

## Processo de Auditoria

## Relatório de Auditoria ao Sistema de Votação Electrónica – Fase de Simulação

### Freguesia de S. Sebastião – Setúbal

2004-07-27

## Conteúdos

1	Introdução .....	3
1.1	Constituição da Comissão de auditoria .....	3
1.2	Apresentação do SVE .....	3
1.3	Resumo da auditoria ao funcionamento do SVE no dia do acto eleitoral .....	5
2	Análise das características do SVE .....	7
2.1	Segurança (S) .....	7
2.2	Transparência (T) .....	9
2.3	Acessibilidade (A) .....	12
3	Conclusões e Recomendações.....	14
3.1	Conclusões .....	14
3.2	Recomendações .....	14
ANEXO - Grelha para as Conclusões e Recomendações do Relatório de Auditoria ao Sistema de Votação Electrónica (RASVE).....		16
Segurança .....		17
Transparência .....		18
Acessibilidade .....		19



## 1 Introdução

### 1.1 Constituição da Comissão de auditoria

Prof. Doutor Gabriel David (relator)

Prof. Doutor José Magalhães Cruz

Engenheiro João Isidro Araújo Vila Verde

**Local:** Freguesia São Sebastião, Setúbal, Escola do 1º ciclo do Monte Belo, 5 secções de voto, cerca de 6500 eleitores inscritos.

**Data e hora:** dia 2004-06-13, 8:05/12:30 e 14:00/20:00

Nesta freguesia, o SVE – Sistema de Votação Electrónica foi instalado em dois locais, cada um com uma mesa e sete postos de votação. Optou-se por observar em contínuo um dos locais, instalado na Escola do 1º ciclo do Monte Belo.

### 1.2 Apresentação do SVE

O SVE observado é constituído por dois subsistemas: o Caderno Eleitoral e os Postos de Votação.

O Caderno Eleitoral é um sistema desenvolvido pela Multicert, baseado num PC (Windows XP) com uma aplicação em que se encontravam registados todos os eleitores da freguesia. O seu objectivo é identificar como eleitores devidamente inscritos as pessoas que se apresentam para votar e registar os votantes. A sua operação foi garantida por uma mesa constituída por elementos designados pela Junta de Freguesia, excepto nas operações de inicialização e fecho, em que contaram com o apoio do elemento da UMIC presente.

O subsistema dos Postos de Votação (Unisys, hardware e software próprios) é constituído por uma estação central operada pela mesa que tem como funções regenerar as chaves de voto, durante a votação, e concentrar os resultados dos vários Postos de Votação locais e enviá-los para o concentrador nacional (no caso, instalado na FCCN); pelas Chaves de Votação, que são a garantia de que o votante foi autorizado pela mesa (estiveram em uso 12); e pelos Postos de Votação, que servem para registar os votos individuais (foram usados 7).

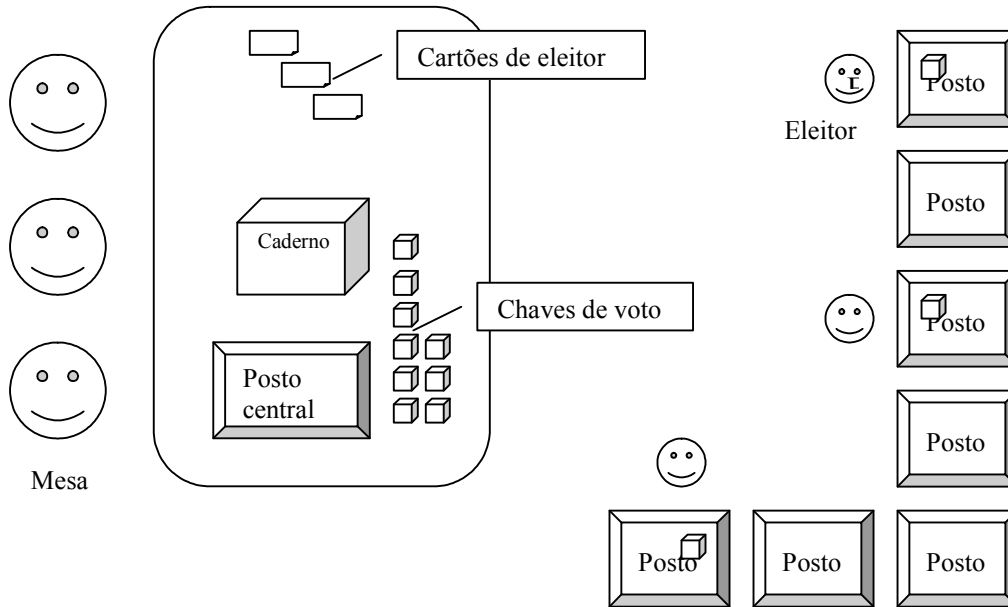


Figura 1. Arquitectura do SVE

O processo de votação é o seguinte:

- o eleitor entrega o seu cartão de eleitor e BI ao presidente da mesa, ao centro, que opera o Caderno Eleitoral;
- este verifica que o eleitor se encontra inscrito no Caderno Eleitoral e que ainda não votou, colocando-o numa lista de eleitores em processo de votação;
- o vogal à direita entrega uma Chave de Voto previamente regenerada no Posto Central ao eleitor;
- o eleitor dirige-se a um dos Postos de Votação, introduz a Chave de Voto numa ranhura que desencadeia a apresentação de uma sequência de 4 painéis a que o eleitor responde e retira a Chave de Voto da ranhura;
  - Painel 1 – escolha da língua (Português ou Inglês)
  - Painel 2 – escolha do partido (mutuamente exclusiva, pode ficar em branco)
  - Painel 3 – inquérito de duas perguntas sim/não sobre o sistema de votação
  - Painel 4 – confirmação das escolhas feitas nos painéis 2 e 3;
- o eleitor dirige-se ao vogal à esquerda a quem entrega a Chave de Voto e que lhe devolve o cartão de eleitor e o BI, após o que aquele se retira;
- o vogal informa o presidente da mesa de que o eleitor concluiu a votação, para que este seja retirado da lista dos eleitores em processo de votação.

O processo de inicialização no subsistema Caderno Eleitoral exige o conhecimento da password da máquina e envolve arrancar um programa que exige a leitura de três cartões magnéticos, um de cada elemento da mesa. O processo de fecho é semelhante e é impresso um relatório onde se refere o total de votantes naquela mesa.

O processo de inicialização no subsistema dos Postos de Votação exige uma Chave do Supervisor (que deveria estar na posse do presidente da mesa mas se encontrava na posse do representante da UMIC); este pode bloquear o processo temporariamente mas só pode fechar após a hora definida para tal. O processo de fecho consiste em encerrar cada Posto com a Chave do Supervisor, a qual recolhe os respectivos dados. Os Postos são encerrados em sequência e os dados concentrados no Posto Central, o qual é nessa altura ligado a uma impressora/modem que imprime os resultados da votação e os envia para o concentrador nacional.

### 1.3 Resumo da auditoria ao funcionamento do SVE no dia do acto eleitoral

A auditoria decorreu da forma planeada, tendo estado dois elementos da equipa presentes durante a abertura e parte da manhã e outro elemento presente no fim da manhã, tarde e fecho.

Todos os elementos presentes na sala se mostraram disponíveis para prestar os esclarecimentos solicitados. Não foi no entanto, mais uma vez, possível obter informações de carácter técnico, por ausência de pessoal qualificado.

O ambiente da sala estava a meio caminho entre uma sessão de votação e uma operação de marketing. Encontrava-se dentro da sala, junto à entrada, um sistema de *home video* a passar ininterruptamente um pequeno anúncio da experiência, contendo instruções sobre o processo de votação, que poucos eleitores observavam mas criava um ruído de fundo na sala. A atitude excessivamente pró-activa no acompanhamento dos eleitores aos Postos de Votação por parte das hospedeiras contratadas para acompanhar o processo, dos elementos da Junta de Freguesia que não se encontravam na mesa e dos representantes da UMIC e do vendedor (Unisys), mais parecia a da venda de um produto do que um teste de funcionamento. Se se compreende a boa vontade no sentido de esclarecer os eleitores de forma a que o processo “corresse bem”, perdeu-se um pouco o realismo da experiência.

Fora da sala do SVE, um conjunto de hospedeiras convidava cada eleitor que acabava de votar numa das secções a dirigir-se ao SVE e, à saída, uma empresa de sondagens fazia um inquérito e oferecia T-shirts alusivas ao voto electrónico, o que motivava claramente uma parte significativa dos eleitores a participar no processo.

A participação dos eleitores foi elevada. A generalidade dos votantes do SVE era também votante numa das cinco secções de voto instaladas na escola. No entanto, num número reduzido, apareceram eleitores de outras secções de voto que também quiseram experimentar o sistema. Assim, num universo de 1539 votantes nas 5 secções de voto, 1019 (66%) também votaram no SVE (mais 55 em branco). A atitude com que o fizeram também pode ser considerada de seriedade, pelo menos estatisticamente, pois os resultados percentuais obtidos pelos partidos no SVE foram muito próximos dos obtidos nas 5 secções de voto (abaixo de 6% de diferença).

O processo de inicialização foi demorado (só ficou concluído perto das 8H20) devido a problemas na leitura dos cartões magnéticos dos elementos da mesa.

O decurso da votação foi praticamente sem incidentes, tendo-se formado pequenas filas na mesa mas nunca havendo filas nos Postos de Votação. Da análise efectuada verificou-se que a cadência máxima da mesa andou por volta dos 2.3 eleitores/minuto, com o procedimento seguido. O que significa um máximo de 1320 eleitores para a mesa instalada. Admitindo um universo de 6500 eleitores nas 5 secções de voto, a experiência decorreu bem devido à elevadíssima abstenção. Estima-se que teriam sido suficientes 4 Postos de Votação, para a cadência da mesa. Os elementos tiveram que ser rodados várias vezes e, atendendo ao cansaço e número de erros que começaram a cometer, pensa-se que deveria ter havido maior rotação, com períodos máximos de 1H na mesa, em particular o presidente.

O único incidente confirmado foi uma demonstração de um voto feito com a Chave do Supervisor (configurada para poder votar) que ficou efectivamente registado.

O fecho decorreu rapidamente (cerca de 20 minutos) e sem incidentes.

## 2 Análise das características do SVE

Apresentam-se nesta secção comentários mais detalhados, relativos a cada uma das características observadas.

### 2.1 Segurança (S)

#### 2.1.1 Auditabilidade

Quer os Postos de Votação quer o Caderno Eleitoral exibem permanentemente o total de votos registados, o que permite manter algum acompanhamento da consistência dos dois registos. No entanto, é este o único aspecto auditável durante o processo de votação.

#### 2.1.2 Autenticação do Operador

Caderno Eleitoral inicializado pela mesa, necessitando de três *smartcards*. Postos de Voto inicializados pela Chave de Voto do supervisor.

#### 2.1.3 Certificabilidade

Caderno Eleitoral - ?

Postos de Voto baseados em hardware e software privado de que não temos informação nem indicação de como é possível certificar.

#### 2.1.4 Fiabilidade

Detectámos duas formas principais de possibilidade de inconsistência entre o número de votantes no Caderno Eleitoral e nos Postos de Votação.

Se o eleitor se identificar, receber a chave de voto, não chegar a usá-la e o presidente da mesa aceitar o voto, o Caderno fica com mais um voto do que os Postos. Este procedimento poderia ser encarado como mais um voto branco (ou nulo?). No entanto pode mascarar diferenças no sentido contrário.

Se um eleitor que já votou se apresentar novamente para votar, a probabilidade de o presidente da mesa não detectar o facto até à entrega da Chave de Voto é elevada pois as únicas indicações que recebe são uma bolinha verde em vez de cinzenta à esquerda do nome do eleitor e o botão em que autoriza o eleitor a votar estar inactivo. O click que faz em cima (ao fim de algumas dezenas de clicks...) pode passar despercebido, e a entrega da Chave de Voto, a partir do momento em que o eleitor vota, é irreversível. Após a devolução da chave é que é mais fácil detectar a ausência do eleitor na lista de pendentes, mas aí é tarde demais e o eleitor já votou duas vezes, ficando o Caderno com menos um voto do que os Postos.

O facto de as duas inconsistências poderem cancelar-se torna o processo especialmente duvidoso.

### **2.1.5 Detectabilidade**

Os Postos de Votação bem como o Posto Central são isolados pelo que não existe possibilidade de intrusão por rede. Relativamente a outros tipos de intrusão, como substituição de componentes, etc. não obtivemos informação para responder a esta pergunta.

O Caderno Eleitoral encontra-se também numa máquina isolada.

### **2.1.6 Disponibilidade do Sistema**

Referimo-nos à disponibilidade em duas perspectivas. Do ponto de vista dos equipamentos, o Caderno Eleitoral demorou cerca de 20 minutos a arrancar por dificuldade de leitura dos *smartcards* pelo que a votação só pode ser iniciada cerca das 8H20. Os Postos funcionaram sem percalços durante todo o período da votação.

Do ponto de vista do eleitor, o sistema teve também alta disponibilidade, pois só se formaram filas na mesa, para verificação do Caderno Eleitoral e nunca nos Postos e mesmo aquelas foram pequenas, inferiores a 5 minutos. Estima-se que para uma mesa a trabalhar em pleno, 4 Postos de Votação fosse o número adequado.

### **2.1.7 Imunidade a Ataques**

Num sistema isolado como o que foi testado esta questão só se põe em termos de adulteração das máquinas antes da votação (não tivemos acesso a informação sobre as medidas previstas contra estas situações) e no envio dos resultados, que é feito por modem associado ao Posto Central. A informação é enviada não cifrada mas com CRC e é sempre possível confirmar os valores, uma vez que os resultados são também impressos na Mesa e assinados pelos respectivos membros. A possibilidade de ataque nesta fase, se bem que existente, é defensável.

O ataque através do uso de Chaves de Votação ilegais está prevenido pelo facto de todas as máquinas terem um número de série bem como as Chaves de Voto e ambos os equipamentos serem activadas especificamente para funcionarem em conjunto, associados a uma Mesa.

### **2.1.8 Integridade dos Votos**

Não existe controlo óbvio sobre o que é armazenado quando o eleitor vota. Não é impresso nenhum “recibo” que se colocasse em urna (embora exista equipamento complementar que permite essa funcionalidade) e não existe nenhum processo de confirmar o voto que ficou registado, depois de o eleitor concluir a votação. A única forma de garantir a integridade dos votos no processo testado passa pela certificação dos Postos de Votação e do Posto Central, tanto em hardware como em software, procedimento relativamente ao qual não obtivemos informação, para além da afirmação de que o equipamento se encontra certificado em alguns países.

### **2.1.9 Invulnerabilidade**

Sem informação, para além da afirmação por elementos da empresa que apresenta o equipamento de que o sistema operativo é próprio, para reduzir as hipóteses de acesso a terceiros.



### **2.1.10 Rastreabilidade**

Sem informação, nos Postos de Votação, para além do facto de existir em cada um uma contagem global dos votos alguma vez por ele efectuados, tentando prevenir contra usos indevidos. No Posto Central é fácil registar o envio de resultados.

### **2.1.11 Recuperabilidade**

Existe bateria com capacidade para várias horas para minimizar o efeito de quebras de energia, e o software garante a recuperação no ponto de uma interrupção. É possível suspender o processo de votação, por exemplo em caso de desordem pública, e reabri-lo mais tarde.

### **2.1.12 Tolerância a Falhas**

Registámos a afirmação, por parte dos elementos da empresa, de que a informação é registada em três memórias diferentes, não voláteis, pelo que existe alguma tolerância a falhas.

### **2.1.13 Isolamento**

Sem informação.

### **2.1.14 Segurança das comunicações**

A informação é enviada não cifrada mas com CRC e é sempre possível confirmar os valores, uma vez que os resultados são também impressos na Mesa e assinados pelos respectivos membros.

### **2.1.15 Escalabilidade do Sistema**

Relativamente ao universo de eleitores nas secções de voto abrangidas pela experiência, o equipamento funcionou bem porque votaram menos de 1320 eleitores. Se a abstenção tivesse sido menor, teria sido necessário abrir mais Mesas, com mais Cadernos Eleitorais, embora cada mesa pudesse dispor de menos Postos de Votação. Na configuração usada, o estrangulamento estava claramente no Caderno Eleitoral, estando os Postos sobredimensionados.

## **2.2 Transparência (T)**

### **2.2.1 Anonimato**

Não existe nenhuma ligação visível entre o Caderno Eleitoral e os Postos de Votação, ou o Posto Central. Para além disso, foi afirmado que os votos não são registados no Posto de Votação por ordem de chegada mas sim por ordem aleatória, para garantir que não se pode associar a posteriori um voto com o eleitor que votou numa determinada ordem.

No entanto, para tornar mais evidente para o eleitor a impossibilidade de associação entre o seu nome e o voto, sugere-se que exista sempre um grupo de Chaves de Voto previamente regeneradas das quais seja o eleitor a escolher a que vai usar e que, ao devolver a Chave, esta seja também colocada num conjunto de outras chaves para se desassociar do eleitor antes do processo de regeneração. Não foi este o procedimento utilizado, sendo um elemento da mesa a entregar a Chave ao eleitor e outro a recebê-la.

### **2.2.2 Atomicidade**

A atomicidade não está garantida. É possível um eleitor levantar a Chave, aparentar votar sem o fazer e ser dado como tendo concluído a votação, criando desse modo uma inconsistência entre o número de votos nos Postos e o número de votos no Caderno Eleitoral. Situações em que este seja superior àquele não parecem muito graves, podendo ser consideradas abstenções. No entanto é uma situação a evitar porque pode mascarar perturbações em sentido contrário, essas sim graves por violarem a singularidade.

Se, por engano, se entregar uma Chave de Voto a um eleitor que já tenha votado, não é possível desfazer esse voto e o número de votos nos Postos fica superior ao do Caderno Eleitoral. Este engano pode ocorrer facilmente devido à falta de alarme com que o Caderno Eleitoral interage nessa situação, detectando-se eventualmente o problema só na fase de devolução da Chave e recuperação do cartão de eleitor.

### **2.2.3 Autenticidade (método de autenticação do utilizador)**

A autenticação é efectuada por cartão de eleitor mais bilhete de identidade, presencialmente. O Caderno Eleitoral tem uma interface em que está sempre um eleitor seleccionado, o primeiro que corresponde à informação já introduzida, seja um número de cartão de eleitor parcialmente introduzido ou um nome de eleitor. O número de erros de aceitação com esta interface poderá ser elevado. Especialmente no caso da pesquisa por nome, uma vez que os eleitores são apresentados sempre ordenados por número. Sugere-se como alternativa a visualização do conjunto de eleitores que satisfazem a chave parcial já introduzida, só sendo possível a aceitação do eleitor quando esse conjunto estivesse reduzido a um elemento.

Acresce o facto de o Caderno Eleitoral ter erros ortográficos e em especial omitir os caracteres acentuados e os c's cedilhados.

### **2.2.4 Confiabilidade**

A confiabilidade é directamente afectada pelas observações a propósito da Integridade dos Votos e do Anonimato.

### **2.2.5 Documentação técnica**

A documentação técnica a que tivemos acesso foi praticamente inexistente, sendo de registar a disponibilidade do responsável pelo processo na empresa para uma reunião de explicação do funcionamento mas sem capacidade de esclarecimento dos aspectos mais técnicos.

### **2.2.6 Integridade do Pessoal**

A Mesa é constituída por elementos da Junta de Freguesia. Não houve mais elementos sobre este aspecto.

### **2.2.7 Integridade do Sistema**

Sem informação.

### **2.2.8 Não-Coercibilidade**

Garantida pelo processo, a menos que num dos Postos de Votação só houvesse um voto.

### **2.2.9 Precisão do SVE**

Não foi detectada nenhuma introdução de erros pelos equipamentos. Quando muito, pelo processo, tal como se referiu a propósito da Atomicidade.

### **2.2.10 Privacidade**

Garantida, a menos que fosse possível obter os votos num determinado posto por sequência de entrada.

### **2.2.11 Singularidade (Não Reutilização)**

O Caderno Eleitoral não alerta suficientemente para a tentativa de o mesmo eleitor votar duas vezes. As únicas indicações visuais de que um eleitor já votou são uma bolinha verde à esquerda do nome do eleitor e o botão que coloca o eleitor em processo de votação fica inactivo. No entanto, não há nenhum outro alarme visual ou sonoro pelo que, devido ao cansaço do presidente da mesa que opera o Caderno Eleitoral, é possível entregar a Chave de Votação inadvertidamente, o eleitor votar pela segunda vez e até nem se tornar notório que o fez ao devolver a chave e levantar o cartão, pois só depois de o cartão já ter sido devolvido é que o vogal informa o presidente de que o eleitor terminou o processo e o presidente retira o eleitor da lista dos que estão em processo de votação e o dá este por concluído. Mesmo aqui, por vezes sucede que o presidente dá por concluído o eleitor ao lado, podendo surgir a dúvida sobre se foi engano do presidente ou se o eleitor já tinha votado e estava a repetir a votação ilegalmente.

### **2.2.12 Transparência do Processo**

É difícil para os eleitores comuns compreenderem em detalhe todos os mecanismos do processo. No entanto, do ponto de vista funcional, encontrava-se a funcionar em permanência um pequeno vídeo com a exemplificação do procedimento.

### **2.2.13 Transparência do Sistema**

Apesar de solicitada a documentação técnica que permitiria responder, ao menos parcialmente a esta questão não foi disponibilizada. Foi em particular solicitado o formato de envio de dos resultados finais e a descrição do conteúdo das memórias flash introduzidas em cada Posto de Votação.

### **2.2.14 Verificabilidade**

Não há nenhuma verificabilidade pois todo o registo é interno ao Posto de Votação e não é emitido nenhum recibo.

### **2.2.15 Separação de papéis**

A abertura e fecho dos Postos de Votação e o envio dos resultados foram efectuadas pelos elementos da empresa e da UMIC e não pelos elementos da Mesa.

## **2.3 Acessibilidade (A)**

### **2.3.1 Conveniência**

O processo foi rápido embora em muitas situações tivesse sido necessário recorrer à ajuda dos elementos de apoio presentes na sala. Uma vez que o Caderno continha todos os eleitores da freguesia, mesmo os eleitores de outras secções de voto puderam votar electronicamente na Mesa do Monte Velho. Possivelmente, alguns terão também votado na outra Mesa, a troco de umas T-shirts, uma vez que as BD's do Caderno Eleitoral eram locais.

### **2.3.2 Direito de Voto**

Já foram referidas acima algumas deficiências do Caderno Eleitoral, que poderiam dificultar a identificação de um eleitor por nome.

### **2.3.3 Documentação para eleitor**

Existe um vídeo demonstrativo e um folheto explicativo.

### **2.3.4 Flexibilidade**

Embora não demonstrada no Monte Velho (por falta de tempo para a programação da informação áudio), existe uma variante dos Postos de Votação com botões e saída de áudio para uso por eleitores com dificuldades visuais ou até por analfabetos. Desta forma, é dispensável o acompanhante que habitualmente auxilia o deficiente visual nas votações em papel.

### **2.3.5 Mobilidade**

Esta propriedade não foi demonstrada no teste efectuado, uma vez que a BD do caderno Eleitoral é local.

### **2.3.6 Usabilidade**

O Caderno Eleitoral apresenta vários problemas do ponto de vista de usabilidade. O mais grave é a “passividade” com que (não) reage a situações de tentativa de o mesmo eleitor votar duas vezes. Limita-se a colocar o botão de autorização inactivo, fazendo com que um click em cima nada produza, em vez de alertar visual e sonoramente o presidente da Mesa para o facto.

A pesquisa por nome seria beneficiada se a lista dos eleitores também pudesse ser ordenada por nome.

O botão que marca o processo de votação de um eleitor como não tendo sido concluído (uma situação que deverá ser rara) tem o mesmo destaque que o botão que marca o processo como

concluído e, pior, encontra-se no caminho do rato entre a caixa onde se selecciona o eleitor e o botão de aceitação. Poderá portanto ser accionado inadvertidamente.

O uso do Caderno Eleitoral é muito desgastante, ocorrendo um aumento significativo da taxa de erros com o cansaço do presidente da Mesa. Deveria haver uma rotação maior do presidente, com períodos de trabalho inferiores a uma hora.

A maior cadência de eleitores observada foi de 2.3 eleitores por minuto, o que limita uma mesa de voto em 11H de trabalho contínuo a processar 1320 eleitores no máximo.

O Posto de Votação, ergonomicamente é bom, com ecrã inclinado para evitar reflexos e protecções superior e laterais para garantir a privacidade do voto, tudo numa mala antichoque fácil de montar, desmontar e transportar.

O Posto de Votação é activado por uma Chave de Voto. Esta chave só pode entrar na ranhura respectiva numa posição. Muitos eleitores, ao falharem uma ou duas vezes o encaixe solicitaram ajuda aos elementos de apoio presentes na sala.

Os ecrãs de votação tinham uma pergunta inicial de idioma, que seria evitável se as versões em Português e Inglês estivessem reunidas num único Boletim. A escolha do partido é muito fácil de fazer e de corrigir num ecrã táctil, sem recurso a rato. As perguntas de inquérito serviram para demonstrar o uso em eleições com vários boletins, mas eram irrelevantes no caso concreto desta eleição. O ecrã de confirmação final das escolhas efectuadas não orientava claramente o eleitor para carregar num botão de conclusão no topo do equipamento, fora do ecrã. De facto toda a interacção era controlada por mensagens ao fundo do ecrã excepto no caso final. Muitas vezes foi necessária a intervenção dos elementos de apoio.

### **2.3.7 Viabilidade (Custo/Benefício)**

Na versão que foi testada, isto é, votação local, sem BD centralizada e, portanto, sem mobilidade, as vantagens do sistema são aparentemente duas: contagem dos votos mais rápida no final da votação e apoio para deficientes. Os custos envolvidos em generalizar estas máquinas a todas as secções de voto parecem assim excessivos para as vantagens obtidas. Sugere-se a possibilidade de montar um número pequeno de postos nas grandes cidades especificamente para a votação de invisuais.

### 3 Conclusões e Recomendações

#### 3.1 Conclusões

As conclusões gerais do sistema observado podem resumir-se nos seguintes aspectos principais:

- A Integridade do Voto e Verificabilidade do processo está dependente da resposta a dar aos aspectos de Certificabilidade, Invulnerabilidade e Integridade do Sistema que não puderam ser analisados por falta de informação e documentação técnica.
- A usabilidade quer do Caderno Eleitoral quer do Posto de Votação tem problemas que poderão ser ultrapassados em posteriores versões de ambos os produtos.
- A Rastreabilidade e correspondente Confiança do sistema são também problemáticas.
- É possível na prática o aparecimento de inconsistências entre o número de votos do Caderno Eleitoral e dos Postos de Votação.
- Do ponto de vista de análise custo/benefício o que se perde em garantia de Anonimato, Integridade do Voto e recursos financeiros não compensa os ganhos em velocidade do processo de contagem.

Não foi demonstrada na experiência que se refere o presente relatório a característica de Mobilidade. Sendo no entanto esta uma das principais vantagens potenciais de um SVE, tentou-se obter alguma informação junto da empresa que apresentou o equipamento de votação. Para obter Mobilidade seria necessário garantir dois aspectos:

- A BD do Caderno Eleitoral teria que ser centralizada por forma a minimizar os problemas com a Singularidade do voto que votações em secções de voto diferentes poderiam colocar.
- Os Postos de Votação teriam que conseguir apresentar boletins de voto diferentes conforme a circunscrição eleitoral do eleitor, em todas as eleições que não a do Parlamento Europeu. O equipamento testado permite fazer isso de dois modos: a regeneração da Chave de Votação pode ser feita especificamente para o eleitor que ao chegar ao Posto de Votação vê o “seu” boletim de voto, mas isso levanta maiores problemas do ponto de vista de Anonimato e Privacidade; ou pode o supervisor activar o posto de votação que o eleitor vai usar especificamente para um determinado boletim de voto, o que parece pouco prático e sujeito a erros. Estes métodos têm problemas adicionais de Privacidade e Anonimato do voto, no caso de haver poucos eleitores de uma determinada circunscrição eleitoral, na fase de impressão e envio dos resultados. Seria necessário pensar num esquema de não publicar os resultados localmente o que agrava ainda mais os problemas de Rastreabilidade e Verificabilidade.

#### 3.2 Recomendações

As recomendações desta CASVE são as seguintes:

- Melhorar as interfaces do Caderno Eleitoral e dos painéis utilizados desta vez no Posto de Votação.
- Melhorar o procedimento na Mesa de forma a induzir confiança no anonimato no eleitor e a acelerar a verificação da identidade e a entrega de Chaves de Voto.
- Utilizar este sistema primordialmente em secções de voto centrais de grandes cidades, para utilização de invisuais e eventualmente analfabetos, garantindo um número total de votantes que não ponha em causa o Anonimato.
- Incluir uma impressora/urna em cada Posto de Votação de forma a melhorar o aspecto da Integridade do Voto e Rastreabilidade do processo.

## **ANEXO - Grelha para as Conclusões e Recomendações do Relatório de Auditoria ao Sistema de Votação Electrónica (RASVE)**

Apresenta-se de seguida a classificação resumo da Grelha de Avaliação usada na auditoria efectuada.



## Segurança

		-				+
<b>SEGURANÇA (S)</b>				X		
S	<b>Auditabilidade</b>			X		
	O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.					
S	<b>Autenticação do Operador</b>				X	
	Os utilizadores autorizados a operar o sistema devem ter mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjunção de alguns dos tipos de autenticação existentes. Por exemplo: cartão inteligente («Smartcard»), PIN ou senha, ou ainda autenticação bio-métrica – impressões digitais, retina ocular e voz.					
S	<b>Certificabilidade</b>			X		
	O sistema deve poder ser testado e certificado por agentes oficiais.					
S	<b>Fiabilidade</b>		X			
	O SVE deve funcionar de forma fiável, sem perda de votos.					
S	<b>Detectabilidade</b>				X	
	O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.					
S	<b>Disponibilidade do Sistema</b>					X
	Durante o período eleitoral, o SVE deve estar sempre disponível para todos os actores legítimos, em particular para os eleitores votantes, para que o processo decorra normalmente.					
S	<b>Imunidade a Ataques</b>			X		
	Medidas de defesa contra fraudes, inclusive vindas dos próprios agentes que projectaram e desenvolveram o sistema, devem ser rigorosas e redundantes. Um SVE, tal como outros sistemas de alto risco, pode ser alvo privilegiado de ataques mal intencionados.					
S	<b>Integridade dos Votos</b>		X			
	Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.					
S	<b>Invulnerabilidade</b>		X			
	A invulnerabilidade do SVE é a garantia de que não se pode aceder e alterar o sistema indevidamente.					
S	<b>Rastreabilidade</b>			X		
	O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir registos ("logs") de entrada e saída de utilizadores não eleitores ou de quaisquer outros acessos, bem como registos do envio e recepção de dados, que obviamente não comprometam as restantes propriedades (anonimato e privacidade do eleitor).					
S	<b>Recuperabilidade</b>					X
	O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.					
S	<b>Tolerância a Falhas</b>					X
	É desejável a existência de métodos de detecção de falhas no equipamento. A troca de um bit num total de um candidato pode ser a diferença entre ganhar ou perder a eleição.					
S	<b>Isolamento</b>				X	
	Só devem existir no SVE os dispositivos de interface externos absolutamente essenciais para o acto eleitoral, sendo todos os componentes certificados e iguais a um padrão, incluindo o software.					
S	<b>Segurança das comunicações</b>			X		
	As comunicações entre as assembleias de voto e o sistema central utilizam mecanismos de validação de identidade de ambos (assembleia e sistema central), de não adulteração da informação e de cifragem da mesma para garantir a confidencialidade, integridade e autenticidade.					
S	<b>Escalabilidade do Sistema</b>					X
	A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.					

## Transparência

		-		X		+
<b>TRANSPARÊNCIA (T)</b>				X		
T	<b>Anonimato</b>				X	
A associação entre o voto e a identidade do eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam manutenção do sistema) quer após a votação (mesmo que por ordem judicial).						
T	<b>Atomicidade</b>		X			
Garantia de que, em caso de falha a meio do processo, não permanecem registos ou percepções inconsistentes relativos ao mesmo. Por exemplo: registos no caderno eleitoral de votantes, mas sem registos de voto no computador; o eleitor e a mesa ficaram com a percepção de que o voto se concretizou, quando na realidade não ficou nenhum registo no computador; falha de alimentação quando o votante confirma a opção de voto no computador, como se sabe se o voto foi concretizado (por forma a tornar os registos consistentes entre si e consistentes com a percepção das pessoas envolvidas)?						
T	<b>Autenticidade (método de autenticação do utilizador)</b>					X
Autenticar o indivíduo é o meio pelo qual a identificação de um votante é validada e confirmada. Apenas os eleitores autorizados devem poder votar. Exemplos de tipos de autenticação são: presencial, PIN, senha, certificado digital, cartão inteligente ou bio-métrica.						
T	<b>Confiabilidade</b>				X	
O SVE deve funcionar de forma fiável e robusta, tornando-se confiável aos olhos dos diversos actores envolvidos, em particular o eleitor.						
T	<b>Documentação técnica</b>			X		
Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema, devem estar documentados, devendo não conter ambiguidades e ser coerente.						
T	<b>Integridade do Pessoal</b>					X
O pessoal envolvido no projecto, implementação, administração e operação do SVE deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.						
T	<b>Integridade do Sistema</b>			X		
Deve ser possível garantir em qualquer momento que o SVE que está a ser usado é o mesmo que foi validado e certificado por auditores externos, pela Comissão Nacional de Eleições e pelos membros da mesa de voto, eventualmente por um processo de amostragem.						
T	<b>Não-Coercibilidade</b>					X
O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.						
T	<b>Precisão do SVE</b>				X	
As eleições podem ser decididas por apenas um voto. O sistema não pode tolerar margens estatísticas de erro durante a sua operação.						
T	<b>Privacidade</b>					X
O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.						
T	<b>Singularidade (Não Reutilização)</b>			X		
O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.						
T	<b>Transparência do Processo</b>				X	
Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.						
T	<b>Transparência do Sistema</b>			X		
Todo o software, documentação, equipamento, micro-código e circuitos especiais devem poder ser abertos para inspecção e auditoria a qualquer instante. Deve ser conhecido o formato dos dados registados e transmitidos.						
T	<b>Verificabilidade</b>	X				
O sistema deve permitir verificar que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a autenticidade dos registos dos votos, sem no entanto quebrar outras propriedades como o anonimato ou a privacidade do votante.						
T	<b>Separação de papéis</b>				X	
O fabricante do SVE, o instalador e o operador não devem ser da mesma instituição ou empresa. Os únicos operadores do SVE durante o acto eleitoral devem ser elementos da mesa de voto ou elementos previamente acreditados pela Comissão Nacional de Eleições.						

**Acessibilidade**

		-				+
<b>ACESSIBILIDADE (A)</b>					X	
<b>A</b>	<b>Conveniência</b>					X
O sistema só será útil se permitir aos votantes exercerem o seu direito de voto de forma rápida, com o mínimo de equipamento, treino e sem necessidades específicas adicionais.						
<b>A</b>	<b>Direito de Voto</b>					X
O Direito de Voto será atribuído a um eleitor sempre que ele verifique simultaneamente as propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de ele poder votar.						
<b>A</b>	<b>Documentação para eleitor</b>					X
O eleitor deve ter acesso com a antecedência adequada a informação de compreensão simples sobre o SVE e as suas características.						
<b>A</b>	<b>Flexibilidade</b>					X
Os equipamentos de votação que fazem parte do SVE devem suportar uma variedade de questões relacionadas com o processo de votação, com por exemplo a utilização por pessoas com necessidades especiais, etc.						
<b>A</b>	<b>Mobilidade</b>					X
O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.						
<b>A</b>	<b>Usabilidade</b>			X		
O sistema deve ser de uso fácil e rápido, quer para eleitores quer para operadores (membros da mesa de voto). A interface do SVE, a linguagem e os termos utilizados, deve ser acessíveis aos eleitores e aos elementos que participam no processo eleitoral, não devendo ser necessário que estes tenham conhecimentos informáticos especializados. A localização, orientação e altura do monitor devem ser apropriadas ao eleitor. Um erro involuntário de um eleitor, mal treinado para votar em dado equipamento, pode inverter ou modificar o resultado eleitoral.						
<b>A</b>	<b>Viabilidade (Custo/Benefício)</b>		X			
O SVE deve ser eficiente e viável economicamente.						