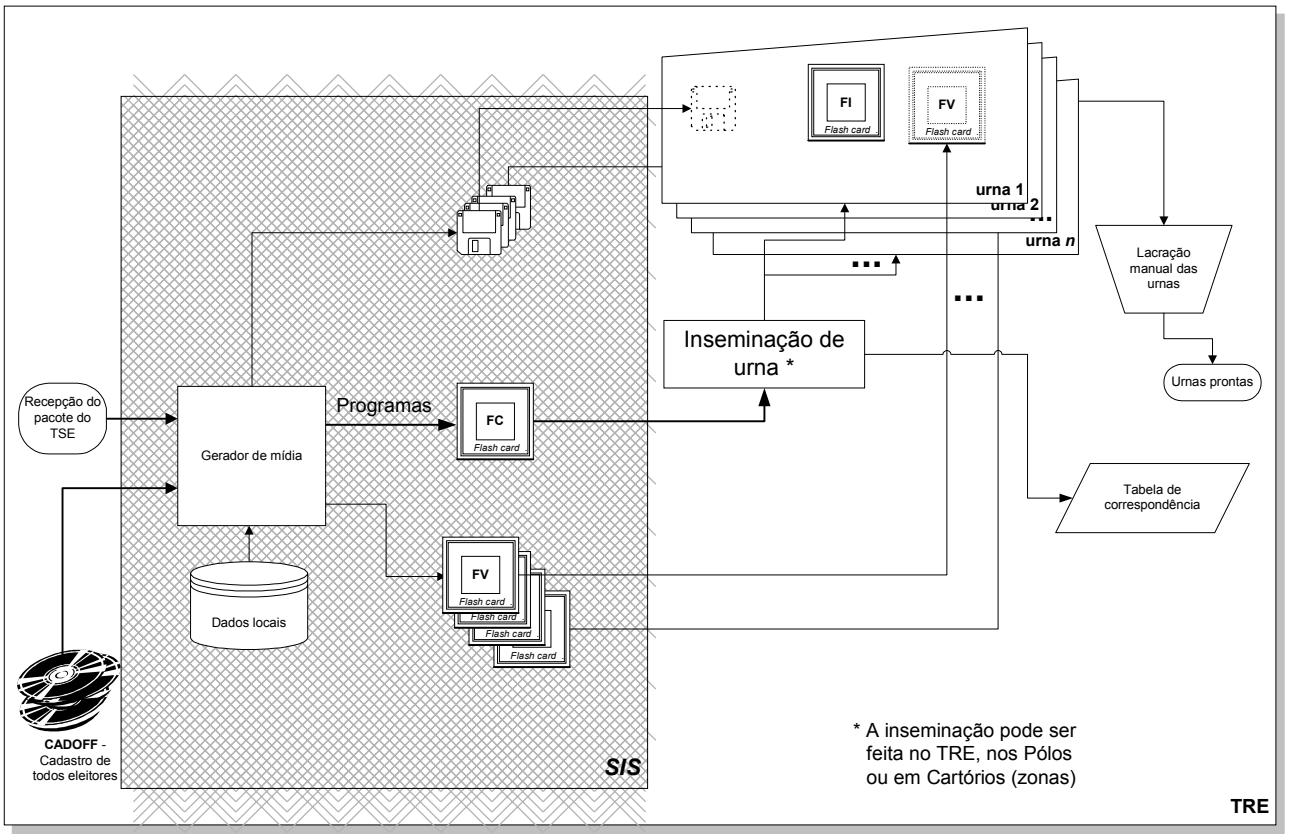

Figura 3.2 - Etapas de geração de mídia e inseminação

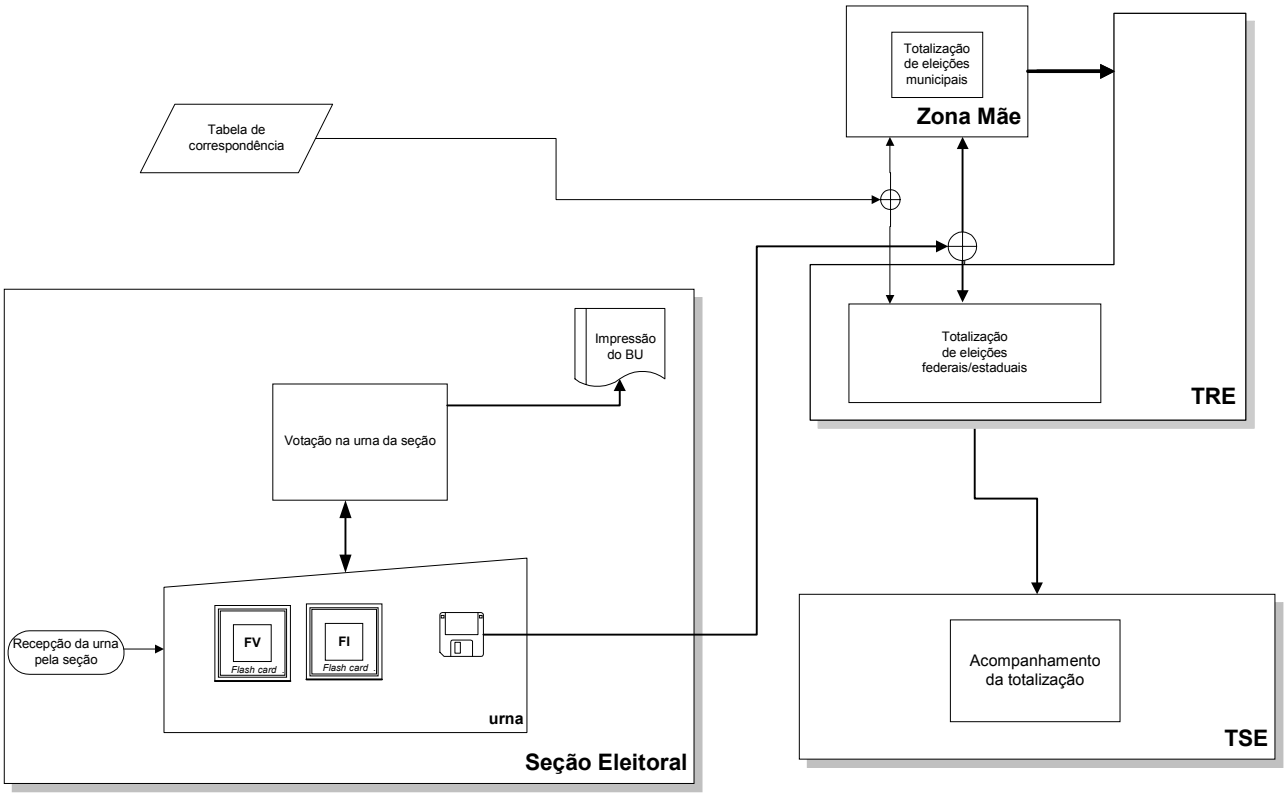

Figura 3.3 - Etapas de votação, geração de BU, transporte e totalização

4 AVALIAÇÃO DO SISTEMA INFORMATIZADO DE ELEIÇÕES

4.1 Introdução

Nesta seção são avaliados os pontos do hardware e do software do SIE que foram considerados mais relevantes para este trabalho e que mereceram comentários específicos.

A fim de prover subsídios suficientes para esta avaliação, efetuou-se uma detalhada coleta de informações e dados, não se limitando àqueles que foram fornecidas pelo TSE. Nesta coleta destacam-se as seguintes atividades:

- leitura e interpretação minuciosa dos programas-fonte da UE;
- compilação dos programas completos e de partes deles para testar funções específicas;
- simulação de eleições tanto nas UEs como em computadores de uso geral (PCs) usando os programas da UE;
- interrupção forçada e reinício do software de votação sob diversas circunstâncias e em momentos variados do processo;
- análise detalhada das estruturas de dados usadas pelos programas e seus conteúdos antes, durante e após uma votação;
- análise detalhada de todos os arquivos presentes nos cartões de memória *flash* e disquete da UE antes, durante e após uma votação.

4.2 O hardware da urna

O hardware da UE se diferencia a cada nova eleição desde 1996, incorporando as melhorias oferecidas por novas tecnologias. Entretanto, sua estrutura fundamental permanece a mesma, pois todas as versões são

basicamente constituídas de uma placa-mãe similar à de um computador pessoal comum, acrescida de periféricos e circuitos adicionais de suporte.

Os circuitos de suporte compreendem uma fonte de alimentação, uma bateria, sensores (para monitorar o funcionamento de vários componentes da UE, como bateria e impressora, por exemplo) e um microcontrolador para gerenciar todos os sensores e alertar o processador principal em caso de ocorrência de situações anormais. Este microcontrolador tem ação limitada no sistema e não tem condições de acessar os dados manipulados pelo processador principal e gravados nos cartões de memória. Entretanto, ele é responsável pelo controle do teclado do terminal do eleitor, enviando ao processador principal o código das teclas pressionadas. Como o código destas teclas é passado ao programa de controle de votação e este os repete na tela da UE para confirmação pelo eleitor, qualquer mecanismo de adulteração de teclas no microcontrolador deveria contar com outro mecanismo equivalente no programa de controle de votação, o qual seria percebido em um exame do código-fonte.

O teclado reduzido da UE corresponde a algumas das teclas de um teclado convencional. Ele é desabilitado automaticamente quando os circuitos internos detectam que um teclado externo (padrão PS/2) está conectado a um conector existente na parte traseira da UE. Este teclado externo é usado em ocasiões de manutenção e testes. O uso de lacres físicos impede seu uso após a inseminação da urna.

A bateria interna objetiva manter a UE em funcionamento por várias horas em caso de queda de energia, sem perda dos dados da votação existentes no momento da perda da alimentação externa. Os testes realizados em três urnas mostraram que não houve perda de dados quando se suprimiu a alimentação de corrente alternada (127 VAC) das mesmas.

O monitor (*display*) é de cristal líquido monocromático com vários tons de cinza, o que possibilita uma boa e nítida visualização da foto do candidato. Tanto o monitor como seu software de acionamento (*driver* de vídeo) comportaram-se normalmente nos testes, isto é, reproduzindo fielmente na tela os dados que foram enviados pelo programa de votação.

Não foi notado nos testes nenhum comportamento fora do esperado, seja no monitor seja no seu software de acionamento (*driver* de vídeo).

Na placa-mãe da UE há uma memória EEPROM com o código principal do BIOS e sua extensão. Esta extensão modifica a forma de inicialização (*boot*) do sistema, inibindo o *boot* via disquete e forçando-o a ser feito via cartão de memória *flash* especialmente configurado para tal.

Na memória EEPROM também reside o número de série da UE, que é usado no rastreamento da mesma e no preenchimento da tabela de correspondência (que associa a UE a uma determinada seção eleitoral durante a inseminação). Este número de série também é usado na criação da chave simétrica de ciframento do boletim de urna e poderia ser usado na criação de chaves criptográficas que viabilizassem a assinatura digital do

boletim e de outras informações geradas na UE, como a lista de justificativas, por exemplo.

Apesar das pequenas diferenças entre o hardware da UE e o de um microcomputador comum, seus comportamentos são similares quando são inicializados por um sistema operacional como o VirtuOS, por exemplo.

Nem todo o hardware está documentado em detalhes, mas há alguns pontos que podem ser ressaltados, tais como:

- existência de *jumpers* que, se mudados, permitiriam a reescrita e/ou apagamento do BIOS na *flash* EEPROM: os programas da UE verificam a configuração destes *jumpers* como parte da inicialização;
- uso de soquete para conectar a *flash* EEPROM, o que facilitaria sua troca, já que não está soldada: os programas da UE também verificam a integridade da *flash* EEPROM do BIOS;
- existência de conectores na placa-mãe que não têm função totalmente esclarecida: tais conectores não são acessíveis externamente, o que torna inviável uma eventual exploração de suas funcionalidades.

A adoção de cartões de memória *flash* em substituição a discos rígidos mecânicos convencionais trouxe benefícios para a UE, pois a tornou mais robusta a choques mecânicos sofridos durante sua distribuição pelas seções eleitorais, facilitou o processo de instalação de programas e facilitou a retirada do disco (representado pelo cartão) de uma UE defeituosa e sua inserção em uma UE de reserva para dar continuidade à eleição.

4.3 O desenvolvimento do código-fonte

Desde 1996 é publicado, a cada nova eleição, um edital que prevê a construção de novas urnas e o desenvolvimento do software para estas e para as já existentes. O software já está bem estável e só tem sofrido modificações decorrentes de alterações na legislação e de inclusão de novas funções de segurança.

Mesmo havendo, por parte do TSE, o acompanhamento do desenvolvimento do software da UE pela empresa contratada, os detalhes de programação que implementam as funções requeridas, tanto nas novas urnas a fabricar como nas já existentes, ficam a cargo da equipe da empresa.

Ao ser entregue ao TSE, este conjunto de programas passa por uma série de testes que avaliam suas funcionalidades frente às especificações do edital e, dependendo do resultado destes testes, podem ocorrer várias interações com a empresa até que o processo convirja para uma versão considerada satisfatória. Nesta etapa final de desenvolvimento, a equipe de desenvolvedores da empresa se transfere para o TSE e passa a executar o trabalho final de desenvolvimento dentro de suas dependências. Entretanto,

não existe um procedimento formal no TSE para validação e aceitação do código-fonte dos programas.

Numa fase final, os programas passam à sessão de apresentação aos partidos durante um período de tempo determinado. Nesta sessão todos os arquivos que constituem o software da UE são gravados em um meio não volátil (CD-ROM), o qual é lacrado e assinado por todos os presentes à sessão de apresentação. Após este período, não há mecanismos simples e eficazes que permitam que representantes de algum partido, em qualquer lugar do país, possam confirmar que os programas usados na UE correspondem fielmente aos mesmos que foram lacrados e guardados no TSE, exceto através de uma auditoria.

A combinação das versões de treinamento e simulação com as versões oficiais do programa em um mesmo código-fonte dificulta o seu exame na sessão de apresentação pública, apesar de facilitar sua manutenção. A análise dos programas pelos representantes dos partidos seria mais eficiente e produtiva se houvesse a separação dos códigos oficiais daqueles de treinamento e simulação.

4.4 O processo de compilação do código-fonte

Para a compilação final dos programas da UE é utilizado o mesmo ambiente comercial padrão empregado no desenvolvimento (Borland C versão 4.5), o que permitiria, em princípio, a reprodução do processo de compilação em instalações independentes. Neste processo, o TSE substitui rotinas fictícias de criptografia (usadas pela contratada para testes de ciframento do BU) pelas rotinas finais de criptografia, em código-objeto, desenvolvidas para uso específico na UE.

Além disto, é incluída no momento de compilação uma biblioteca com as rotinas que provêem suporte para o ambiente multiprogramado do sistema operacional VirtuOS (biblioteca para uso de múltiplas *threads* do VirtuOS). Esta biblioteca é fornecida pela Microbase em código-objeto (LMVOS.LIB).

Estando prontos os códigos-fonte e as rotinas adicionais, é feita então a compilação e ligação dos módulos que compõem o software de votação da UE.

O uso de um compilador convencional disponível no mercado é um ponto positivo, já que permite uma avaliação independente usando-se um compilador idêntico, mas adquirido separadamente.

Entretanto, o uso de uma biblioteca cujo código-fonte não é aberto, como as bibliotecas de criptografia e de suporte a múltiplas *threads*, inviabiliza uma avaliação completa, já que é difícil determinarem-se as funcionalidades de um programa baseando-se apenas em seu código executável correspondente. Pelo exame do código-fonte dos programas da UE, constata-se que a biblioteca de criptografia é utilizada somente no fim da

eleição, momentos antes da impressão do BU, o que dá margem a alguma discussão sobre o impacto das operações realizadas pela mesma. Este ponto será mais discutido em seções seguintes.

4.5 Os mecanismos de verificação de integridade de arquivos

Após a compilação dos programas, é iniciada uma etapa de preparação de resumos criptográficos (funções *hash*) que ajudarão a verificar a integridade dos arquivos de programas e de dados durante o restante do processo da eleição.

Os algoritmos de resumo criptográfico (funções *hash*) utilizados são:

- Message Digest 5 (MD5): é universalmente adotado e de conhecimento público; fornece o resumo criptográfico de 128 bits a partir de um conjunto de dados de tamanho arbitrário; apesar de ser um algoritmo adequado para as aplicações em questão, sugere-se uma avaliação sobre a possibilidade de uso nas urnas atuais de um algoritmo mais robusto, como o SHA-1, por exemplo;

- ASSINA: é uma função não pública desenvolvida pela Microbase, que implementa um resumo criptográfico de 256 bits; é usada principalmente para gerar o resumo e garantir a integridade e a autenticidade (já que não é pública) de um conjunto de resumos criptográficos gerados pelo MD5.

Estes dois algoritmos são empregados da forma descrita a seguir.

Usando o algoritmo convencional (MD5), é calculado um resumo criptográfico para cada arquivo da árvore de diretórios da aplicação de votação. Os nomes dos arquivos e seus resumos são gravados, um por linha, num arquivo com extensão .CRC. Para prover um nível extra de segurança, é calculado também o resumo criptográfico (com o algoritmo ASSINA) de cada arquivo .CRC, o qual é guardado em um outro arquivo com extensão .SIG.

Estes resumos são verificados pelos programas executados durante a inseminação da UE e todas as vezes em que ela sofrer uma inicialização (*boot*). Esta verificação também é realizada durante a execução de alguns programas que compõem o aplicativo de votação.

Qualquer modificação feita em algum arquivo da UE que não seja acompanhada pela correspondente modificação dos arquivos .CRC e .SIG será detectada, já que os procedimentos de verificação recalculam os resumos e os comparam com aqueles que foram gravados nos diretórios na época da criação dos mesmos.

Como o mecanismo de verificação de integridade e autenticidade dos arquivos está embutido dentro da própria UE, torna-se difícil criar um esquema totalmente seguro, já que os parâmetros de verificação estão

contidos dentro da própria estrutura a ser verificada (neste caso, nos cartões de memória *flash*). Esta verificação poderia ser aprimorada com a adição de um mecanismo externo independente, o qual é objeto de recomendação deste relatório.

Conclui-se que a combinação do uso das técnicas públicas e proprietárias de resumo criptográfico torna muito difícil o sucesso de qualquer tentativa de modificação posterior dos programas executáveis sem que tal tentativa seja detectada. Toda a segurança do mecanismo de verificação de integridade e autenticidade empregado se baseia no segredo do algoritmo de resumo criptográfico ASSINA responsável pelos 256 bits guardados nos arquivos .SIG.

4.6 O sistema operacional residente na urna

A UE tem usado desde sua primeira versão (UE-96) o sistema operacional VirtuOS, desenvolvido pela empresa brasileira Microbase. Trata-se de um SO compatível e muito similar ao MS-DOS, mas que contém uma gama de recursos extras que o tornam adequado a aplicações industriais de tempo real.

O VirtuOS possui as funcionalidades do MS-DOS e oferece recursos adicionais, como processamento concorrente (*threads*), por exemplo.

Deve ser observado que o VirtuOS usado recebeu algumas extensões a fim de satisfazer vários requisitos previstos no edital da UE. Estas extensões levam em consideração as especificidades da arquitetura da urna, bem como provêem rotinas auxiliares para verificação de integridade de dados.

Não é só nas extensões que o sistema operacional da UE difere de uma versão de mercado. O TSE informou que o sistema operacional empregado na UE é uma variante da versão *embedded* do mesmo. Esta variante está identificada por um número de versão específico contido dentro do arquivo do sistema.

O fato da UE não se basear integralmente em um sistema operacional idêntico a um disponível no mercado pode gerar dúvidas quanto à segurança e não é uma prática recomendável.

Nota-se ainda que não há no TSE um procedimento formal de verificação detalhada do código das extensões do sistema operacional, adicionalmente aos testes funcionais da UE.

4.7 O empacotamento e a transferência do software da UE

O carregamento do software nas UEs (inseminação) é feito de forma descentralizada. Com a finalidade de preparar os programas da UE para serem enviados aos TREs, é realizado um processo de empacotamento no TSE com a ajuda de funcionários da empresa Módulo. Este processo

consiste no agrupamento de todos os programas necessários para o funcionamento da UE, acrescidos de parte dos dados necessários (cadastro de eleitores, por exemplo). Outra parte dos dados precisa ser inserida em cada TRE de acordo com as candidaturas da região.

O pacote é cifrado e transmitido aos TREs e pólos de inseminação via rede (FTP) ou enviado em CD-ROM dos TREs aos pólos que não têm conexão à rede. Devido ao uso de criptografia sobre todo o conteúdo do pacote, é extremamente improvável que os programas possam ser substituídos ou alterados, desde que haja uma política apropriada de criação, distribuição e manutenção de senhas. O algoritmo de criptografia adotado nesta etapa é o IDEA-128, bastante documentado na literatura e considerado adequado para este propósito.

Além da proteção provida pela criptografia de todo o pacote, deve ser lembrado que cada arquivo nele contido está também protegido pelos resumos criptográficos descritos anteriormente.

Após a chegada do pacote nos TREs, ele é decifrado, é aberto e fica armazenado sob a proteção de acesso provida pelo Subsistema de Instalação e Segurança (SIS) e pelo sistema operacional nativo (Windows NT 4.0).

Um ponto a se notar aqui é o acesso ao código binário da UE por funcionários de uma empresa. Entretanto, esta é contratada sob cláusula de sigilo e este trabalho de empacotamento é feito nas dependências do TSE. Nota-se também a inexistência de um procedimento mais formalizado para esta fase.

4.8 O Subsistema de Instalação e Segurança (SIS)

O SIS, da empresa Módulo, é uma das ferramentas básicas de segurança do SIE e é empregado nos computadores do TSE, dos TREs e dos pólos de inseminação de UEs com o objetivo de controlar de forma mais rigorosa o acesso e as operações feitas pelos usuários destes computadores.

O SIS provê uma forma mais sofisticada de controle de acesso ao sistema de arquivos do que o sistema operacional nativo (MS Windows NT), oferecendo um nível extra de proteção e auditoria. Este nível extra de proteção se inicia com a instalação de todo o SIS, a qual é feita concomitantemente com a instalação do sistema operacional.

Para usuários comuns cadastrados no sistema, o controle de acesso ao computador controlado pelo SIS não é distinto daquele normalmente encontrado em uma instalação com Windows NT: o usuário precisa fornecer uma identificação (número do título de eleitor) e uma senha.

Entretanto, para que um usuário do grupo de administradores do sistema (usuário com controle total sobre o sistema) possa ter acesso ao mesmo, ele terá que fornecer várias informações: a identificação do papel que ele irá assumir (administrador, suporte etc), a senha correspondente a esta

identificação, sua própria identificação (número do título de eleitor), sua senha individual e uma contra-senha, que deve ser solicitada por telefone ao TRE no momento do acesso e que só é válida para um único acesso. Novas tentativas de acesso necessitarão de novas contra-senhas.

A contra-senha é formada por oito caracteres alfanuméricos e é calculada com base nas informações descritas acima e em outras (identificação do computador, data, hora, identificação do operador, código de operação e município) que o usuário deve fornecer por telefone ao TRE. Após a confirmação de todas as informações fornecidas, a contra-senha é calculada, registrada e informada pelo TRE ao usuário.

A necessidade desta contra-senha é um dos pontos importantes da segurança provida pelo SIS, pois ela permite ao TRE ter um controle preciso sobre quem (e quando) está tendo acesso privilegiado a um computador sob a proteção deste sistema. Trata-se de um mecanismo paralelo e independente para registro de operações de *logon* sensíveis no sistema e que não está sob o controle dos administradores locais do mesmo.

Além do controle de acesso, o SIS possui outras funções importantes para a segurança. Ele cuida de coletar informações detalhadas sobre as operações que os usuários realizam no computador de forma a permitir uma auditoria posterior. As informações registradas são guardadas em um diretório específico sem permissão de acesso para usuários que não sejam administradores do sistema. Além disso, estes registros estão protegidos por assinaturas digitais que impedem sua modificação indevida.

A segurança provida pelo SIS é reforçada pelo controle físico de acesso ao equipamento.

Conclui-se que, por suas características, o SIS permite a criação de um ambiente de trabalho homogêneo e disciplinado em todos os computadores onde for instalado (TREs, pólos de inseminação etc).

4.9 A geração de mídia e a inseminação da UE

O pacote de software recebido do TSE é usado por um programa chamado Gerador de Mídia, que é o encarregado de gravar em cartões de memória *flash* e disquetes as informações necessárias para a preparação (inseminação) de uma UE. São gerados cartões de memória *flash* com dois tipos distintos de conteúdos (*Flash* de Carga, FC, e *Flash* de Votação, FV) e vários tipos de disquetes, que determinam o modo de operação da UE. Uma única FC será usada na inseminação de várias UEs, mas para cada uma delas será preciso um disquete e uma FV.

Quando se liga a UE com uma FC instalada, ocorre a inicialização da UE, seguida de uma série de testes de integridade dos programas.

O processo de inseminação continua com a cópia do conteúdo da FC para a *flash* interna (FI). Em seguida, o programa de inseminação solicita a

inserção da FV e do disquete na UE para fazer testes adicionais de integridade e de correção dos dados. Tendo sido concluído o processo com sucesso, os *slots* de acesso ao conector do cartão *flash* e ao disquete são lacrados com lacres oficiais numerados. A partir de então não há forma de se ter acesso aos dados e programas armazenados nos cartões FI, FV e no disquete sem que se rompam os selos de lacração. No caso de haver necessidade de manutenção, o processo de inseminação é repetido e a urna é relacrada.

Após a inseminação das urnas associadas a uma FC, esta volta ao programa Gerador de Mídia, levando dados relativos à correspondência entre urnas e seções eleitorais. Neste momento, há uma verificação adicional da integridade da *flash* de carga.

Deve-se notar que o processo de inseminação é de difícil controle dada a grande quantidade de urnas, grande número de pessoas envolvidas e sua distribuição geográfica. Apesar de os partidos políticos poderem acompanhar o processo de inseminação, de acordo com as informações do TSE, o acompanhamento não é realizado integralmente durante todo o processo, já que o mesmo é bastante demorado e repetitivo. Entretanto, os representantes dos partidos podem solicitar um teste de funcionamento em até 3% das urnas, escolhidas aleatoriamente após a inseminação. Não há obrigatoriedade da realização deste teste, mas as urnas que são testadas são re-inseminadas.

Nota-se também que durante o processo de inseminação é relativamente grande o número de pessoas com acesso aos cartões FC. Mesmo assim, os testes de integridade acima citados, aliados a um controle físico sobre cada cartão de memória *flash* (de carga e de votação), tornam improvável qualquer manipulação do seu conteúdo. Esta questão é objeto de recomendação neste relatório.

4.10 A preparação da urna para o segundo turno

Para o segundo turno da eleição a urna não é re-inseminada. O programa aplicativo é o mesmo utilizado no primeiro turno das eleições, sendo necessário apenas informar a lista de candidatos para o segundo turno. A preparação da urna é feita com o uso de um disquete específico que contém o arquivo de candidatos para segundo turno, um *script* usado para atualização dos arquivos internos de candidatos e arquivos de controle usados para verificação da integridade e autenticidade do disquete. Esse mesmo disquete é utilizado para gravação do boletim de urna no final da votação, já que ele permanece lacrado dentro da urna.

Uma vez que os lacres da urna, exceto o do disquete, são preservados entre o primeiro e o segundo turno, e que a urna não pode ser inicializada pelo disquete, conclui-se que os programas originalmente carregados no processo de inseminação não podem ser alterados. Assim, a verificação da integridade e autenticidade do disquete de preparação para o segundo turno

por esses programas, confere a esta verificação a mesma confiabilidade dada à verificação realizada na inseminação.

Entretanto, verificou-se que a utilização de um arquivo de *script* (.BAT), introduzido na UE via o disquete para cópia do arquivo de candidatos, não seria necessária uma vez que o *script* utilizado para inicialização da urna poderia ser alterado para incluir esta tarefa.

A execução de um arquivo de *script* externo é um ponto sensível na segurança da UE. Uma eventual alteração do *script* transferido do disquete para o *flash card* interno, que fosse acompanhada da correta alteração dos arquivos utilizados para verificação da integridade e autenticidade do disquete, possibilitaria a execução de programas externos ou a transferência de arquivos para o interior da urna de forma não prevista.

A segurança seria aprimorada pela alteração do *script* interno. Esta questão é objeto de recomendação neste relatório.

4.11 Software do aplicativo

O programa de votação é constituído de múltiplas *threads* (também chamadas de "processos leves" ou "linhas de execução"), que são disparadas a partir do processo principal ou de outros processos. A utilização de um sistema operacional com suporte a *threads* garante o atendimento das condições impostas pela aplicação, isto é, a execução simultânea de tarefas e a manutenção de informações necessárias para a retomada da eleição em caso de falhas.

A manutenção de cópias atualizadas das principais estruturas de dados da aplicação (matriz de partidos, matriz de candidatos, matriz de eleitores) armazenadas em memória não volátil (cartões de memória *flash*) permite a retomada da aplicação do ponto de interrupção sem perda de informações. A utilização de arquivos em duplicata para essas estruturas, armazenados na *flash* interna e na *flash* de votação, garante a retomada da aplicação mesmo no caso de necessidade de substituição da urna eletrônica.

A clara separação entre programas e dados confere grande flexibilidade à aplicação, permitindo a uniformização do aplicativo para todas as seções eleitorais do país e a manutenção de um núcleo relativamente estável e adaptável para diferentes eleições.

A execução controlada e supervisionada do aplicativo de votação mostrou que a contabilização dos votos introduzidos foi feita corretamente.

A análise do código-fonte e das estruturas de dados utilizadas mostrou que há um alto grau de relacionamento e redundância dos dados das estruturas (matrizes) que armazenam a soma dos votos dos candidatos e legendas, o que permite a verificação da consistência dos mesmos, e que a posição na memória RAM dos dados de um determinado candidato depende da ordem

da lista de candidatos e de uma alocação dinâmica de memória feita pelo sistema operacional.

Além disso, considerando que o aplicativo de votação é único em todas as urnas eletrônicas, pode-se concluir que modificações do programa (originadas por código clandestino ou ação do sistema operacional) que levassem à manipulação do conteúdo de posições específicas da matriz de acumulação não seriam efetivas no sentido de alterar consistente e uniformemente o resultado de uma eleição.

Foi possível observar também que não há registros que vinculem a identidade do eleitor com os votos registrados. Em cada novo ciclo de votação (ou seja, a cada eleitor), os votos introduzidos são armazenados temporariamente na mesma região de memória RAM onde foram armazenados os votos do eleitor anterior, sobrepondo-os. Não há registros em outro meio de armazenamento (cartões de memória *flash* ou disquete) dos votos do eleitor.

Assim que o ciclo se encerra (o último voto do eleitor é introduzido), o programa atualiza as tabelas de totalização da urna e as grava imediatamente nos cartões de memória *flash* interna e de votação (FI e FV). Desta forma, no caso de haver algum tipo de falha que interrompa o funcionamento da urna, todas as informações correspondentes à totalização até o momento da falha estão duplamente gravadas, o que permite sua recuperação e o prosseguimento da eleição.

Como conclusão pode-se afirmar que a estrutura da aplicação:

- é adequada ao processo eleitoral, visto que atende os requisitos essenciais de correta contabilização e manutenção de sigilo dos votos;
- é robusta quanto à recuperação de falhas sem perda de informações;
- proporciona a uniformização dos programas da urna eletrônica para todas as seções eleitorais.

4.12 Uso de técnicas criptográficas

Técnicas criptográficas são usadas em várias fases do processo, desde a instalação de software nos TREs e a inseminação de urnas até a execução dos programas e emissão do BU.

O maior uso destas técnicas está ligado ao cálculo dos resumos criptográficos (*hash*) para verificação de integridade e autenticidade dos arquivos da urna, como descrito em seções anteriores.

O protocolo utilizado no ciframento do BU é padrão, ainda que os algoritmos empregados sejam sigilosos. As informações obtidas indicam tratar-se de algoritmos robustos.

Pela análise do código-fonte do aplicativo de votação, constatou-se que o processo de ciframento com os algoritmos de criptografia secretos só é usado ao final da eleição, momentos antes de se imprimir o BU.

Antes de ser impresso, o BU em claro e cifrado é gravado nos cartões FI e FV e no disquete, juntamente com outros arquivos de interesse tais como os de eleitores faltosos e de justificativas. Em seguida o aplicativo envia para a impressora o arquivo com o BU claro e várias cópias do mesmo são impressas.

Grande parte da polêmica que tem surgido em torno do uso de algoritmos de criptografia secretos para cifrar o BU se deve ao fato de não se ter certeza de que tais algoritmos não modificariam os resultados antes dos mesmos serem divulgados. Experimentos realizados com o programa de votação mostraram, pela verificação da data e horário de acesso dos arquivos de resultados, que tal fato não ocorre. Isto foi comprovado também pela comparação de um arquivo adicional (gerado por uma versão modificada do programa de votação), obtido antes da chamada da função de criptografia, com os arquivos que contêm o BU claro armazenados na FI, FV e disquete.

A desconfiança com relação à manipulação do BU pelo algoritmo de criptografia poderia ser minimizada com a simples inversão na ordem dos procedimentos finais, fazendo com que a impressão (divulgação) do BU ocorresse antes da chamada às rotinas de criptografia.

Como será mencionado na seção seguinte, acredita-se que seria possível criar um mecanismo de assinatura digital (com código verificável) para a proteção da integridade do BU e para a garantia da autenticidade de sua origem, uma vez que cada UE possui uma identificação única (em EEPROM) da qual poderiam ser derivadas chaves públicas e privadas. Esta questão é objeto de recomendação neste relatório.

4.13 O boletim de urna e seu transporte

Antes de ser copiado no disquete para transmissão, o boletim de urna (BU), que contém os resultados da eleição é criptografado. A criptografia não é usada com o objetivo de manter o sigilo do BU, uma vez que o mesmo já foi impresso e divulgado na seção. O objetivo do ciframento é criar um BU que possa ter sua autenticidade e integridade verificadas no destino: se ele puder ser decifrado corretamente no destino é porque foi cifrado sob as condições previstas, isto é, com um algoritmo e chave pré-estabelecidos pelo TSE; isso previne a alteração do BU no trajeto até o totalizador e a confecção de BUs espúrios. Apesar de uma imagem aberta (não cifrada) do BU ser gravada no disquete que vai para a totalização, somente a versão cifrada é usada no cômputo de votos.

A criptografia poderia ser empregada apenas para fazer uma assinatura digital do BU com uma chave privada que fosse única em cada urna e a

identificasse nas etapas de totalização. Como cada UE possui um número de série único, acredita-se que é possível projetar um mecanismo que viabilize o uso de assinatura digital de forma confiável.

Deve ser ressaltado que um mecanismo de assinatura digital baseado em criptografia de chave pública provê garantia de integridade e autenticidade, mas não de sigilo. Se um mecanismo deste tipo fosse empregado, o BU passaria a ser um arquivo aberto e legível por qualquer indivíduo com acesso ao disquete e/ou ao transportador. Neste BU seria anexada uma sequência de caracteres (assinatura digital) que seria totalmente dependente e acusaria qualquer modificação do texto contido no mesmo. Como o BU é um documento público que já foi divulgado na seção eleitoral e como uma cópia do BU claro já é atualmente inserida no disquete que vai para o totalizador, entende-se que não haveria problemas na mudança do formato de gravação do BU no disquete.

Um outro aspecto notado é que, na totalização, não se faz teste de consistência da chave simétrica que foi gerada na UE para o ciframento do BU, ainda que o totalizador tenha as informações necessárias para a reconstrução da mesma. Esta chave, cifrada com a chave pública do TRE, acompanha o BU. Se esta consistência fosse verificada, teria-se uma garantia a mais da autenticidade do BU recebido, já que o mecanismo de criação da chave simétrica não é público.

Por outro lado, o ciframento de um BU com uma chave que não fosse gerada da forma esperada é improvável, pois exigiria a obtenção do código do algoritmo secreto de criptografia, que é parte de um programa executável armazenado dentro de um cartão de memória *flash*. Além disto, o recebimento de mais de um BU de uma mesma seção é detectável e pode ser auditado. De acordo com informações do TSE, é comum a retransmissão do BU de uma mesma urna devido a problemas técnicos (atrasos na rede, por exemplo) e erros de operação. Nestes casos a chegada no sistema de totalização de mais de um BU válido de uma mesma seção é registrada para posterior averiguação.

4.14 A totalização

Apesar de toda a complexidade envolvida no processo de totalização, a verificação da corretude dos resultados deste processo não se caracteriza como problema de difícil solução, visto que não apresenta a mesma característica de sigilo imposta pela UE.

Segundo informações fornecidas pelo TSE, após as eleições é possível obter-se um CD contendo cópias de todos os BUs do país. Este fato, aliado à impressão e distribuição de várias cópias dos BUs em cada seção imediatamente após o encerramento da eleição, permite a verificação (ainda que por amostragem) da autenticidade dos dados contidos no CD. Feita esta verificação, torna-se possível uma totalização paralela (externa) e a conferência dos resultados finais publicados pelo TSE.

Para esta totalização paralela, o próprio TSE poderia disponibilizar sugestões de programas (em código-fonte), os quais seriam cuidadosamente avaliados e testados pelos interessados.

Como a oficialização do resultado leva cerca de uma semana, somente após este período é que os BUs podem ser publicados oficialmente em CD e estão em condições de serem usados em uma totalização paralela. Entretanto, para efeito da verificação da autenticidade dos dados, entende-se que já é possível para o TSE divulgar via Internet os BUs à medida em que vão sendo recebidos, o que permitiria um acompanhamento e conferência no momento de interesse máximo da população e dos partidos.

O software totalizador é baseado em um banco de dados cujo acesso é controlado por meio de senhas. Na oficialização deste totalizador, o banco de dados é zerado, as chaves privadas necessárias para decifrar os BUs são atualizadas e medidas extras de segurança são tomadas. Estas medidas incluem, entre outras, a desativação de serviços de rede tais como *telnet* e FTP.

Entretanto, não existe um procedimento formal que exija a alteração das senhas já existentes neste sistema, a fim de se criar uma proteção contra o eventual comprometimento (quebra) de alguma delas. O início de uma totalização oficial na qual todas as senhas envolvidas tivessem sido trocadas seria certamente mais seguro. Deve ser lembrado, no entanto, que uma totalização paralela, como a sugerida anteriormente nesta seção, permitiria detectar qualquer problema que ocorresse com a totalização oficial.

4.15 A rede de computadores do TSE

A rede privada do TSE, que interliga todos os TREs e provê conexão à Internet, é uma rede WAN complexa, provida basicamente por *links* da Embratel. Seus *links* internos variavam, em 2000, de 64 Kbps a 1 Mbps, com um total de 4 Mbps de conexão com a Internet.

Devido à grande cobertura territorial necessária para alcançar todos os TREs e respectivos pólos, a rede do TSE apresenta grande capilaridade, sem necessariamente apresentar grande volume de tráfego interno.

Internamente, o ambiente de computação do TSE obedece rígida política de segurança, com compartimentalizações em sub-redes de regiões mais críticas.

Durante a eleição, a rede do TSE é fisicamente isolada e a integridade da rede privada utilizada durante a apuração é garantida pelo isolamento e fiscalização do acesso à infraestrutura. Uma solução de *firewall* provê facilidades de comunicação e de isolamento controlado entre a rede privada e a Internet.

Este isolamento é importante e necessário, visto que a existência de uma conexão à Internet traria preocupações sob o ponto de vista da segurança.

A topologia de rede empregada não contempla um cenário de segurança mais rígido por incluir diversos servidores de todo o TSE nas VLANs segregadas. Entretanto, a transmissão do software da urna recebe atenção especial do fabricante e do TSE: por acordo mútuo decidiu-se pela utilização do PGP como meio seguro de transporte, o que é adequado, desde que a geração e manutenção das chaves seja feita corretamente. Além disso, há registros dos eventos e uso de proteção criptográfica (sigilo e autenticação).

Após a recepção do código final da urna, o mesmo é expandido na forma de sua hierarquia original de arquivos, ficando residente no computador de recepção, localizado na SVI (Seção do Voto Informatizado) do TSE.

Adicionalmente às proteções de acesso via rede, uma forma de se garantir a integridade do software nesta fase é a adoção de uma política rigorosa de assinaturas de código, começando no fabricante. Na eventualidade de corrupção acidental ou intencional de algum arquivo, a verificação das assinaturas por ocasião da compilação final do software detectaria qualquer alteração, impedindo sua propagação.

O *firewall* do TSE segue uma topologia particular e utiliza várias redes de perímetro, também conhecidas como DMZs (abreviação da expressão em inglês para "Zona DesMilitarizada"). Conta com os tradicionais serviços públicos (servidores Web, FTP e e-mail) e com os de apoio à Internet (DNS e *proxy*). Para acompanhamento da segurança dispõe também de IDS (Intrusion Detection System).

Observa-se uma cultura local própria na área de segurança, com a presença de soluções comerciais lado-a-lado com soluções de projeto próprio da equipe do TSE. Nota-se atenção especial dedicada ao atendimento de cada serviço Internet. A utilização de diversas DMZs provê uma segurança extra à rede interna, mas uma reorganização da topologia e uma maior exploração das funcionalidades dos elementos traria benefícios extras à segurança da rede.

5 RECOMENDAÇÕES

Como resultado da avaliação realizada, é apresentado nesta seção um conjunto de recomendações cujo objetivo é o aumento da segurança e da confiabilidade do Sistema Informatizado de Eleições, em especial de seu componente mais sensível que é a urna eletrônica. Deve-se ressaltar que a necessidade de preservação do sigilo do voto torna o processo de segurança da urna eletrônica mais difícil e complexo quando comparado a outros sistemas de informação.

Um sistema seguro e confiável deve contemplar as seguintes características:

- dificuldade de ser violado;
- detectabilidade;
- rastreabilidade;
- recuperabilidade.

Técnicas comumente usadas para o desenvolvimento de sistemas seguros e confiáveis baseiam-se em diferentes formas de proteção, sendo as mais comuns:

- proteção física;
- sigilo de informações;
- uso de técnicas criptográficas e de resumo digital;
- registros de ações e atividades realizadas (*logs*);
- auditorias.

A segurança da urna eletrônica está fundamentada numa combinação destas formas de proteção, destacando-se:

- desenvolvimento estanque do sistema;
- conhecimento individual limitado do sistema;
- instalações padronizadas de ambientes computacionais nas diversas instâncias (TSE, TREs, pólos, zonas eleitorais etc) e registro sistemático dos acessos e das atividades realizadas nesses sistemas;

- utilização de contra-senhas, registradas no TSE e nos TREs, para usuários com maior poder de acesso aos sistemas (administradores);
- acesso controlado aos componentes físicos (computadores, *flash cards*, urnas etc);
- proteção da integridade do software da urna baseada em resumos criptográficos dos arquivos executáveis, dos arquivos de dados e da estrutura de diretórios;
- geração de arquivos de *log* para todos os eventos da urna eletrônica.

A combinação dessas formas de proteção tem como resultado a criação de uma barreira de segurança de difícil transposição. Mesmo que cada uma das formas de proteção possa ser individualmente superada, a superação do conjunto é pouco provável, dados a extensão e a profundidade do conhecimento necessário e o grande número de participantes cujo envolvimento seria requerido para a sua realização.

É importante observar, entretanto, que, em uma estrutura hierárquica de distribuição do software como a da urna eletrônica, eventuais quebras do sistema de segurança teriam diferentes níveis de dificuldade a superar e diferentes graus de impacto como resultado, dependendo do ponto exato e do momento em que a eventual quebra ocorresse.

O aumento do grau de segurança em um sistema informatizado está diretamente relacionado com o incremento das medidas e formas de segurança utilizadas. Esta relação, entretanto, não é linear; um grande aumento nas medidas de segurança pode resultar em redução pouco significativa do risco de quebra. Observa-se também que uma política de segurança extremamente rígida pode ter custos elevados e criar ambientes restritivos que afetem a produtividade e que até mesmo inviabilizem a realização de procedimentos essenciais da aplicação.

Entre as recomendações discutidas a seguir as apresentadas nas Subseções 5.4, 5.5, 5.6 e 5.7 são consideradas de grande relevância para o aumento da segurança do sistema de voto eletrônico. Sua implementação é fortemente recomendada para as Eleições de 2002.

5.1 Desenvolvimento dos aplicativos de votação baseados em blocos estáveis e permanentes para todas as eleições

Esta condição já é praticamente atendida para o sistema de voto eletrônico. Embora o desenvolvimento do aplicativo de votação venha sendo regularmente objeto de licitação, juntamente com a produção das urnas, observa-se que sua arquitetura e os programas que o constituem foram pouco alterados nos últimos anos, permanecendo estáveis e apresentando condições adequadas para serem considerados como ponto de partida no desenvolvimento de um sistema permanente e estável.

O sistema atual permite a geração de versões do programa de votação destinadas à votação oficial, ao treinamento de eleitores e ao treinamento de mesários. Todas estas versões são originadas do mesmo código-fonte e os blocos do programa-fonte selecionados por diretivas condicionais do compilador (compilação condicional) e variáveis de ambiente. Esta abordagem facilita a manutenção consistente do software mas dificulta a verificação que deveria ater-se à versão usada para votação oficial. Os programas-fonte para diferentes aplicações poderiam ser desenvolvidos separadamente para facilitar sua análise.

5.2 Formalização do ciclo de desenvolvimento do software

De um modo geral, o TSE deve formalizar o ciclo de desenvolvimento do software da urna e de outros programas em procedimentos e marcos. Um marco é a formalização da transição do software de um procedimento para outro.

Em cada marco, além dos testes funcionais, é mandatória a execução de procedimentos de segurança que garantam a manutenção da integridade e autenticidade do software durante a transição de uma fase para outra, como os listados a seguir:

- cálculo de um resumo criptográfico (com SHA-1, por exemplo) para cada componente de software transferido para o procedimento seguinte. O resumo de cada componente deve ser tornado público e oficializado dentro do TSE;
- para todos os componentes recebidos de procedimento anterior, deve-se computar o seu resumo criptográfico e comparar o valor obtido com o valor público e oficializado dentro do TSE. Diferenças entre esses valores devem ser verificadas e as causas que lhes deram origem identificadas;
- uma vez determinados os resumos criptográficos e verificada a integridade dos componentes recebidos, estes devem ser gravados em CD-ROM, que deve ser guardado em local seguro. Mesmo que, por praticidade, cópias dos componentes estejam armazenadas em diferentes meios magnéticos, uma versão em meio não alterável deve ser obrigatoriamente mantida por razões de auditabilidade.

5.3 Avaliação do código-fonte do núcleo do aplicativo e seus componentes acessórios por especialistas em informática independentes do TSE

A verificação do código-fonte do aplicativo e dos componentes acessórios por especialistas independentes do TSE contribui para o aumento da confiabilidade da urna eletrônica.

O eventual enfraquecimento da segurança decorrente da abertura do código-fonte para exame externo é compensado pela maior credibilidade conferida ao sistema pelo exame mais detalhado do codigo-fonte.

O conhecimento global do sistema por um indivíduo e a redução do nível de segurança decorrente deste fato podem ser evitados pela divisão do código em blocos funcionais e a definição de interfaces precisas entre estes blocos. Cada revisor teria acesso ao código-fonte de um único bloco funcional e o mesmo bloco funcional poderia ser revisto por mais de um revisor.

Cada bloco de código teria seu resumo criptográfico calculado pelo TSE antes de ser encaminhado para revisão e o seu valor divulgado. Este procedimento teriam como objetivo garantir a integridade do bloco, bem como sua autenticidade. Estes resumos seriam verificados no momento da compilação e ligação dos aplicativos.

O atual esquema que permite aos partidos políticos o exame dos programas-fonte deve ser mantido e aprimorado.

5.4 Compilação e determinação de resumos criptográficos dos arquivos em sessão pública

A compilação dos programas-fonte e o cálculo dos resumos criptográficos dos programas executáveis devem ocorrer na presença de representantes partidários e representantes de sociedades ou entidades com efetivo conhecimento de sistemas informatizados. Os resumos e os algoritmos empregados na sua determinação devem ser tornados de conhecimento público, possibilitando a verificação desses programas nas urnas eletrônicas durante o processo de inseminação.

A configuração do ambiente de compilação deve ser completamente documentada (software empregado e as respectivas versões, variáveis de ambiente, diretivas do compilador etc). Deve ser possível a reprodução do mesmo ambiente de compilação utilizando cópias do software empregado adquiridas no mercado.

A mesma condição aplica-se aos sistemas básicos que complementam a aplicação na urna eletrônica (sistema operacional e outros). Na impossibilidade de aquisição de cópias do mesmo software e versão no mercado, ele deve receber tratamento equivalente ao da aplicação e submetido ao processo de validação já discutido na subseção anterior.

Estes procedimentos têm como objetivo garantir a replicabilidade do processo de compilação e integração dos programas da urna eletrônica e subsidiar a auditoria do sistema. Devem ser disponibilizados recursos para que a compilação dos programas e cálculo dos resumos criptográficos possam ser feitos em paralelo por representantes dos partidos políticos, em ambientes gerados por eles mesmos, usando sistemas operacionais e compiladores comerciais.

5.5 Verificação, por representantes partidários, dos resumos criptográficos dos arquivos instalados nas urnas inseminadas

Como forma de reforçar a verificação de integridade e autenticidade dos programas da urna, por meio de um elemento externo, o acompanhamento do processo de inseminação por representantes partidários deve incluir a verificação do resumo criptográfico dos programas instalados nas urnas eletrônicas e não somente a verificação do funcionamento correto das urnas por simulação de eleição.

Após a inseminação da urna deve ser permitido aos representantes de partidos o acesso aos programas internos da urna para cálculo e verificação da conformidade de seu resumo com aquele divulgado ao final do processo de compilação.

De modo a não provocar atrasos ou inviabilizar o processo de inseminação, o mesmo índice hoje praticado (até 3%) de urnas a serem verificadas poderá ser mantido. Entretanto, considerando que várias urnas são inseminadas por uma única FC, a verificação não precisaria ser feita em mais de uma urna inseminada pela mesma FC. A urna a ser examinada deve ser escolhida aleatoriamente após a inseminação.

As urnas verificadas devem ser obrigatoriamente re-inseminadas, a fim de eliminar qualquer suspeita de alteração durante a verificação. Caso os representantes o desejarem, as urnas re-inseminadas poderão ser novamente verificadas.

Como sugestões para a implementação da verificação da autenticidade dos programas, podem ser consideradas as seguintes alternativas:

- utilização de um *flash card* externo que contenha um programa verificador;
- verificação do *flash card* interno em computador independente.

A melhor forma de implementação de tal verificação deve ser decidida pelo TSE com base nas implicações logísticas das alternativas e deve atender aos objetivos a que se propõe.

Em ambos os casos, como forma de reforçar a política de segurança, deve-se prever mecanismos que impeçam a cópia de programas da urna eletrônica durante o processo de verificação.

A distribuição de um programa fonte de verificação, que pudesse ser analisado e compilado independentemente, poderia facilitar e agilizar o trabalho de fiscalização. Alternativamente os programas verificadores poderiam ser desenvolvidos independentemente.

5.6 Revisão do procedimento de preparação da urna para o segundo turno

O processo de preparação da urna para o segundo turno das eleições deve ser alterado de forma a eliminar a execução de qualquer *script* externo armazenado no disquete.

Caso haja motivos para se preservar a atual forma de preparação da urna para o segundo turno, as seguintes ações devem ser realizadas:

1. a lacração do acionador de disquete, pela mesa receptora, após a retirada do disquete com o boletim de urna do primeiro turno;
2. a verificação por representantes de partidos da autenticidade dos disquetes preparados para o segundo turno da eleição, na ocasião da preparação e lacração da urna. A seleção de disquetes para verificação deve seguir critérios similares aos sugeridos em 5.5.

5.7 Impressão do boletim de urna antes do ciframento dos resultados da votação

Recomenda-se a alteração do programa de forma a imprimir o boletim de urna antes do ciframento dos resultados da votação. A seguinte seqüência deve ser executada:

1. uma imagem do boletim de urna é gerada e armazenada nos *flash cards* interno e externo e no disquete;
2. os boletins de urna são impressos;
3. o boletim de urna é cifrado e armazenado nos *flash cards* interno e externo e no disquete;

A publicação do resultado da votação antes de seu ciframento e transferência para o meio de transporte contribui para o aumento da confiança na urna eletrônica.

5.8 Substituição do uso de ciframento por assinaturas digitais como forma de autenticação dos Boletins de Urnas

Ainda que a impressão do boletim de urna antes do ciframento dos resultados contribua para o aumento da confiança na urna eletrônica, observa-se que todo mecanismo de autenticação digital deve envolver alguma informação sigilosa: a chave ou o algoritmo. Do ponto de vista de segurança do sistema é preferível que o segredo seja uma chave a um algoritmo, pois sendo o algoritmo conhecido, sua implementação pode ser verificada.

Na urna eletrônica o mecanismo de autenticação usado atualmente é dependente do sigilo do algoritmo de ciframento simétrico utilizado. A utilização de um algoritmo sigiloso, implementado por uma função ativada a partir do código executável do programa de votação, se por um lado facilita a implementação do mecanismo de autenticação para o elevado número de urnas utilizadas no processo eleitoral, por outro lado cria restrições à total revisão dos programas instalados na urna eletrônica.

A opção pela utilização de um algoritmo público de assinatura digital teria como conseqüência a obrigatoriedade da manutenção do sigilo da chave. A questão que se levanta nesse caso é a forma de proteção da chave, visto que quase 350.000 urnas são utilizadas no processo eleitoral.

A solução para esta questão demanda um estudo mais aprofundado que extrapola o escopo da avaliação realizada, e que deve considerar não somente as características de segurança dos algoritmos empregados, mas também os aspectos logísticos envolvidos na preparação das urnas e a abrangência geográfica do processo eleitoral.

Uma sugestão para a geração, distribuição e armazenamento das chaves e que leva em conta o procedimento de preparação das urnas é apresentado a seguir.

Durante a inseminação, um par de chaves, pública e privada, seria gerado para cada urna. A chave pública seria armazenada na tabela de correspondência no processo de inseminação e a chave privada seria armazenada na urna. O boletim de urna seria assinado ao final da votação com a chave privada armazenada na urna e verificado no totalizador usando a chave pública daquela urna, previamente recebida através da tabela de correspondência. Este esquema garante que um BU corretamente assinado veio realmente da urna indicada, mas requer que as tabelas de correspondência sejam recebidas pelo totalizador em tempo hábil para que os votos sejam contabilizados.

Quanto à chave privada da urna, há três alternativas que podem ser consideradas para seu armazenamento no *flash card* interno, por ordem crescente de dificuldade que elas impõem ao vazamento da chave:

- armazenamento em aberto;
- armazenamento cifrado por algoritmo conhecido: a chave é cifrada por um algoritmo de ciframento conhecido que usa como chave de ciframento os dados específicos de cada urna que estão armazenados internamente em memória EEPROM;
- armazenamento cifrado por algoritmo secreto: a chave fica armazenada de forma cifrada usando-se um algoritmo secreto.

A primeira alternativa seria suficiente se a inseminação da urna fosse sempre observada por fiscais e seguida de sua imediata lacração. A segunda alternativa garantiria que a chave não poderia ser inspecionada diretamente com a utilização de ferramentas simples, pois sua recuperação demandaria a

leitura de dados armazenados na memória EEPROM da urna. Finalmente, a terceira opção imporia maiores dificuldades ao vazamento das chaves pois além do acesso aos dados da urna exigiria o conhecimento do algoritmo de ciframento. Note-se que a terceira opção, embora utilize o sigilo do algoritmo como forma de proteção da chave privada, difere do mecanismo de autenticação hoje empregado, visto que o algoritmo sigiloso, cuja implementação não pode ser verificada, não seria aplicado ao boletim de urna, mas apenas à chave que o cifraria.

Como pode ser observado da sugestão de implementação apresentada, a autenticação do boletim de urna é uma questão complexa e reforça o fato de que a solução adotada não deve levar em conta apenas os aspectos computacionais do algoritmo, mas deve considerar, principalmente, a logística necessária para sua implantação no sistema eleitoral.

6 CONCLUSÕES

O sistema eletrônico de votação implantado no Brasil a partir de 1996 é um sistema robusto, seguro e confiável atendendo todos os requisitos do sistema eleitoral brasileiro:

- eleições simultâneas para diversos tipos e números de cargos majoritários e proporcionais;
- votação nominal e por partido, tanto para cargos majoritários como para cargos proporcionais;
- elevado número de partidos e candidatos;
- cobertura de vasto território nacional com diferentes características regionais, de acesso, infra-estrutura básica e densidade populacional;
- elevado número de eleitores e com diferentes graus de formação.

Estas características conferem ao sistema eleitoral brasileiro uma complexidade muito maior do que a usualmente encontrada em outros sistemas eletrônicos de votação.

A avaliação da urna eletrônica e dos procedimentos relacionados com sua preparação e utilização mostrou que:

- o modelo de urna eletrônica adotado, construída com base em um microcomputador de arquitetura IBM-PC, possibilitou o atendimento dos requisitos acima relacionados e tem permitido sua adequação às modificações da legislação eleitoral;
- a clara separação entre programas e dados confere grande flexibilidade à aplicação, permitindo a uniformização do aplicativo para todas as seções eleitorais do país e a manutenção de um núcleo estável e adaptável para todas as eleições;
- a manutenção de cópias atualizadas das principais estruturas de dados da aplicação (matriz de partidos, matriz de candidatos, matriz de eleitores) armazenadas em memória não volátil (*flash cards*) permite, em caso de falhas, a retomada da aplicação do ponto de interrupção sem perda de informações. A utilização de arquivos em duplicata para essas estruturas, armazenados no *flash card* interno e no *flash card* de

votação, garante a retomada da aplicação mesmo no caso de necessidade de substituição da urna eletrônica;

- a contabilização dos votos introduzidos é feita corretamente. O alto grau de relacionamento existente entre as estruturas internas de dados e a redundância desses dados confere confiabilidade e consistência aos mesmos;
- não são armazenados em memória não volátil dados que vinculem o eleitor ao seu voto, impossibilitando eventual quebra de sigilo; na memória volátil estes dados são sobrepostos pelos dados do eleitor seguinte;
- a utilização de sistemas padronizados de instalação e segurança permite a criação de ambientes de trabalho homogêneos em todos os pontos de inseminação de urnas, possibilitando a uniformização dos procedimentos de geração dos *flash cards* de carga e o controle do processo de inseminação das urnas eletrônicas;
- o uso de algoritmos públicos e proprietários de resumo criptográfico para verificação da integridade do software em todas as etapas de sua transferência (do desenvolvimento à inseminação) e durante sua execução na urna eletrônica permite a detecção de qualquer modificação dos programas executáveis.

Como resultado da avaliação realizada conclui-se que o sistema eletrônico de votação analisado atende as exigências fundamentais do processo eleitoral, ou seja, o respeito à expressão do voto do eleitor e a garantia do seu sigilo. Conclui-se também que a segurança e a confiabilidade do sistema de votação eletrônico podem ainda ser aprimoradas pela adoção de procedimentos e modificações apontados na Seção 5 deste relatório e listados a seguir:

- desenvolvimento dos aplicativos de votação baseados em blocos estáveis e permanentes para todas as eleições;
- formalização do ciclo de desenvolvimento do software;
- avaliação do código-fonte do núcleo do aplicativo e seus componentes acessórios por especialistas em informática independentes do TSE;
- compilação e determinação de resumos criptográficos dos arquivos em sessão pública;
- verificação, por representantes partidários, dos resumos criptográficos dos arquivos instalados nas urnas inseminadas;
- revisão do procedimento de preparação da urna para o segundo turno;
- impressão do boletim de urna antes do ciframento dos resultados da votação;
- substituição do uso de ciframento por assinaturas digitais como forma de autenticação dos boletins de urna.

A confiabilidade do processo eleitoral depende crucialmente do controle sobre todas as etapas de sua condução, que deve ser exercido pela sociedade por meio dos partidos políticos, dos fiscais, dos mesários, dos juízes eleitorais e dos próprios eleitores. Algumas das recomendações acima só terão seus objetivos totalmente atendidos se houver a efetiva fiscalização e acompanhamento por representantes aptos a fazê-lo.

O desenvolvimento e a implantação do Sistema Informatizado de Eleições demandaram alto investimento em equipamentos, infra-estrutura e treinamento de técnicos, mesários e eleitores. Assim, acredita-se que, a partir da experiência acumulada pelo TSE e partidos políticos na implantação do voto eletrônico e a partir da contribuição da comunidade científica e dos setores organizados da sociedade, é possível o aprimoramento do atual sistema e a consolidação dos processos de votação e totalização eletrônicos que se configuram como um enorme avanço no processo eleitoral brasileiro, principalmente quando confrontado com o uso de cédulas de papel e urnas convencionais.