

# **Projecto de Avaliação de Sistemas de Votação Electrónica – Resultados da Auditoria**

PEDRO ANTUNES  
NUNO NEVES  
LUÍS CARRIÇO  
PAULO VERÍSSIMO  
RUI ROCHA PINTO  
FILIPE SIMÕES

**VERSÃO 1.1**

**5 DE AGOSTO DE 2004**

LaSIGE – Laboratório de Sistemas Informáticos de Grande Escala  
Departamento de Informática  
Faculdade de Ciências da Universidade de Lisboa  
Campo Grande, 1700 Lisboa  
Portugal

## ÍNDICE

<b>1. SUMÁRIO</b> .....	1
<b>2. ANÁLISE DA EXPERIÊNCIA</b> .....	2
<b>3. ANÁLISE DA DOCUMENTAÇÃO</b> .....	11
<b>4. RESULTADOS DA AVALIAÇÃO</b> .....	12
<b>5. ANEXO – QUESTIONÁRIO AOS FORNECEDORES</b> .....	13

## 1. SUMÁRIO

Este documento apresenta os resultados da avaliação da experiência de voto electrónico realizada no dia 13 de Junho de 2004. A análise da experiência revelou um conjunto de problemas relacionados com falhas dos sistemas, falhas nos processos e, em particular, falhas na usabilidade e informação fornecida aos eleitores. Esta análise foi complementada com uma avaliação da documentação disponibilizada pelos fornecedores, incluindo as respostas ao inquérito enviado pela equipa da FCUL. Os resultados obtidos por estas duas vias indicaram que:

1. Os sistemas Indra e Unisys possuem qualidades apercebidas suficientes para poderem ser utilizados num processo eleitoral.
2. O sistema Multicert não revelou aos auditores essas qualidades, sendo apercebido como um protótipo com problemas de fiabilidade e usabilidade.
3. O sistema Unisys revelou ligeiras vantagens face ao sistema Indra.

## **2. ANÁLISE DA EXPERIÊNCIA**

### **Nota prévia**

Este texto tem como finalidade reportar as ocorrências e anotações que foram recolhidas pelos auditores durante a experiência de voto electrónico realiza em 13 de Junho de 2004. Procurou-se detectar quer falhas neste tipo de sistemas, para posterior correcção, quer distinções que permitam identificar que sistemas se encontram melhor preparados para cumprir os requisitos de um processo eleitoral.

Pela sua própria natureza, esta análise tende a realçar mais os factos negativos que os positivos, razão pela qual não deve ser usada fora do contexto acima indicado. Em geral, entende o grupo de auditores que a experiência de voto electrónico foi bem sucedida, não só pelo entusiasmo revelado por eleitores, representantes autárquicos e outros agentes, incluindo os da UMIC, com também pelo manancial de informação que permitiu recolher, com o objectivo de no futuro permitir que o voto electrónico passe de uma experiência a uma realidade.

### **Locais visitados**

A equipa da FCUL visitou as seguintes freguesias:

- Santa Maria de Belém (Lisboa)
- São Sebastião (Setúbal)
- Sé (Portalegre)
- São Bernardo (Aveiro)
- Salvador (Beja)

### **Descrição genérica do ambiente experimental**

Em todas as freguesias visitadas verificou-se que o local de voto electrónico se encontrava bem visível e próximo do local de voto “legal”. Verificou-se também que os eleitores estavam bem informados da ocorrência da experiência e – aspecto muito positivo a evidenciar da experiência realizada – demonstraram grande entusiasmo em participar no processo.

A tipologia do local de voto electrónico variou consoante o número de eleitores, sendo caracterizada por 1-2 mesas eleitorais, onde se fazia a verificação de direito de voto do eleitor (e nalguns casos, consoante o sistema utilizado, se colocavam os votos na urna), e 2-10 máquinas de votação.

Verificou-se que numa freguesia (São Bernardo) o número de mesas eleitorais e de máquinas de votação não estava dimensionado de forma a evitar longas filas de espera. Como será referido mais adiante, esta situação esteve fundamentalmente ligada ao facto de o sistema de votação utilizado requerer um processo de votação muito longo.

Notou-se uma clara distinção entre a sala de voto “legal” e a sala de “voto electrónico”, sendo a primeira claramente mais formal que a segunda. Para esta situação contribuíram dois aspectos fundamentais:

- Na sala de voto electrónico estavam diversos elementos da UMIC com a função de ajudar os eleitores no processo de votação.
- No caso do voto electrónico, a constituição das mesas eleitorais não seguia exactamente a lei eleitoral.

Este último aspecto aqui referido foi bastante evidente na freguesia de Santa Maria de Belém, onde as mesas eram unicamente constituídas por elementos da UMIC. Ao contrário, na freguesia de São Bernardo, estavam presentes na mesa eleitoral elementos designados pelos partidos e que normalmente participam no processo eleitoral.

Esta informalidade associada à experiência de voto electrónico criou alguma dificuldade ao processo de auditoria, já que dificultou a obtenção de comentários pertinentes dos agentes normalmente envolvidos num processo eleitoral e criou um cenário demasiado artificial, com consequentes enviesamentos na análise dos resultados.

### **Descrição genérica do papel dos avaliadores**

Os avaliadores assumiram fundamentalmente o papel de observadores do processo. Observaram-se as acções dos eleitores, sem no entanto colocar em causa o anonimato do voto: na maior parte das situações não foi possível observar directamente as interacções dos eleitores com os dispositivos de votação (nas outras ocorreu por solicitação dos eleitores, para fornecer ajuda). Foi possível observar sem restrições as acções dos elementos nas mesas eleitorais.

As observações foram complementadas com conversas informais com os diversos agentes envolvidos no processo, desde presidentes de juntas de freguesia aos elementos das mesas eleitorais, elementos do STAPE e elementos da UMIC.

### **Falhas detectadas relacionadas com os equipamentos**

Na freguesia da Sé ocorreram problemas com a inicialização do software de gestão dos eleitores (Multicert), aparentemente devidas a incompatibilidades com o tipo de ficheiro de dados fornecido pela junta de freguesia. Esses problemas resultaram num atraso de 45 minutos na abertura do voto electrónico.

Na freguesia de São Bernardo ocorreram também problemas na inicialização do software de gestão dos eleitores (Multicert), agravados pela demora do software em gerar os cartões de identificação dos membros da mesa eleitoral. Aliás, este mesmo problema já tinha ocorrido no ensaio geral realizado nas instalações do LNEC em 5 de Junho. Estes problemas originaram um atraso de cerca de uma hora na abertura do voto electrónico.

Na freguesia de Salvador ocorreu a avaria de um cartão de memória flash, deixando uma máquina de votação (Unisys) inoperacional. O elemento da empresa responsável pelo sistema presente no local de voto não conseguiu resolver o problema, tendo este sido posteriormente resolvido após a chegada de outro elemento chamado para o efeito. Note-se que os votos armazenados na máquina não foram perdidos. Notou-se no entanto a inexistência de procedimentos em caso de ocorrência de falhas nos equipamentos.

Na freguesia da Sé, ocorreu uma falha numa das máquinas de votação (Indra), mas que ficou resolvida após reinicialização da máquina. Os votos armazenados na máquina não foram perdidos.

Em Santa Maria de Belém, após o fecho das eleições, uma das máquinas de votação (Indra) apresentou dificuldades em estabelecer ligação telefónica para proceder ao envio de resultados. Este problema foi resolvido após algumas tentativas da operadora da UMIC, sendo devido a problemas nos contactos da ficha telefónica.

Note-se no entanto que, tendo por base a situação que foi observada em Santa Maria de Belém, o uso em grande escala da ligação telefónica deve ser estudado com detalhe, parecendo ser um processo demorado. A título de exemplo, a transmissão dos resultados da freguesia de Santa Maria de Belém, constituída por apenas 10 urnas, demorou cerca de meia hora.

Na freguesia da Sé ocorreu um caso em que o cartão magnético (Indra) apresentou um problema técnico, não permitindo o voto do eleitor. Neste caso, o cartão, supostamente defeituoso, foi colocado à parte por um elemento da mesa e ao eleitor foi atribuído um novo cartão. Observou-se que não existia nenhum procedimento especial para lidar com cartões defeituosos.

Ainda relativamente à freguesia da Sé, observou-se que o cabo de alimentação de uma das máquinas de votação (Indra) se soltou e a urna não emitiu qualquer aviso sonoro, ao contrário do que refere a documentação do sistema e foi experimentado nas instalações da Indra pela equipa de avaliadores da FCUL. Observou-se que a máquina continuou a funcionar devido à existência de uma UPS embutida.

Na freguesia de Salvador ocorreu uma falha de energia de cerca de 10 minutos. Durante esse período as máquinas de votação (Unisys) continuaram a funcionar, devido à existência de UPS nas máquinas. No entanto observou-se que o software de gestão dos eleitores (Multicert), executado num PC normal sem fonte de energia alternativa, não esteve disponível durante esse período, situação em que foram utilizados os cadernos eleitorais tradicionais.

Não tendo a equipa de auditores visitado a freguesia de Paranhos, foi informada pela UMIC que uma das máquinas do sistema (Multicert) não enviou em tempo útil a contagem de votos.

Em resumo, pode considerar-se que do ponto de vista das falhas de equipamento os resultados da experiência foram apenas razoáveis. Existiram múltiplas ocorrências, nenhuma delas crítica, mas observou-se também que não existiam procedimentos estabelecidos para lidar com essas ocorrências.

Tudo indica que a probabilidade de falha localizada do sistema de voto electrónico é significativa. Não temos dados científicos para atribuir um valor a essa probabilidade, mas evidenciamos que em 5 freguesias ocorreram 2 falhas de inicialização com atraso superior a 45 minutos.

### **Falhas detectadas nos procedimentos de operação do sistema**

Como já foi referido anteriormente, o ambiente geral em que decorreu a experiência não permitiu estabelecer padrões rígidos de controlo do sistema. Por essa razão, todo o processo de selagem das máquinas de voto antes das eleições e verificação imediatamente antes de dar início ao processo eleitoral não foi realizado.

A finalização formal do processo eleitoral não foi igualmente realizada. Em particular, considerando que a contagem de votos pode ser verificada cruzando informação das máquinas de voto e do software de verificação do direito de voto, não foi acautelado o rigor necessário a esse cruzamento.

Na freguesia de São Sebastião, foi possível verificar que foi dado o direito de voto sem que esse direito tenha sido efectivamente exercido e sem que o direito de voto tenha sido posteriormente cancelado.

Na freguesia de Santa Maria de Belém verificou-se que o software que fazia a verificação de direito de voto (Multicert) não foi fechado às 20:00, pelo que era possível aos passantes usar o software, por exemplo para indicar que novos eleitores tinham votado.

Na freguesia de São Bernardo ocorreu um caso mais complexo, mas que por isso mesmo deve ser descrito em maior detalhe. O caso ocorreu quando uma eleitora, depois de votar, saiu do local levando o cartão magnético. Após alguns instantes sem que a eleitora voltasse, foi decidido pelo membro da mesa que o seu direito de voto devia ser cancelado. O software de verificação de direito de voto (Multicert) gere uma lista dos eleitores a quem foi atribuído o direito de voto, materializado na posse do cartão magnético. Junto a cada entrada dessa lista existem botões que permitem aceitar ou cancelar o direito de voto. A situação que ocorreu foi que o membro da mesa se enganou, acabando por cancelar o direito de voto de outro eleitor. Esta operação não é reversível. Em seguida a eleitora voltou ao local, sendo o membro da mesa obrigado a pedir-lhe que votasse de novo, tendo para o efeito, no software, seleccionado não o nome da eleitora mas sim o nome do outro eleitor que sem o saber viu o seu voto cancelado. Notou-se que não existiam procedimentos de registo de ocorrências pelos elementos da mesa, de forma a acautelar possíveis problemas levantados por auditorias posteriores.

Nalguns casos o ciclo de utilização dos cartões magnéticos também não foi devidamente acautelado. Em particular, o processo utilizado na freguesia de Santa Maria de Belém (Indra), onde cada voto era autorizado por um cartão magnético não reutilizável, exigia que os cartões fossem guardados de forma segura, o que não veio a acontecer. Aliás toda a gestão dos cartões magnéticos foi pouco controlada, devendo estes idealmente encontrar-se numa caixa especial que permitisse a entrega de um único cartão de cada vez, não estando nenhum outro cartão acessível.

Não é claro para os avaliadores se os cartões utilizados pelo sistema Indra armazenam os votos. Admite-se que não. No entanto observou-se que os cartões magnéticos entregues a cada votante para realização da votação apresentavam uma numeração, o que possibilita a quebra de anonimato se forem relacionados com informação de log da máquina de voto. Observou-se ainda que os cartões entregues aos eleitores não eram entregues de forma totalmente aleatória, mas sim de forma sequencial, o que também facilita a quebra de anonimato do voto.

### **Falhas detectadas no processo de votação**

Verificou-se que na freguesia de São Bernardo se formavam longas filas de espera para votar. Apesar de a relação mesas eleitorais/máquinas de votação ser desfavorável (existia apenas uma mesa e duas máquinas de votação), o problema deveu-se fundamentalmente a um processo pouco optimizado de votação (Multicert). As medições efectuadas indicaram:

- Duração média de uma utilização da máquina de voto: 4 minutos
- Duração mínima observada de uma utilização da máquina de voto: 2 minutos
- Tempo necessário para a leitura do cartão magnético na urna: 15 segundos

Em contraponto, na freguesia de Santa Maria de Belém foram medidos:

- Duração média de uma utilização da máquina de voto: 2 minutos
- Duração mínima observada de uma utilização da máquina de voto: 1 minuto
- O sistema (Indra) não exigia leitura do cartão magnético

Foi registado que os membros da mesa eleitoral da freguesia de São Bernardo se queixavam em particular da demora na leitura dos cartões magnéticos. Na realidade, a arquitectura do sistema, tal como estava concebida, originava três filas de espera distintas: (1) diante da mesa de voto, para votar; (2) diante das máquinas de voto; e (3) de novo diante da mesa de voto, para proceder à leitura do cartão magnético.

### **Usabilidade dos dispositivos**

A usabilidade dos dispositivos de interface de todas as máquinas de voto revelou-se particularmente crítica na experiência que foi realizada, tendo sido observados múltiplos problemas.

A interface de votação do sistema Multicert iniciava-se com a apresentação de duas bandeiras, para escolha de idioma, sem qualquer texto adicional ou indicação visual de que os eleitores deviam seleccionar uma das bandeiras. Observou-se que os eleitores, não percebendo o que fazer, ficavam à espera de ajuda dos elementos da UMIC.

A interface de votação do sistema Multicert tinha um botão de “terminar” a votação que levava os eleitores a pensar que já podiam retirar o cartão da máquina de voto, pois o processo estava terminado. A interface no entanto não funcionava desse modo, apresentando aos utilizadores, demasiado tempo após seleccionarem tal botão, uma janela a dizer que já podiam retirar o cartão. Esta funcionalidade inadequada resultou numa taxa muito elevada de cartões que posteriormente eram rejeitados pela urna, obrigando os eleitores a votar segunda vez.

Ainda relativamente ao sistema de votação Multicert, observou-se que a urna demorava demasiado tempo a ler os cartões (cerca de 15 segundos), gerando um evidente desconforto quer nos eleitores quer nos membros da mesa eleitoral.

O “cartucho” utilizado pelo sistema Unisys não dava indicações aos utilizadores de como deveria ser colocado na ranhura dos dispositivo de votação, tendo sido observado que os utilizadores sistematicamente realizavam diversas tentativas, com consequentes demoras no processo de votação. Este problema observou-se praticamente com todos os utilizadores.



Ainda relativamente ao sistema Unisys, observou-se que o botão de bloqueamento do cartucho – um botão físico colocado no topo da máquina, ao centro – estava fora da área de foco dos utilizadores, que era normalmente em baixo, deixando assim os eleitores perdidos e a necessitarem de ajuda. Apesar de o botão físico colocado no topo da máquina ter uma luz que ficava intermitente, avisando assim os eleitores que tinham ainda que bloquear o cartucho, esse aviso foi sistematicamente ignorado.

Observou-se também que no sistema Unisys os botões de selecção de idioma (Português/Inglês) se encontravam demasiado juntos e num alinhamento vertical, o que originou que diversos eleitores acabassem por seleccionar o idioma errado (o alinhamento horizontal reduz a taxa de erros, por causa do alinhamento dos dedos na mão). A agravar esta situação, observou-se que a selecção de idioma não era reversível.

Ainda relativamente ao sistema Unisys, observou-se que os eleitores tinham muitas dificuldades em perceber o mecanismo de interacção que consistia em seleccionar o voto e premir um botão amarelo com a palavra “seguinte”.

Na freguesia da Sé (Indra), observou-se que a ranhura frontal do dispositivo de votação, que se encontra na urna para saída do relatório em papel, foi muitas vezes confundida pelos eleitores (independentemente da idade) com a ranhura para introdução do cartão magnético.

Não foram encontrados problemas de usabilidade no que se refere ao software de verificação de direito de voto (Multicert).

As maiores dificuldades relacionadas com usabilidade foram sem dúvida o auxílio prestado aos menos letrados. As pessoas menos letradas apresentaram imensas dificuldades em lidar com o processo de votação, sendo sempre necessária a intervenção dos elementos da UMIC para que o eleitor iniciasse e completasse o processo de votação.

Na freguesia da Sé ainda se experimentou que os eleitores menos letrados usassem a urna destinada aos invisuais, mas tal solução não resultou: para além do processo se tornar demasiado lento, nunca deixou de ser necessária a ajuda dos elementos da UMIC, pelo que tal solução rapidamente deixou de ser aplicada.

Em geral, a linguagem utilizada nas interfaces estava correcta mas tendia a ser pouco compreensível para pessoas menos letradas. Foram utilizadas palavras demasiado extensas, como “terminar”. Teria sido preferível a utilização sistemática de palavras mais curtas como “fim”. Os sistemas deveriam também ter recorrido ao uso sistemático de cores, como o “verde” para aceitar ou “vermelho” para cancelar ou alguns símbolos comuns, como o “X” para cancelar.

Relativamente à interface para invisuais, notou-se que a sua utilização era extremamente demorada (cerca de 15 minutos por eleitor). Registou-se inclusivamente um caso, na freguesia da Sé, em que o tempo limite temporal imposto pela urna para votar foi excedido. Notou-se em particular que a vocalização dos textos era realizada de forma demasiado lenta.

Nas máquinas da Unisys não estavam disponíveis interfaces para invisuais.

### **Informação disponibilizada aos eleitores**

Este tema está obviamente relacionado com o anterior, no sentido em que a falta de informação clara e precisa sobre o processo de votação e uso dos dispositivos agravou muito substancialmente os problemas de usabilidade, em particular no caso da máquina de votação da Unisys.

A informação distribuída aos eleitores foi insuficiente, tendo sido notado que praticamente 100% dos eleitores necessitaram de ajuda dos operadores. Foi particularmente evidente que mesmo os eleitores mais letrados recorreram sistematicamente à ajuda dos elementos da UMIC.

Na freguesia de São Bernardo foram distribuídos aos eleitores uns folhetos que apresentavam as instruções, em poucos passos mas com grande exactidão, utilizando fotografias que reproduziam exactamente o local e o modo como iriam votar. Foi observado que alguns eleitores votavam seguindo as instruções desse folheto, convenientemente colocado na mão esquerda, enquanto votavam com a mão direita. Ao contrário, em Santa Maria de Belém, os folhetos eram totalmente desadequados para fornecer essa ajuda: sem imagens e com um número demasiado elevado de passos (10). Observou-se que não eram utilizados.

Na freguesia de Salvador, ao invés de folhetos era apresentado um filme que ilustrava o processo de votação. O equipamento de projecção ficava precisamente nas costas da fila que os eleitores formavam para votar, pelo que acabava por não ter papel relevante.

O uso de palavras técnicas, como “smartcard”, deve ser evitado neste tipo de folhetos.

Ficou absolutamente evidente que os folhetos são um componente fundamental do sistema de votação electrónica, não podendo de todo ser negligenciados.

Foi sugerido por elementos das juntas de freguesia que alguns exemplares dos sistemas de votação deveriam ser facultados antes do processo eleitoral, de forma a que os elementos das mesas se pudessem familiarizar com a tecnologia antes do acto eleitoral.

### **Avaliação dos sistemas face aos dados obtidos da experiência**

A partir dos dados acima analisados a equipa de avaliadores retirou as seguintes conclusões sobre os sistemas em avaliação:

Dispositivos que se mostraram aptos para utilização num sistema eleitoral:

- Indra
- Unisys

Apesar de estes dispositivos apresentarem conjuntos distintos de vantagens e desvantagem, ambos demonstraram ser produtos de engenharia suficientemente desenvolvidos e testados, possuindo elevada qualidade técnica apercebida. Uma comparação entre os dois dispositivos será realizada mais adiante.

Dispositivos que se mostraram não preparados para utilização num sistema eleitoral:

- Multicert (dispositivo de votação)
- Multicert (dispositivo de verificação do direito de voto)

O dispositivo de votação da Multicert apresentou duas limitações técnicas fundamentais: (1) deficiente usabilidade, já explicada, que levou a uma taxa elevada de cartões rejeitados; (2) processo de votação lento, devido à arquitectura utilizada e atrasos na leitura dos cartões magnéticos.

O dispositivo de verificação do direito de voto da Multicert apresentou problemas repetidos de fiabilidade. Por outro lado, devem também ser ponderados os seus poucos benefícios face à possibilidade de verificação de voto pelos meios tradicionais (cadernos eleitorais).

As limitações técnicas relacionadas com os dispositivos da Multicert sugerem que estes produtos não foram suficientemente experimentados e desenvolvidos ao ponto de serem utilizados num sistema eleitoral.

## Comparação dos dispositivos Indra e Unisys

Na tabela seguinte apresentam-se os principais factores de diferenciação que foram identificados durante a experiência.

	<b>Indra</b>	<b>Unisys</b>
Arquitectura	Muito simples, consistindo em dispositivos individuais e autónomos. Esta solução é prejudicada pelos potenciais atrasos na comunicação de dados, já que cada dispositivo tem de enviar os dados autonomamente. Não permite a supervisão dos dispositivos pela mesa eleitoral.	Mais complexa, consistindo em dispositivos de votação e um dispositivo de supervisão, envio de dados e impressão. No entanto permite otimizar o envio de dados, que é centralizado. Permite a supervisão dos dispositivos pela mesa eleitoral.
Cartões magnéticos	Servem apenas para desbloquear o dispositivo de votação. Há um cartão especial que permite aceder aos dispositivos de votação em modo de supervisão. Sendo numerados, é possível quebrar o anonimato do voto.	Servem para desbloquear e supervisionar o dispositivo de votação. Há um cartão especial que acumula os votos dos dispositivos de votação e depois os transfere para o dispositivo supervisor. Oferece um meio adicional e redundante de verificação dos resultados.
Usabilidade	Utilizadores confundiram a saída de impressão com a ranhura de introdução do cartão, problema facilmente solucionável.	Interface mais complexa, devido à combinação de botões físicos e virtuais. Cartão tem usabilidade deficiente. Problemas solucionáveis por via de adequada informação aos eleitores.
Processo	Tem passos difíceis de controlar: se o eleitor votou ou não; controlar o ciclo dos cartões.	Muito semelhante ao processo tradicional e por isso mesmo mais fácil de controlar.
Falhas	4 detectadas e facilmente resolvidas. Uma dessas falhas teve aparentemente comportamento diferente do especificado.	1 detectada e facilmente resolvida.
Qualidade apercebida	Muito boa	Muito boa

Tendo por base a comparação dos critérios apresentados na tabela, pode-se observar que relativamente aos critérios de usabilidade e qualidade apercebida os dois sistemas se igualam. No entanto o sistema Unisys apresenta vantagens relativamente aos critérios arquitectura, cartões magnéticos processo e falhas. Consequentemente, os avaliadores posicionam o sistema Unisys à frente do sistema Indra.

### 3. ANÁLISE DA DOCUMENTAÇÃO

A seguinte avaliação decorreu da análise da documentação dos sistemas de votação fornecidos, apreciação das respostas ao questionário em anexo enviadas pelos fornecedores dos sistemas, assim como da experimentação dos sistemas realizada pela equipa da FCUL. Os critérios de avaliação, assim como o tipo de pontuação foram especificados no documento Projecto de Avaliação de Sistemas de Votação Electrónica – Definição do Contexto e Critérios de Avaliação.

	<b>Indra</b>		<b>Unisys</b>		<b>Multicert</b>	
Fiabilidade						
Rastreabilidade	3	Fornece log total dos eventos, não fica clara a disponibilidade imediata	9	Fornece log total dos eventos	1	Log não utiliza relógio
Anonimato	3	Pode ser quebrado	9	Garantido pelo cartão	3	Pode ser quebrado
Confiabilidade	3	Suficiente	3	Suficiente	1	Protótipo
Verificabilidade						
Não-coercibilidade	9	Sem recibo	9	Sem recibo	9	Sem recibo
Transparência do processo	3	Distinto do tradicional, sendo necessário controlar cartão	9	Semelhante ao tradicional	9	Semelhante ao tradicional, incluindo urna
Conveniência	9	Muito fácil para os eleitores	3	Mais complicado	1	Complexo
Acessibilidade	3	Funciona, mas muito lento	3	Disponível no futuro	0	Não disponível
Usabilidade	9	Bem testada	9	Bem pensada	1	Problemas sérios
Transparência do sistema						
Certificabilidade	9	EUA, cumpre várias normas e certificados	9	EUA	0	Não tem
Auditabilidade	3	Possível	3	Entidades externas	9	Disponível
Integridade dos votos					3	Assinaturas
Tolerância a ataques	3	SO controlado, mas é preocupante por ser MS	9	Utilização de SO próprio, outras medidas	1	Apenas discos controlados, uso da Internet, desenvolvimento em máquinas ligadas a Internet
Autenticação do operador	3	Standard	3	Standard	3	Standard
Integridade do pessoal	3	Procedimentos internos de segurança				
Recuperabilidade						
Tolerância a faltas	3	Dispositivos de diagnóstico e recuperação	9	Dispositivos em triplicado		
Disponibilidade	3	Dispositivos de diagnóstico e recuperação	3	Dispositivos de diagnóstico e recuperação		
Detectabilidade						
Integridade do sistema			9	Combinação de diversos dispositivos		
Invulnerabilidade						
Testes	9	Diversos, incluindo eleições	9	Diversos, incluindo eleições	0	Protótipo, testes internos
Certificados	9	Cumprir várias normas e certificados	9	Cumprir várias normas e certificados		
<b>Totais</b>	<b>87</b>		<b>117</b>		<b>41</b>	

Note-se que os resultados aqui apresentados resultam de um processo de avaliação com características experimentais definidas pela UMIC. Sendo assim, estes resultados não têm as características definitivas que resultariam do estudo profundo e sistemático dos diversos sistemas em avaliação. Por outro lado, deve ser referido que a comparação envolve sistemas que, na apreciação dos avaliadores, apresentam graus distintos de maturidade, sendo o sistema Multicert claramente um protótipo, pelo que se apresenta naturalmente desfavorecido face aos restantes.

#### **4. RESULTADOS DA AVALIAÇÃO**

O processo de avaliação revelou que os sistemas Indra e Unisys possuem qualidades apercebidas suficientes para poderem ser utilizados num processo eleitoral.

O sistema Multicert não revelou aos auditores essas qualidades, sendo apercebido como um protótipo com problemas sérios de fiabilidade e usabilidade.

O sistema Unisys revelou uma ligeira vantagem face ao sistema Indra principalmente em aspectos relacionados com diferenças arquitecturais. A avaliação mais fina da documentação fornecida face aos critérios de avaliação que foram estabelecidos confirmou essa ligeira vantagem.

Foram detectados diversos problemas que devem ser analisados cuidadosamente no caso de qualquer um destes ou outros sistemas serem utilizados em larga escala em futuras eleições. Em particular destacam-se:

- Definição clara e controlo rigoroso do processo de votação.
- Definição de medidas e procedimentos para tratar os casos de falha mais comuns.
- Fornecimento de informação adequada e simples sobre o processo de votação.
- Escolha criteriosa e sistemática de comandos das interfaces com os eleitores, utilizando palavras, formas e cores facilmente identificáveis.
- Simplificação do processo de votação dos eleitores com deficiências visuais.
- Realização de auditorias rigorosas aos sistemas e dispositivos adoptados.

## 5. ANEXO – QUESTIONÁRIO AOS FORNECEDORES

### PROCESSO ELEITORAL

1. Como é realizada a abertura do processo eleitoral? Quem a realiza?
2. Como é realizado o fecho do processo eleitoral? Quem o realiza?
3. Que passos são realizados para verificar o direito de voto do eleitor?
4. Que passos são realizados para autorizar a votação do eleitor?
5. Quem autoriza a votação do eleitor? Pode ser substituído?
6. O eleitor, após autorizado a votar, pode abandonar o local sem votar? Como é controlada tal acção?
7. Como continua o processo caso o eleitor se recuse a votar, desmaie ou fuja, por exemplo? Pode ser “desbloqueado”? Quem é responsável pela reposição da situação?
8. Que passos são realizados para bloquear a urna depois do voto de um eleitor?
9. Que passos são realizados para proceder à contagens dos votos?
10. Que passos são realizados para proceder à comunicação dos resultados?

### PRODUTO

1. O código fonte é auditável?
2. Foi desenvolvido algum microcódigo? Onde é utilizado?
3. Em que linguagens de programação foi desenvolvido o software?
4. Que sistemas de gestão de bases de dados são utilizados?
5. Que sistemas operativos são utilizados?
6. Que periféricos são utilizados?
7. O software está comentado?
8. Qual é a dimensão do produto, em linhas de código?
9. Qual é a dimensão do produto, em número de ficheiros?
10. São utilizadas ferramentas de controlo de versões? Quais?
11. São utilizadas ferramentas de gestão da configuração? Quais?
12. São utilizadas ferramentas de gestão de projectos? Quais?
13. São utilizadas ferramentas de análise e desenho de software? Quais?
14. São utilizadas ferramentas de teste de software? Quais?
15. São realizadas regularmente inspecções ao código?
16. São utilizados planos de teste do software? Os resultados estão disponíveis para auditoria?
17. Foram realizados testes com utilizadores reais? Os resultados estão disponíveis para auditoria?
18. Foram realizados testes com utilizadores com necessidades especiais? Os resultados estão disponíveis para auditoria?
19. Existem certificados actualizados de qualidade de processos ou produtos (ISO, por exemplo)? Quais?
20. Foram utilizadas normas para a realização de interfaces com os utilizadores (ISO, por exemplo)? Quais?
21. O produto encontra-se dividido em componentes? A descrição desses componentes está disponível para auditoria?
22. Existe uma descrição exaustiva das medidas de segurança implementadas? Estão disponíveis para auditoria?
23. O modelo de dados é auditável?
24. Existem assinaturas digitais associadas a cada componente de software?
25. Que medidas de segurança informática são internamente utilizadas para salvaguardar o produto? O produto está a ser desenvolvido em máquinas ligadas em rede ao exterior da empresa?

### SISTEMA

1. Os operadores são autenticados perante o sistema? Como?
2. O eleitor é identificado perante o sistema antes de votar? Como?
3. Que dados têm de ser inseridos no sistema antes do acto eleitoral?

4. Como é feita a “inseminação” de dados? Nomeadamente como e quem insere os candidatos no sistema?
5. Que dados são apagados após o acto eleitoral? Como são apagados?
6. Que dados são preservados após o acto eleitoral? Como são preservados?
7. Existe algum procedimento de selagem do sistema antes do processo eleitoral?
8. Existe algum procedimento de selagem do sistema depois do processo eleitoral?
9. Existe algum procedimento de manutenção do sistema antes do processo eleitoral?
10. Existe algum procedimento de teste do sistema antes do processo eleitoral? O procedimento de teste exige alguma configuração do sistema especial?
11. É feito o registo de todas as ocorrências (logs)? Que eventos são registados?
12. O registo de ocorrências utiliza um relógio?
13. O registo de ocorrências é persistente?
14. O registo de ocorrências pode ser modificado pelos utilizadores privilegiados do sistema?
15. O sistema garante o acesso dos auditores ao registo de ocorrências?
16. Existem duas ou mais formas alternativas de registo de ocorrências? Quais?
17. Como é garantida a selagem das bases de dados?
18. Os votos são guardados em claro ou codificados?
19. Que técnicas de cifragem são utilizada para codificar os votos?
20. Os votos são guardados em associação, mesmo que indirecta, a alguns outros dados? Quais?
21. Quais os níveis de segurança para os vários utilizadores (administrador, operador, eleitor, etc)?
22. Qual é o número de utilizadores privilegiados do sistema?
23. São utilizadas técnicas especiais para prevenir ataques ao sistema?
24. Foram implementados mecanismos para evitar acções maliciosas realizadas pelos operadores privilegiados do sistema?
25. Foram implementadas técnicas para evitar ataques do tipo negação de serviço? Em particular relativamente à utilização de linhas telefónicas?
26. Existem procedimentos para garantir que o sistema operativo não foi modificado, por exemplo por vírus ou cavalos de troia?
27. O sistema encontra-se ligado em rede? Sempre? Quando? Que tipo de rede?
28. Que tipo de ligação é estabelecido entre componentes remotos do sistema? Que tipos de autenticação e codificação de dados são utilizados?
29. Que dados são transmitidos entre componentes remotos do sistema?
30. É utilizado algum mecanismo de tolerância a faltas na transmissão de mensagens?
31. É utilizado algum mecanismo de replicação na transmissão de mensagens?
32. Estão disponíveis alguns mecanismos de teste na transmissão de mensagens?

## URNA

1. A urna serve também para verificar se o eleitor pode votar?
2. Qual é o mecanismo de garantia de que um eleitor apenas pode votar uma vez?
3. A urna tem alguma fonte de energia alternativa (UPS, por exemplo)?
4. Caso seja preciso reinicializar a urna, está prevista a recuperação do sistema e da informação no ponto exacto onde foi suspensa?
5. Está previsto algum mecanismo ou procedimento de reinicialização?
6. A urna tem cabos de alimentação, conexão, etc.) acessível aos votantes?
7. A urna tem interfaces físicas (USB, por exemplo) acessível aos votantes?
8. A urna tem dispositivos físicos facilmente amovíveis pelos utilizadores (rato, por exemplo)?
9. A urna tem algum mecanismo de diagnóstico do seu funcionamento?
10. A urna mostra todas as mensagens críticas dos sistema? Designadamente as que reportam interrupções? Falhas de componentes ou serviços? Erros de software? Erros de transmissão?
11. A urna fornece um relatório de operação depois de terminada a votação?
12. É possível ensaiar uma votação, como se de uma votação se tratasse, sem procedimentos especiais?
13. A urna utiliza recibos em papel? Os recibos são colocados onde?
14. Existe separação física entre a urna e os restantes componentes do sistema?
15. A urna está ligada a alguma rede de comunicação de dados? Sempre? Quando?



16. A urna permite ligação ou recepção de dados originados no exterior? Como?
17. A urna tem alguma interface visível para o público a indicar quando está bloqueada e desbloqueada?
18. A urna tem alguma interface visível para o público a indicar a contagem dos votos?
19. A urna tem alguma interface que confirme qual o voto que o eleitor realizou e que esse voto foi armazenado no sistema?
20. Após o fecho das eleições, como são transmitidos os resultados? Para onde são transmitidos?

## **DISPOSITIVO DE VOTAÇÃO**

1. O dispositivo de votação é também urna, ou seja, serve também para guardar e contar votos?
2. O dispositivo de votação serve também para verificar se o eleitor pode votar?
3. O dispositivo de votação tem interfaces alternativas para utilizadores com necessidades especiais? Que tipos de utilizadores? Que tipos de interface?
4. O dispositivo de votação tem interfaces que confirmem qual o voto que o eleitor realizou?
5. O dispositivo de votação tem interfaces de confirmação do voto pelos eleitores?
6. A votação inclui a hipótese de voto em branco? E de voto nulo?
7. Após se dar início ao voto, o processo pode ser anulado pelo eleitor? Pode ser anulado pelo responsável da mesa eleitoral?
8. Qual é a dimensão do ecrã do dispositivo de votação? E a resolução?
9. Como é que o dispositivo de votação mostra aos utilizadores a lista de candidatos quando esta excede o espaço disponível no ecrã?
10. Os eleitores podem escolher a língua a utilizar nas interfaces? Que línguas estão disponíveis?