Segurança da Informação na Eleição Eletrônica Brasileira[1]

Luiz Victor de Andrade Lima[2]
Flávia Barros da Silveira
Maria Betânia Gonçalves Xavier
Carlos Alberto Sobral Loureiro

Resumo

A legislação eleitoral vigente no Brasil determina o uso de urnas eletrônicas e as regras para a apuração dos resultados.Os critérios de avaliação prescritos na norma BS7799 sobre segurança da informação foram utilizados para nortear a análise dos processos e das atividades envolvidas nas etapas de votação eletrônica e de consolidação dos resultados. A Política de Segurança do Tribunal Superior Eleitoral (TSE) apresenta os requisitos de segurança a serem utilizados no processo eleitoral. A Política de Contingência do TSE prevê ações para as principais falhas possíveis e viabiliza a continuidade do processo eleitoral. Há diferentes opiniões sobre as fragilidades do processo, as quais serão discutidas no presente trabalho.

Palavras-chave

Segurança de Sistema da Informação; Auditoria de Sistema; Lista de Risco; Requisitos de Segurança; Voto Eletrônico; Urna Eletrônica; Política de Segurança; Eleição.

Information's Security in Brazilian Electronic Election

Summary

The effective electoral legislation in Brazil determines the use of electronic voting machine and the rules for vote's counting. The evaluation criteria proposed in norm BS7799 on information security had been used to guide the analysis of the processes and activities related to electronic voting and consolidation of the results. The Politics of Security of the Electoral Superior Court (TSE) presents the security requirements to be used in the electoral process. The main possible problems were predicted by the TSE Contingency Politics, making possible the continuity of the electoral process. There are many different opinions on process fragilities, which are discussed in the present paper.

Keywords

Security of Information System; System's Audit; List of Risk; Security Requirements; Electronic Vote; Electronic Voting Machine; Politics of Security; Election.

[1] Trabalho desenvolvido como parte da disciplina Segurança da Informação do MBA em Gestão de Sistemas de Informação da UCB, no 1º semestre de 2002

[2] Todos os autores são alunos do MBA em Gestão de Sistemas de Informação da UCB

1. Introdução

O processo eleitoral no Brasil é regido por legislação específica, regulamentada através de resoluções do Tribunal Superior Eleitoral.

Incentivadora da evolução do processo de votação brasileiro, a Lei 4737/1965 **[http1]**, conhecida como Código Eleitoral, autoriza o uso de "máquinas de votar", a exemplo das máquinas eletro-mecânicas utilizadas em votações norte-americanas, no ano anterior.

Com base em testes realizados em 1996, a Lei 9504/1997 **[http2]** determina o uso das urnas eletrônicas em substituição às antigas cédulas eleitorais e define regras para o Sistema Eletrônico de Votação e de Totalização dos Votos.

Das eleições de 1998 e 2000 surgiram críticas e sugestões apresentadas por especialistas em sistemas eleitorais automatizados, incorporadas à legislação através da Lei 10408/2002 **[http3]** que estabelece normas para ampliar a segurança e a fiscalização do voto eletrônico.

Este artigo se concentra exclusivamente sobre o aspecto de segurança da informação da urna eletrônica e do sistema de apuração e consolidação de resultados, levando em conta que eventuais falhas nos sistemas desenvolvidos pelo TSE podem imputar descrédito a todo o processo eleitoral.

A análise das informações foi realizada com base na norma BS7799, que é adotada pelo Reino Unido como regra para gestão de segurança da informação. Além de servir de orientação e referência em diversos países, o conteúdo daquela norma deu origem à norma ISO 17799.

2. Visão Geral do Processo Eleitoral

O processo eleitoral é composto por diversas etapas distribuídas ao longo do tempo, conforme representado na figura 1.

Pela sua importância, quer pelo total de pessoas envolvidas, quer pelo âmbito das medidas de segurança que se concentram em um único dia, pode-se dizer que a etapa chamada de eleição é a mais importante.

Fig. 1 - Representação do processo eleitoral

2.1 A Urna Eletrônica

A urna eletrônica foi utilizada, experimentalmente, nas eleições brasileiras de 1996. Desde então vem se consolidando como poderoso instrumento eleitoral brasileiro.

As urnas eletrônicas já foram usadas em três eleições oficiais no Brasil e não se tem conhecimento comprovado de casos de fraude. Muitos tipos de fraude foram eliminados, na apuração e na totalização dos votos, com a utilização da urna eletrônica.

Em 2001, as urnas eletrônicas brasileiras também foram utilizadas no exterior. Por meio de um convênio firmado entre o Brasil e a Organização dos Estados Americanos, o Paraguai pode experimentar o voto eletrônico. As eleições transcorreram normalmente e a inovação tecnológica foi bem aceita naquele país. A imprensa local elogiou principalmente a agilidade e a transparência do processo eleitoral.

O Tribunal Superior Eleitoral (TSE) tem incentivado o manuseio da urna em eleições não oficiais, para a familiarização dos eleitores. Em 2001 foram realizadas mais de 150 eleições, todas elas consideradas completamente seguras.

2.2 A Votação

Para que possam ser entendidas as questões relativas à segurança do voto eletrônico, é necessária uma compreensão geral sobre o processo eleitoral brasileiro.

No dia da eleição, os eleitores comparecem à suas seções eleitorais para votar. As urnas eletrônicas estão localizadas nas seções eleitorais.

2.3 A Apuração

Conforme apresentado na figura 2, após o término da votação, o disquete com os votos, chamado de boletim de urna (BU) é retirado da urna e encaminhado à uma Zona Eleitoral do município ou da região. De lá, os arquivos BU são transmitidos aos Tribunais Regionais Eleitorais (TRE) que são responsáveis pela totalização dos votos para os cargos de governador, senador, deputado federal e deputado estadual/distrital.

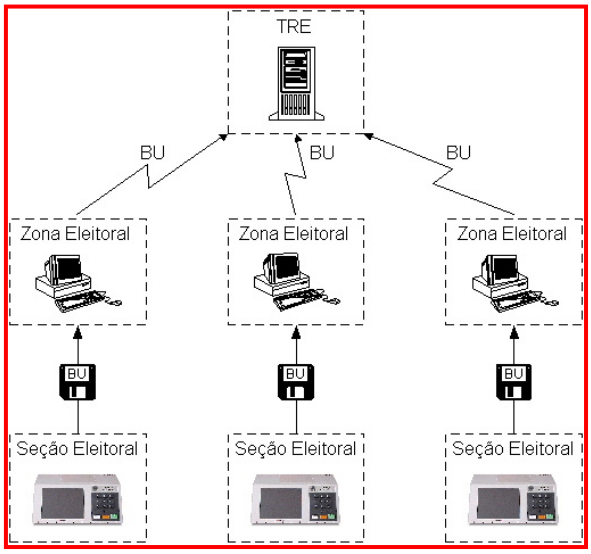

Figura 2 – Visão geral do processo de apuração

Apenas os votos para o cargo de presidente são transmitidos pelo TRE ao TSE, responsável por realizar a totalização dos mesmos.

Somente após o encerramento da apuração, em todos os estados, de todos os votos atribuídos a todos os cargos, o TSE divulga o resultado final das eleições.

3. Política de Segurança

Apesar do TSE possuir política de segurança da informação documentada, parte dela não é tornada pública, o que dificulta a análise que aqui se desejou fazer. Além disto, o cenário apresentado no documento disponível deixa a desejar.

Foi necessário o levantamento de outros cenários para o entendimento, acompanhamento e implementação dos quesitos de segurança mais apropriados. Somente desse modo, foi possível identificar o objetivo geral da Política de Segurança da Informação elaborada pelo TSE **[POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, 1998]** que pretende *delinear as diretrizes básicas e recomendações, no âmbito da Justiça Eleitoral, para assegurar uma conduta adequada na geração, tratamento, divulgação, acesso e arquivamento das informações, garantindo sua confiabilidade, integridade, disponibilidade, autenticidade e legalidade*.

As peculiaridades do processo eleitoral são retratadas nas divisões dos sistemas eleitorais que podem ser divididos em sistemas que sustentam os atos preparatórios, a recepção de votos e as garantias eleitorais **[RESOLUÇÃO N.º 20.997, 2002]** e os que sustentam a apuração e totalização dos votos **[RESOLUÇÃO N.º 21.000, 2002]**.

O documento que propõe a Política de Segurança do TSE, reforça a necessidade de que sejam elencados os requisitos de segurança a serem abordados. Dentre eles destacam-se:

- Integridade do sistema
- Integridade e confiabilidade dos dados;
- Anonimato do eleitor;
- Autenticação do operador;
- Auditoria do sistema;
- Disponibilidade do sistema;
- Confiabilidade;
- Facilidade de uso;
- Documentação de segurança;
- Integridade de pessoal;
- Precisão;
- Resistência a falhas; e
- Resistência a fraudes.

4. Identificação e Análise de Riscos

Para atender aos requisitos da Política de Segurança, faz-se necessária a identificação de ameaças, a avaliação da probabilidade de ocorrência e o impacto causado caso esta ameaça venha a ocorrer. Tem-se, então, um mecanismo para identificar claramente quais os maiores riscos que afetam o processo.

O questionamento constante é o ponto de partida para uma revisão periódica dos riscos de segurança identificados e dos controles implementados para:

a) considerar mudanças de requisitos do negócio e prioridades;
b) considerar novas ameaças e vulnerabilidade;
c) confirmar os controles que continuam eficientes e apropriados à nova situação.

4.1 Principais Riscos

Para o dimensionamento dos riscos foi utilizado um método sugerido na literatura **[CLÁUDIA DIAS, 2000]**, classificando as ameaças por impacto e probabilidade, atribuindo-se a cada fator um valor crescente de 0 a 5. O valor do risco é obtido a partir do resultado da multiplicação dos valores dos fatores de cada ameaça.

A figura 3 apresenta exemplo da análise de risco feita a partir de ameaças identificadas.

AMEAÇAS	Impacto 0 - 5	Probabilidade 0 - 5	Risco
Identificação e Autenticação			
Ameaça programada que mascara sua identificação (cavalos de tróia)	**4**	**3**	**12**
Confidencialidade			
Monitoramento de tráfego de informações na rede externa	**1**	**3**	**3**
Integridade			
Dano deliberado ao conteúdo de arquivos ou sistemas confidenciais	**4**	**2**	**8**
Legais			
Usuários internos praticando atos ilegais	**4**	**5**	**20**

figura 3 – exemplos de análise de risco

5. Pontos de Partida para a Segurança da Informação

Os controles implementados para segurança da informação permitem avaliar os custos frente aos riscos da reputação da organização.

Estes controles foram divididos em assuntos que abordam:

- Segurança Operacional;
- Segurança Pessoal;
- Segurança Ambiental e Física.

Outros pontos que requereram atenção especial da Justiça Eleitoral foram os aspectos legais que envolvem, basicamente, os direitos de propriedade intelectual, a salvaguarda dos registros organizacionais e a proteção e privacidade da informação pessoal.

5.1 Controle e Classificação de Bens

Com o objetivo de garantir a manutenção de uma proteção apropriada das urnas eletrônicas, o Tribunal Superior Eleitoral regulamentou **[RESOLUÇÃO 20771, 2001]** o armazenamento, a movimentação e o controle das mesmas. No que se refere ao armazenamento das urnas, a resolução é bem específica chegando a detalhar até mesmo a altura máxima (2,2 m) em que elas podem ser empilhadas.

Já em relação ao controle e movimentação das urnas, a resolução não chega a um menor nível de detalhes, discorrendo apenas sobre a criação de uma Comissão Nacional, no âmbito do TSE, e de Comissões Regionais, no âmbito de cada TRE. Tais comissões têm como função o controle das condições de armazenamento e segurança das urnas, bem como o controle quantitativo das urnas armazenadas em cada local. Quanto à movimentação das urnas, o controle é feito mediante guias de transferência emitidas pelo setor responsável pelo armazenamento.

O TSE também regulamentou **[RESOLUÇÃO 20771, 2001]** os procedimentos para aceitação dos lotes das urnas eletrônicas, a serem obedecidos pelos fabricantes. Resumidamente, o aceite é feito por meio de testes de amostragens nos lotes das urnas e quanto maior o lote, maior será a amostragem.

Percebe-se haver grande preocupação do TSE em estabelecer normas para tudo o que se refere ao controle e à manutenção das urnas eletrônicas, de forma a garantir que não aconteçam desvios das urnas ou mesmo que venham a ser utilizadas urnas com algum tipo de defeito de fábrica.

5.2 Segurança de Pessoal

Observa-se haver atenção para com os riscos de erro humano, roubo, fraude ou uso indevido das facilidades.

Um grande problema a ser enfrentado atualmente pelo TSE refere-se à forma de controlar os trabalhos dos desenvolvedores dos sistemas, que são funcionários de empresa contratada. Supõe-se que deva haver alguma cláusula no contrato com a empresa sobre fraude nos sistemas.

O TSE se protege contratando a consultoria de uma empresa especializada que ministra palestras para os funcionários sobre como garantir a segurança das informações.

Existe também a preocupação sobre o acesso às dependências de processamento do TSE. Somente tem acesso a tais dependências, as pessoas autorizadas e identificadas por um cartão magnético. Percebe-se que tal dispositivo de segurança pode tornar-se um grande problema, principalmente a partir da perda de um desses cartões.

Por fim existe o treinamento dos membros da mesa receptora para o dia da votação, orientação quanto aos requisitos de segurança e a instalação correta das urnas eletrônicas.

5.3 Segurança Ambiental e Física

Identificou-se a preocupação de manter separados os servidores usados para ambientes de desenvolvimento, homologação e produção.

São efetuadas cópias de segurança (backup) mensalmente e enviadas para armazenamento em outro prédio. Apesar desta rotina ser realizada, o risco de retrabalho é alto e crescente à medida em que se distancia a data em que o último backup tiver sido realizado.

Verificou-se que há padronização quanto aos nomes de servidores, fato que aumenta a vulnerabilidade dos sistemas em caso de ataque.

5.4 Controle de Acesso

O acesso aos ambientes de sistemas passa por controles de senhas que são obrigatoriamente alteradas a cada período de 15 dias.

Não é permitido o tele-trabalho, diminuindo os riscos de penetração de intrusos através de acesso remoto.

Somente é permitido o uso de equipamentos móveis, do tipo notebook, quando ligados diretamente à rede local, dentro do prédio do TSE. Considera-se que o uso deste tipo de equipamento pode por em risco a segurança se o mesmo for retirado do prédio.

Foi identificado como positivo o uso de acesso com endereço IP fixo para a transmissão de boletins de urna, no dia da eleição.

6. Desenvolvimento e Manutenção

Os ambientes de desenvolvimento, homologação e produção são padronizados quanto ao uso de hardware e software, diminuindo o risco de problemas e o próprio custo de manutenção.

Nas estações de trabalho apenas são instalados os softwares necessários ao andamento dos serviços.

Há restrições quanto ao tipo e ao tamanho de arquivos que podem transitar anexados a mensagens do correio eletrônico.

Para que um programa possa passar para o ambiente de produção, ele precisa passar por um programa validador que anexa uma rotina de uso exclusivo do ambiente de produção.

O uso de criptografia para transmissão de dados e a codificação dos nomes de arquivos também é fator considerado positivo.

Há uso de software controlador de versões, para garantir a rápida recuperação de versões de programas.

7. Contingência

O TSE se preocupa de uma forma bem enfática no que se refere ao plano de contingência do processo de votação eletrônica. Além das 250.000 urnas eletrônicas existentes para atender a eleição de 2002, ainda existem cerca de 50.000 urnas de contingência, distribuídas nas diversas zonas eleitorais.

Tendo em vista, o surgimento em maio de 2001 de problema de racionamento de energia que afetou o Brasil, conhecido como "Apagão", as urnas passaram a ser dotadas de baterias que na falta de energia, ainda sustentam o sistema por 12 horas. Além disso, cada TRE tem um gerador de energia e as maiores zonas eleitorais também.

Está prevista a opção pelo uso do voto em cédulas, sendo este de fato o último recurso no caso de falhas nas urnas eletrônicas.

Para a apuração de votos, e no caso de falhas dos equipamentos servidores, o TSE também tem uma política de contingência configurando os servidores de outros TRE para continuar com o processo de apuração de votos.

Após as eleições, são previstos backups dos dados armazenados nos sistemas, diariamente, mantendo-se a guarda das últimas três cópias, devidamente identificadas e acondicionadas.

8. Auditoria

Na Política de Segurança da Informação do TSE a abordagem da auditoria de sistemas é direcionada para equipes independentes e especializadas e determina que *todos os sistemas, equipamentos e programas, quando em condições de "Produção", devem possuir todos os recursos necessários para serem considerados como auditáveis*.

Desde sua primeira utilização, a Urna Eletrônica, vêm causando grandes debates entre os defensores da ampla transparência do processo eleitoral e o TSE. Tais debates geraram inúmeras manifestações contrárias ao processo, qual vinha ocorrendo, exigindo a implementação de controles com vistas a dar maior credibilidade ao gesto de votar por meio eletrônico.

Várias fragilidades da urna eletrônica foram apresentadas, como:

- Não permitirem a recontagem dos votos;
- Permitirem fraudes por meio de programação;
- Parte dos programas eram mantidos em segredo; e
- Possibilidade de identificação do voto**.[AMILCAR BRUZANO, 2001]**

Estes pontos de insegurança estão sendo trabalhados e grande parte dos controles está sendo implementada pelo TSE com vistas à melhoria dos sistemas.

Nas eleições de 2002, serão utilizadas, no Distrito Federal e em Sergipe, urnas eletrônicas com impressão dos votos, permitindo verificação visual do voto antes da confirmação pelo eleitor. Além disto, será minimizado o trabalho em caso de eventual apuração paralela.

No prazo de 60 dias antes da dia da eleição, está previsto haver abertura completa de todos os sistemas e programas para auditoria por candidatos e partidos políticos.

Cabe observar que o requisito anonimato do eleitor é apresentado pelo TSE como atendido, uma vez que o sistema de identificação, onde é exigida a digitação do número do Título Eleitoral, não tem qualquer vinculação com o sistema de totalização existente na urna eleitoral. Contudo, cabe a sugestão de total desvinculação entre os sistemas.

Por fim, na véspera da eleição, serão escolhidas, em cada estado, pelo menos 2 urnas para realização de auditoria, sendo as mesmas substituídas por urnas previstas para contingenciamento.

9. Conclusão

Após a análise das questões relativas ao voto eletrônico e das mudanças implementadas pelo TSE para as eleições gerais 2002 é possível afirmar que a eleição eletrônica continua dando subsídios para a evolução da democracia brasileira, quer seja dando mais agilidade, quer seja dando mais transparência ao processo eleitoral.

Pode-se afirmar que as críticas até o momento observadas tem contribuído fortemente para a melhoria do processo eleitoral, visto que as principais sugestões apresentadas já foram incorporadas à legislação. Percebe-se, no entanto, que ainda há grande espaço para melhoria do processo.

10. Referências

[POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, 1998] *Política de Segurança da Informação* - Tribunal Superior Eleitoral, v. 1.0, 1998.

[RESOLUÇÃO N.º 20.997, 2002] Tribunal Superior Eleitoral - Instrução n.º 61 - Classe 12ª - Distrito Federal, 26/02/2002.

[RESOLUÇÃO N.º 21.000, 2002] Tribunal Superior Eleitoral - Instrução n.º 64 - Classe 12ª - Distrito Federal, 26/02/2002.

[AMILCAR BRUZANO, 2001] BRUZANO FILHO, Amílcar. *"Critérios para Avaliação da Segurança do Voto Eletrônico"* : http://www.votoseguro.org.

[RESOLUÇÃO 20771, 2001] Tribunal Superior Eleitoral - Distrito Federal, 20/02/2001.

[CLAUDIA DIAS, 2000] DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação.* Rio de Janeiro: Axcel Books do Brasil, 2000.

[http1] *Lei 4747/1965* : http://www.senado.gov.br/legisla.htm

[http2] *Lei 9504/1997* : http://www.senado.gov.br/legisla.htm

[http3] *Lei 10408/2002* : http://www.senado.gov.br/legisla.htm