

**II SOLISC**  
**2 Dez 2005**



# **Vulnerabilidades do Sistema Eleitoral Brasileiro**

Prof. Pedro A. D. Rezende

Ciência da Computação - UnB

Colaboração: Evandro Oliveira  
Diretor de Auditoria - ITI

# Sistema Eleitoral



O processo de informatização **NÃO** se resume na implementação da máquina de votar “Urna Eletrônica” (UE). Inclui:

- Recadastramento eleitoral (1985)
- Completa informatização da votação (2000)
- Rede de totalização p boletins de urna (BU)

Desmaterializou-se o voto, restando o BU como subsídio para verificação, fiscalização e auditoria da votação.

# Sistema Eleitoral



O Sistema Informatizado de Eleições (SIE) **NÃO** se resume na utilização das UE.

- Inicia-se na licitação dos equipamentos (*hardware*) e programas (*software*),
- Deveria passar por homologação independente de sistemas e equipamentos
- Deveria encerrar com meios de auditoria dos resultados eleitorais publicados, contra os resultados intermediários.

# Sistema Eleitoral



Agentes envolvidos,  
com interesses potencialmente conflitantes:

- Candidatos (>1)
- Eleitores
- Fiscais de Partidos
- Juízes Eleitorais
- Mesários
- Técnicos Internos (TSE e TREs)
- Auxiliars Externos (Técnicos e Não-técnicos)

# Sistema Eleitoral



Pontos e canais do processo eleitoral:

- TSE / TREs
- Zonais / Comarcas Eleitorais
- Seções Eleitorais / Locais de Votação
- Locais de Armazenamento das Urnas
- Estações de Transmissão Digital (sw e dados)
- Meios de Transporte de Software, Urnas e Disquetes com BUs e Logs.

# Sistema Eleitoral



Conceitos envolvidos:

- **Segurança = Controle da proteção**

**Proteger, segurar NÃO** são verbos intransitivos ou transitivos, são bi-transitivos

- Protege-se **ALGUÉM** (algum interesse) contra **ALGO** (algum risco), **NÃO** se protege “o sistema”
- Mais de dois interesses em jogo introduzem riscos de **CONLUIO**: Neste caso, segurança é equilíbrio de riscos e responsabilidades, NÃO pode ser 100%

# Sistema Eleitoral



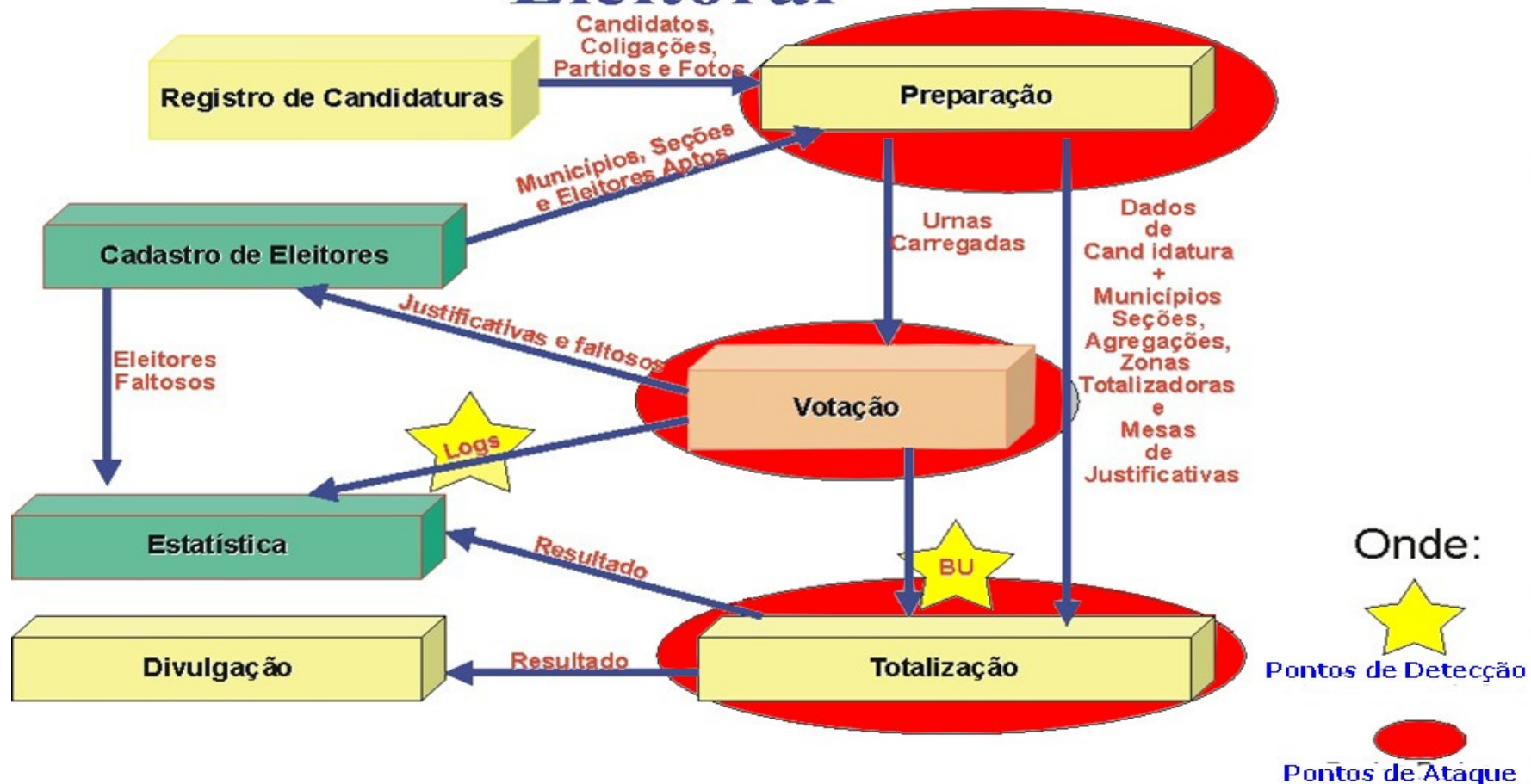
Processos eletrônicos envolvendo mais de dois interesses deveriam exigir:

- Mapas de Risco
- Auditorias Independentes
- *Software* Básico e Aplicativos em Código Aberto (auditável contra compilação)
- Fiscalização externa em Pontos Vulneráveis
- Simulação de Ataques (teste de penetração)

# Sistema Eleitoral



## Etapas do Processo Eleitoral





# Sistema Eleitoral



A imagem ao lado é uma foto de divulgação oficial do TSE destinada a mostrar como é a votação oficial.

O que tem de errado na foto??

# Sistema Eleitoral



## Vulnerabilidades externas:

- Transmissão de disquete clonado
- Voto de falecidos / ausentes
- Quebra de senha na apuração (TSE e TREs)
- Troca de *Flash* de Votação (FV)
- Clones a partir de *Flash* de Carga (FC) oficial
- Código malicioso em fotografias (formato jpeg)
- Troca de votos no processo de “voto cantado”
- Extravio de BUs para inviabilizar conferência

# Sistema Eleitoral



## Vulnerabilidades internas:

- Inserção de cavalos de tróia antes, ou quando da distribuição dos softwares para UEs aos TREs
- Inserção de cavalos de tróia antes da carga das UE
- Inserção de cavalos de tróia depois da carga (via disquetes de recuperação/configuração da UE)
- Distribuição de votos desviados em seções com BUs extraviados ou denegados, introduzidos por atacado durante a totalização, antes da divulgação das planilhas de totalização.

**Azul:** Fraudes “por atacado”, sem correspondentes em sistemas tradicionais, que materializam votos

# Sistema Eleitoral



## Roteiro básico para cavalos de tróia na UE

- Desarme imperceptível da auto-verificação de integridade (assinatura digital, etc.) no arquivo setup.bat (ou equivalente)
- Instalação de rotina para desvio de votos pós-votação e pré-gravação do BU (baseado em porcentagens, limiares, etc.), no sistema da UE
- Auto-deleção da rotina de desvio e do gatilho de desarme, após a gravação do BU.

# Sistema Eleitoral



Ex: desarme da auto-verificação da UE 2000  
análise publicada no Observatório da Imprensa em  
7/9/04 (**cinza**: Setup.bat; **azul**: Cavalo de tróia)

....

```
diskfix c: /vs > nul
```

```
REM if errorlevel 1 goto TentaRecuperar
```

```
ckpack c:\raiz.crc c:\ > nul
```

```
REM if errorlevel 1 goto ebatger
```

....

# Sistema Eleitoral

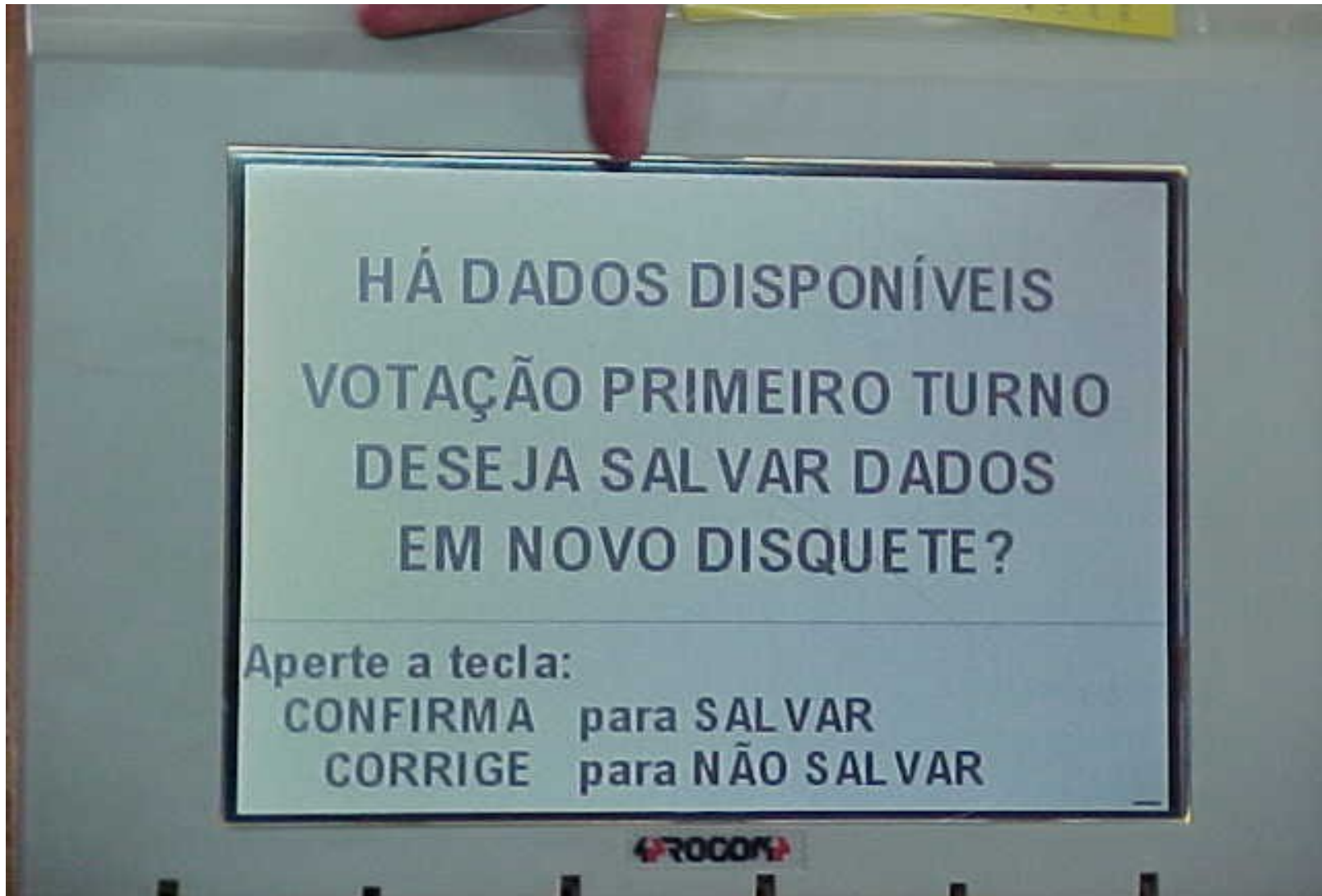


Ex: Modelo de rotina para desvio de 5% de votos de A (ex:13) para B (ex:45), em C (estrutura de dados em pseudocódigo).  
Análise apresentada no seminário de votação eletrônica, Camara Federal, em 28/5/02

```
int fator = 40;  
int x = bu.prefeito.votos["13"]/fator;  
    bu.prefeito.votos["45"] += x;  
    bu.prefeito.votos["13"] -= x;
```



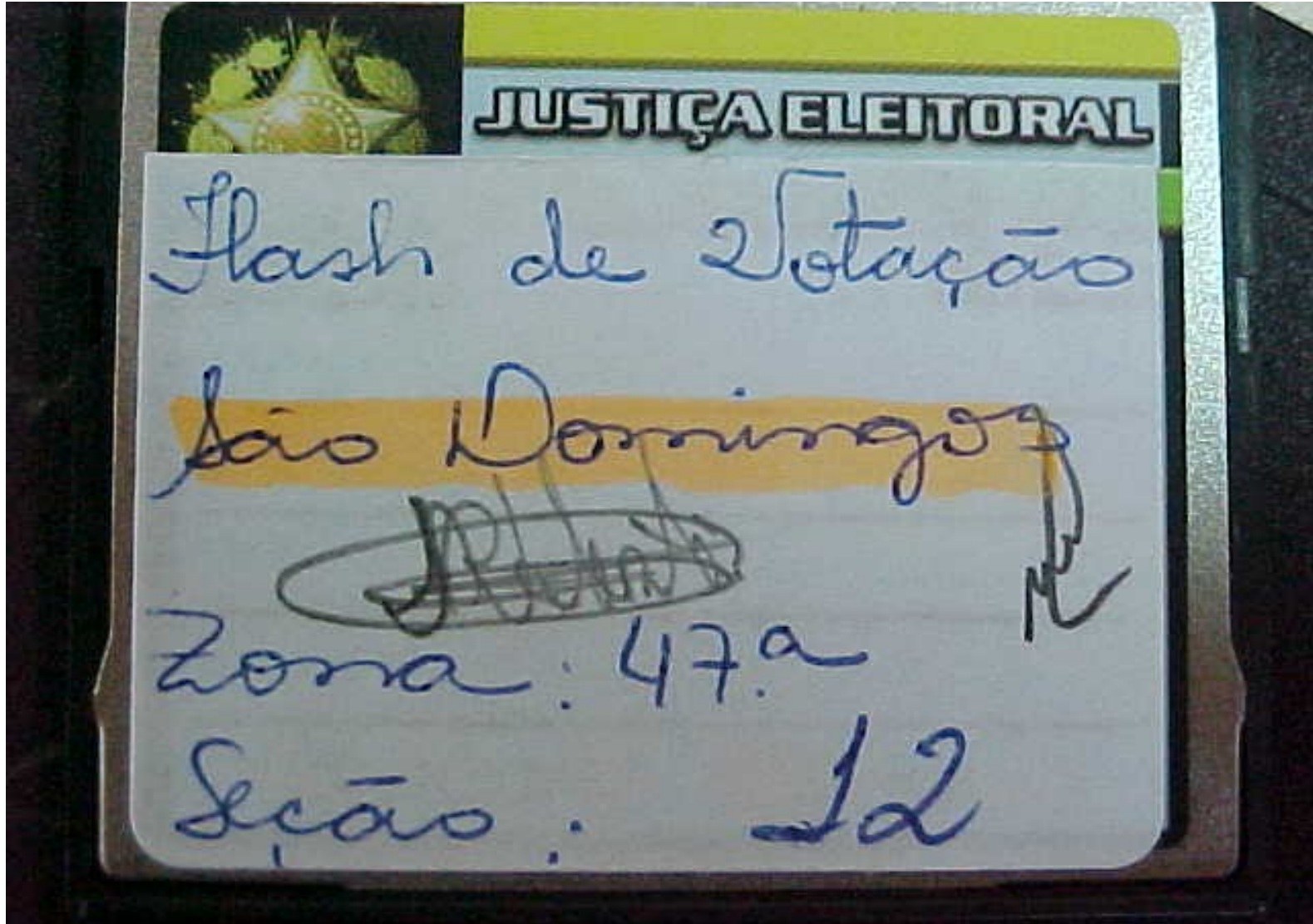
# Sistema Eleitoral







# Sistema Eleitoral



Flash de Votação

São Domingos

~~XXXXXXXXXX~~

Zona: 47ª

Seção: 12



# Sistema Eleitoral





## Sites Brasil:

Forum do voto seguro: [www.votoseguro.org](http://www.votoseguro.org)

Prof. Pedro Rezende:

[www.cic.unb.br/docentes/pedro/sd.htm](http://www.cic.unb.br/docentes/pedro/sd.htm)

## Sites EUA:

Forum do voto verificável: [www.verifiedvoting.org](http://www.verifiedvoting.org)

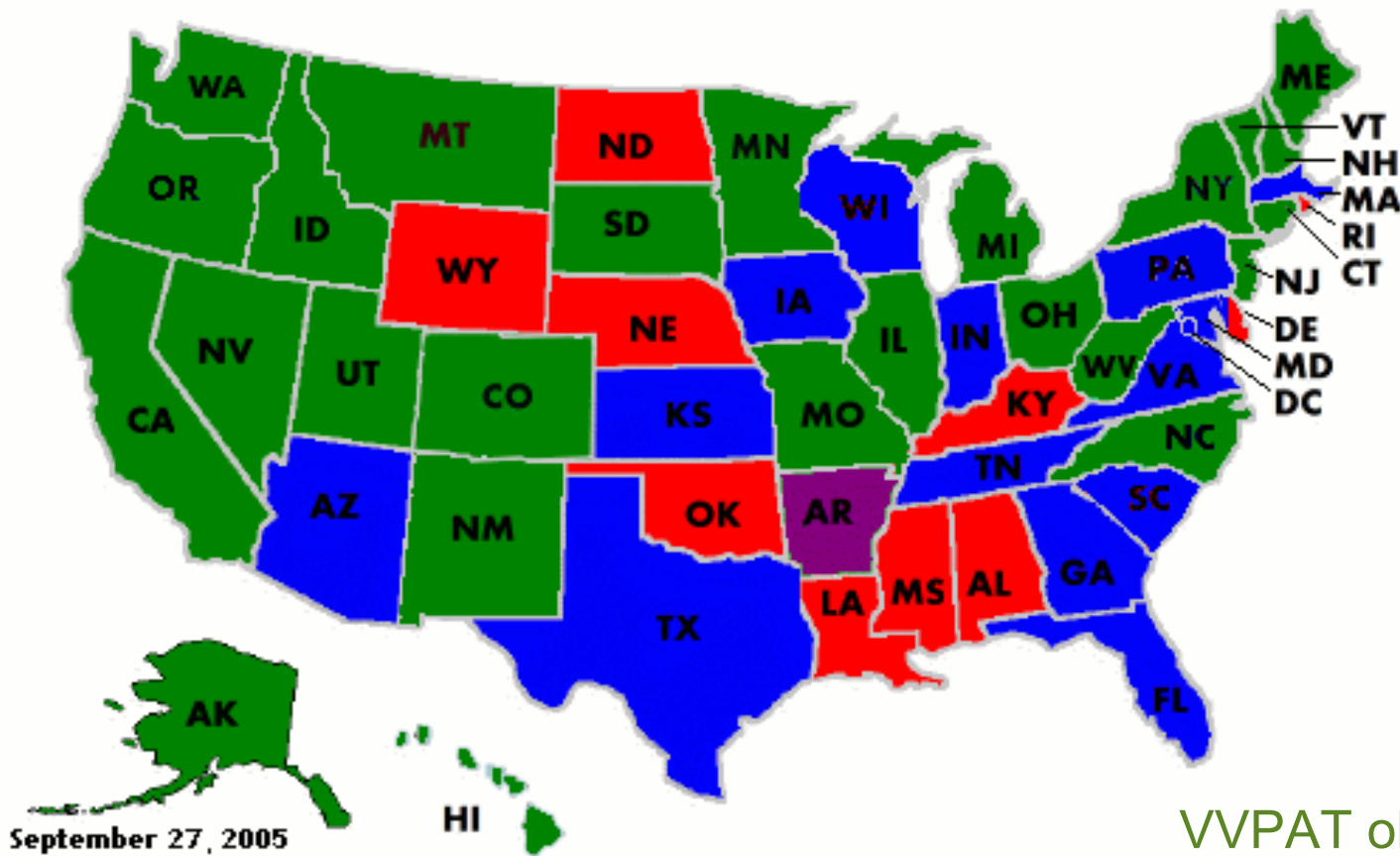
Caixa-preta eleitoral: [www.blackboxvoting.org](http://www.blackboxvoting.org)



# Sistemas Eleitorais: EUA

[www.verifiedvoting.org](http://www.verifiedvoting.org) - VVPAT

Voter-Verifiable Paper Audit Trail



September 27, 2005

Set 2005  
VVPAT obrigatório  
Lei em tramitação



(jagube e chacrona)

# A Seita do Santo Byte

Artigo publicado em vários portais, s/ a canhestra e atabalhoada votação da nova lei eleitoral (1/10/03):

- Adeptos fanáticos ingerem uma beberagem de propaganda oficial pelos ouvidos (e olhos);
- Põem-se a bailar, com a mídia corporativa, sob o mantra “*Nosso sistema é 100% seguro, ninguém nunca provou o contrário. Nós dominamos a tecnologia!*”;
- Entram em processo alucinatório, têm visões de seres angelicais programando urnas eletrônicas e apurando eleições. Acham os infiéis retrógrados.