Auditoria ao Projecto de Voto Electrónico

Eleições Legislativas de 20 de Fevereiro de 2005

Relatório de Síntese Final

Fase de Pós-Simulação

Faculdade de Engenharia da Universidade do Porto

Porto, 15 de Abril de 2005

FEUP Rua Dr. Roberto Frias
4200-465 Porto
jfcunha@fe.up.pt Tel.: 22 508 1639
Fax: 22 508 1538

Relatório de Síntese Final da Auditoria ao Projecto de Voto Electrónico nas Eleições Legislativas de 2005-02-20

2005-04-15

Voto presencial

- Freguesia de S. Sebastião da Pedreira ..... Lisboa .....Empresa UNISYS
- Freguesia de Santos-o-Velho ..... Lisboa .....Empresa UNISYS
- Freguesia da Conceição .....Covilhã.....Empresa INDRA
- Freguesia de Coração de Jesus ..... Lisboa .....Empresa INDRA

Voto presencial com mobilidade

- Freguesia de Santa Iria de Azóia ..... Loures .....Empresa MULTICERT

Voto não presencial ou à distância pela Internet

- Europa e Resto do Mundo .....Empresa NOVABASE

Conteúdos

Página

Sumário Executivo 4
Agradecimentos 7
1 Introdução 8
1.1 Fases da Auditoria 10
1.2 Constituição da Comissão de Auditoria 13
2 Descrição da metodologia utilizada para comparação de sistemas de voto electrónico (SVE) 15
2.1 Análise e atribuição de ponderações aos sub-critérios 15
2.1.1 Aferição de entendimento acerca dos sub-critérios 15
2.1.2 Detecção de sub-critérios enquadrados em critérios não adequados 16
2.1.3 Ponderação de cada sub-critério em cada critério 16
2.1.4 Observações relativamente aos sub-critérios 19
2.2 Método de comparação dos sistemas de voto electrónico 19
2.3 Observação geral 22
3 Apreciação dos sistemas de voto electrónico 23
3.1 Resultados do inquérito aos eleitores 23
3.2 Descrição dos sistemas utilizados 24
3.2.1 Sistema de Voto Electrónico da UNYSIS 25
3.2.2 Sistema de Voto Electrónico da INDRA 29

3.2.3 Sistema de Voto Electrónico da MULTICERT 33
3.2.4 Sistema de Voto Electrónico da NOVABASE 35
3.3 Resumo de vantagens e desvantagens dos vários tipos de sistemas 41
3.3.1 Sistemas de voto electrónico presencial 41
3.3.2 Sistemas de voto electrónico presencial com mobilidade 42
3.3.3 Sistemas de voto electrónico não presencial pela Internet 43
3.4 Resumo de vantagens e desvantagens dos vários sistemas 44
3.4.1 Sistema de Gestão do Caderno Eleitoral da MULTICERT (utilizado em todas as experiências piloto presenciais) 44
3.4.2 Sistema de Voto Electrónico Presencial da UNISYS 46
3.4.3 Sistema de Voto Electrónico Presencial da INDRA 48
3.4.4 Sistema de Voto Electrónico Presencial com Mobilidade da MULTICERT 50
3.4.5 Sistema de Voto Electrónico à Distância pela Internet da NOVABASE 53
3.4.6 Quadro de Avaliação dos 4 SVE 54
4 Conclusões e recomendações 57
4.1 Conclusões 57
4.2 Recomendações 59
5 Referências e bibliografia 63
ANEXO A - Comissão de Auditoria da FEUP 67
ANEXO B - Propriedades de um sistema de votação electrónica 71
ANEXO C – Grelha para apoio à avaliação dos Requisitos de segurança, Transparência, Acessibilidade e Usabilidade 76

Sumário Executivo

A FEUP auditou as experiências de voto electrónico não vinculativo realizadas nas eleições legislativas de 2005-02-20. Estas experiências foram coordenadas pela UMIC e contaram com o envolvimento da CNE, do STAPE e da CNPD. A FEUP concluiu que a forma bem sucedida como decorreram torna viável e desejável a realização de testes de voto electrónico vinculativo presencial em próximas eleições. Os testes realizados foram voluntários e seria importante estudar a reacção a testes mais abrangentes.

Os níveis de segurança, transparência, usabilidade e acessibilidade já atingidos pelos sistemas de voto presencial disponibilizados pelas empresas UNISYS e INDRA, indicam claramente como possível, desejável e até prioritária a realização de testes de eleições electrónicas vinculativas, em alguns locais seleccionados ou abrangendo um universo limitado de eleitores que optem por este novo processo. Avançar no sentido de experiências vinculativas é agora essencial para se poderem vir a realizar eleições a nível nacional de forma electrónica, e para permitir a Portugal acompanhar os países europeus mais desenvolvidos neste processo.

No caso da experiência de votação electrónica realizada pela MULTICERT com o apoio da PT Inovação, em alguns aspectos inovadora a nível internacional, onde os eleitores podiam escolher a assembleia onde votar, a auditoria da FEUP concluiu que globalmente foi bem sucedida e com níveis de satisfação dos eleitores muito elevados. Esta conclusão considera em particular o prazo muito curto em que os sistemas foram desenvolvidos. No entanto, houve vários problemas técnicos na gestão do caderno eleitoral distribuído e houve um número significativo de dúvidas nos eleitores sobre se tinham de facto concluído a votação electrónica. As dúvidas foram partilhadas pelas pessoas na mesa de voto que permitiram assim a muitos eleitores votar mais do que uma vez. Recomenda-se assim que prossigam os esforços agora iniciados pelos vários parceiros envolvidos no sentido de melhorar a qualidade do sistema e do processo de votação para permitir a mobilidade dos eleitores e a escalabilidade do processo a nível nacional. Seria talvez desejável avançar para uma próxima experiência não vinculativa com assembleias de voto em algumas sedes de distrito, para testar a mobilidade a nível nacional.

O sistema desenvolvido pela NOVABASE para que os eleitores recenseados no estrangeiro tivessem disponível uma experiência de exercício de voto pela Internet decorreu de forma adequada, sendo possível antever que venha a ser uma alternativa directa ao voto por correspondência, com vantagens interessantes. A auditoria da FEUP recomenda que se continue o trabalho agora iniciado, melhorando a qualidade do sistema e segurança do processo de votação, em particular revendo a solução para distribuição de credenciais e a forma de autenticação, para que os eleitores autorizados

possam vir a optar por esta forma de exercer o seu direito de voto com maior garantia de anonimato. Também será importante estudar melhor as questões de segurança tentando prevenir a actuação de software malicioso nos clientes.

No sentido de melhorar os sistemas e os processos de voto electrónico, a equipa de auditores da FEUP recomenda de forma mais específica o seguinte:

- Melhorar a informação sobre o processo de voto electrónico, permitindo por exemplo ao eleitor o acesso a um sistema de voto electrónico para teste ou para treino no local de voto, e antes de votar vinculativamente ou não.

- Manter a impressão do voto em papel, garantindo assim a possibilidade de verificação pelo eleitor de que a sua opção de voto é registada da forma tradicional e garantindo ainda a possibilidade de contagem final pela mesa de voto.

- Melhorar os sistemas para garantir uma melhor percepção pelo eleitor e pelos elementos da mesa de voto sobre a ocorrência do exercício efectivo do voto. Deve ser possível ao eleitor não votar, mas não deve haver a mínima dúvida quando de facto o eleitor votou.

- Definir procedimentos rigorosos para todas as fases do processo e melhorar o conhecimento e experiência dos elementos da mesa de voto sobre o sistema a utilizar, em particular sobre os procedimentos que permitam eliminar discrepâncias entre o número de votantes e de votos expressos.

- No caso do voto pela Internet, melhorar o processo de distribuição de credenciais e considerar alternativas à utilização do código de eleitor para confirmar a sua identificação. Melhorar a informação para evitar software malicioso nos clientes.

- No caso do voto em mobilidade, para se permitir ao eleitor votar presencialmente em local diferente de onde está recenseado, considerar alternativas ao modelo do processo testado nestas eleições, para permitir a sua disponibilização a nível nacional de forma faseada, por exemplo recorrendo a um pedido prévio dos eleitores que optem por votar nessas condições.

- Aprofundar as soluções de apoio à acessibilidade, garantindo a inclusão de cidadãos com deficiências visuais ou com défice de literacia. No caso Internet, oferecer alternativas de acesso, por exemplo disponibilizando equipamentos em locais apropriados.

A equipa de auditores da FEUP considera que é essencial e urgente definir objectivos concretos em relação ao voto electrónico, ao mais alto nível nacional dos vários poderes legislativos e executivos, com um horizonte mínimo do final do próximo ciclo eleitoral completo, que se inicia com a próxima eleição para Presidente da República.

A definição de tais objectivos deve ser feita de forma inclusiva com as várias tendências políticas representadas na Assembleia da República. Os conhecimentos e as experiências já adquiridas a nível nacional pelas várias instituições e pessoas envolvidas nos testes realizados, deve ser aproveitada na definição desses objectivos, por forma a que as estratégias e acções a desenvolver para os atingir se possam concretizar com sucesso no horizonte estipulado. Um projecto com uma missão clara, gerido com sabedoria e apoio político, e com uma equipa experiente e empenhada será certamente essencial. Tal projecto deve envolver também a modernização de todos os processos necessários para a realização de consultas aos eleitores, que permita uma maior qualidade, flexibilidade e satisfação.

A disponibilidade para os processos de consulta pública de um sistema de voto electrónico flexível de elevada qualidade é sem dúvida um requisito relevante para a nossa sociedade em rápida evolução e para aproximar eleitores e governantes.

Agradecimentos

A equipa de auditores da FEUP agradece toda a colaboração prestada por todas as instituições e pessoas envolvidas no projecto, e pela sua disponibilidade para prestarem esclarecimentos e responderem a dúvidas, bem como para comentarem versões provisórias dos relatórios de auditoria. Atendendo aos prazos curtos em que o projecto decorreu esta disponibilidade é ainda mais relevante.

Para além disso a auditoria da FEUP gostaria de sublinhar a enorme dedicação e empenhamento no projecto que observou por parte de todos os técnicos e gestores das empresas directamente envolvidas, bem como dos técnicos de outras empresas por estas contratadas. Mais uma vez com os prazos curtos só essa dedicação permitiu a realização atempada do projecto, nas suas várias componentes, com um sucesso global indiscutível.

A equipa de auditores da FEUP não pode também deixar de fazer uma referência muito elogiosa à equipa técnica da UMIC responsável pela gestão e acompanhamento da iniciativa. Demonstrou ser incansável nas várias fases do projecto e acompanhou sempre todas as suas actividades. Em particular são de realçar os comentários apresentados às versões provisórias dos relatórios de auditoria, à proposta de apresentação pública de resultados preliminares e a uma versão inicial deste relatório final. Embora estivesse prevista na metodologia proposta pela FEUP, a interacção com a UMIC ultrapassou positivamente as expectativas e contribuiu assim também para o resultado desta auditoria. Em particular gostaríamos de realçar e louvar explicitamente as intervenções do Dr. João Ricardo Vasconcelos e da Dra. Sara Raquel Piteira.

1 Introdução

O presente relatório de auditoria à experiência piloto de voto electrónico, presencial, facultativo e não vinculativo, decorrida nas Eleições Legislativas de 20 de Fevereiro de 2005, envolveu 16 especialistas da FEUP, permitindo avaliar com grande rigor, independência e transparência os sistemas de voto electrónico utilizados pelas empresas UNISYS, INDRA, MULTICERT e NOVABASE, tendo em conta requisitos de segurança, transparência, usabilidade e acessibilidade. Dessa avaliação resulta a possibilidade de comparar a eficiência e a eficácia das diferentes tecnologias de votação utilizadas, com base em critérios e princípios estabelecidos à partida, e considerando ainda experiências e investigação em curso em outros países (ver por exemplo [IWEVE 2004]).

Globalmente a experiência piloto foi um enorme sucesso do ponto de vista de adesão e satisfação dos eleitores, do funcionamento dos sistemas e do conhecimento e experiência adicional que todos os agentes envolvidos obtiveram, tendo em vista a futura realização de eleições electrónicas em Portugal.

De acordo com os parâmetros internacionais mais exigentes (por exemplo [ACM 2004], [Bederson & Herrnson 2004], [Camp *et al* 2004], [Libbenga 2004], [Mercuri 2000] e [Thompson 1984]), alguns dos actuais sistemas são já adequados à realização de eleições vinculativas, considerando os requisitos referidos de segurança, transparência, usabilidade e acessibilidade. Embora nem toda a informação tenha sido disponibilizada à equipa de auditoria da FEUP por todas as empresas que participaram na experiência, todos os sistemas avaliados parecem permitir ou poder vir a permitir níveis adequados de segurança, transparência, usabilidade e acessibilidade, uma vez ultrapassado o período de aprendizagem com a sua utilização e resolvidos os problemas detectados (conforme relatórios de auditoria aos sistemas da UNISYS: [FEUP 2005a], INDRA: [FEUP 2005b], MULTICERT: [FEUP 2005c] e NOVABASE: [FEUP 2005d] abrangidos pelo presente trabalho).

A equipa de auditoria da FEUP assume como prioritárias as três seguintes orientações para o desenvolvimento dos sistemas de voto electrónico:

- Permitir a todos os eleitores o exercício do voto presencial em qualquer assembleia de voto. Para tal é necessária a integração e disponibilização global de uma base de dados nacional de eleitores, e a possibilidade de, em qualquer assembleia de voto, ao eleitor ser apresentado o boletim de voto apropriado. Este último requisito é particularmente exigente no caso de eleições locais. Este objectivo de permitir a mobilidade pode ser atingido de forma faseada, disponibilizando assembleias de voto distribuídas pelo país, onde tal seja

possível, eventualmente associada a uma manifestação de interesse por parte de um conjunto de eleitores.

- Garantir a possibilidade de re-contagem dos votos por parte de não especialistas de informática quando apareçam dúvidas sobre a correcção dos sistemas de voto electrónico ou para auditar uma amostra dos resultados obtidos por via electrónica nos sistemas em utilização. O registo do voto em papel requer cuidados especiais de informação ao eleitor e coloca entraves à possibilidade de oferecer mobilidade. Não é possível o registo em papel na votação não presencial.

- Divulgar publicamente, com suficiente antecipação, todos os detalhes dos sistemas e processos em uso pelos sistemas de voto electrónico[1], com preferência para os sistemas abertos e aplicações baseadas em sistemas abertos, não proprietários, e seguindo normas nacionais ou internacionais do domínio público.

Os meios de votação electrónica podem e devem contribuir para que os cidadãos confiem e participem nos actos eleitorais, e nessa medida estes sistemas devem ser utilizados e aperfeiçoados. A disponibilidade de um ou mais sistemas de voto electrónico satisfatórios é sem dúvida um requisito relevante para a nossa sociedade.

As tecnologias de informação e comunicação podem e devem ser pensadas de forma estratégica. Neste caso não podem ser pensadas apenas para substituir os meios tradicionais com vantagens operacionais, devem ser pensadas para melhorar o sistema de governação democrática, de forma a aumentar o conhecimento e a satisfação dos cidadãos e diminuir a distância para com as decisões mais relevantes.

Uma análise de custos e benefícios deverá considerar as várias alternativas de disponibilização dos sistemas (por exemplo: faseada, progressiva, híbrida ou total, dedicada a eleições nacionais ou não) e envolver o estudo das vantagens dos novos processos para todas as partes envolvidas, bem como as perspectivas de evolução social e económica subjacentes. Esta análise deverá ser efectuada conjuntamente com a definição de objectivos e estratégias ao mais alto nível político dos vários poderes requeridos.

De seguida referem-se as fases do processo de auditoria e apresentam-se os colaboradores da FEUP envolvidos. Na Secção 2 apresenta-se com detalhe a

[1] As normas do Conselho da Europa são claras neste aspecto: «Voters shall be provided with an opportunity to practise any new method of e-voting before and separately from the moment of casting an electronic vote." [Braun 2004].

metodologia de avaliação e comparação usada, e na Secção 3 faz-se uma apresentação e apreciação sumária de cada um dos 4 sistemas testados. Finalmente apresentam-se as principais conclusões e recomendações do estudo de auditoria. Neste aspecto são incluídas informações para orientação do ponto de vista técnico da acção política no domínio dos sistemas electrónicos de votação, e para impulsionar o debate nacional sobre as novas formas de participação electrónica em geral, e sobre os sistemas electrónicos de votação em particular.

1.1 Fases da Auditoria

Conforme definido à partida, a auditoria à experiência piloto de voto electrónico presencial, facultativo e não vinculativo decorrida nas Eleições Legislativas visava avaliar com grande rigor, independência e transparência os sistemas de voto electrónico (SVE) propostos pelas empresas UNISYS, INDRA, MULTICERT e NOVABASE, tendo em conta requisitos de segurança, transparência, usabilidade e acessibilidade.

Para tal efeito foi definido o seguinte processo a seguir pela equipa de auditoria da FEUP de acordo com as fases propostas pela UMIC (ver também Figura 1):

Fase I ? Pré-Simulação – Análise dos SVE propostos:

1. Análise da documentação disponibilizada pelos fornecedores, incluindo as fontes dos programas utilizados.

2. Esclarecimento de dúvidas sobre as características e funcionamento dos SVE, nomeadamente através de reuniões com as empresas fornecedoras.

Fase II ? Simulação – Acompanhamento geral do processo de votação electrónica, nomeadamente através da presença em todos os locais de voto no dia das eleições:

1. Acompanhamento da preparação dos SVE para o acto eleitoral.

2. Acompanhamento da inicialização do processo eleitoral nos SVE no dia das eleições – **abertura das mesas de voto electrónico**.

3. Acompanhamento geral do processo eleitoral e do funcionamento do SVE no dia das eleições – **processo de voto electrónico**.

4. Acompanhamento do processo de fecho do acto eleitoral nos SVE – **fecho das mesas de voto electrónico**.

5. Acompanhamento do processo de contagem e comunicação de resultados pelos SVE ao centro de integração de resultados na UMIC (voto presencial) e na CNE (voto pela Internet) – **comunicação e contagem dos votos electrónicos**.

Fase III ? Pós-Simulação – Conclusão da Auditoria e elaboração do Relatório Final de Auditoria incluindo conclusões e recomendações.

1. Caracterização e Comparação dos SVE.
2. Preparação dos Resultados da Auditoria e de Sugestões.
3. Análise Final dos Resultados e Preparação de Sugestões.

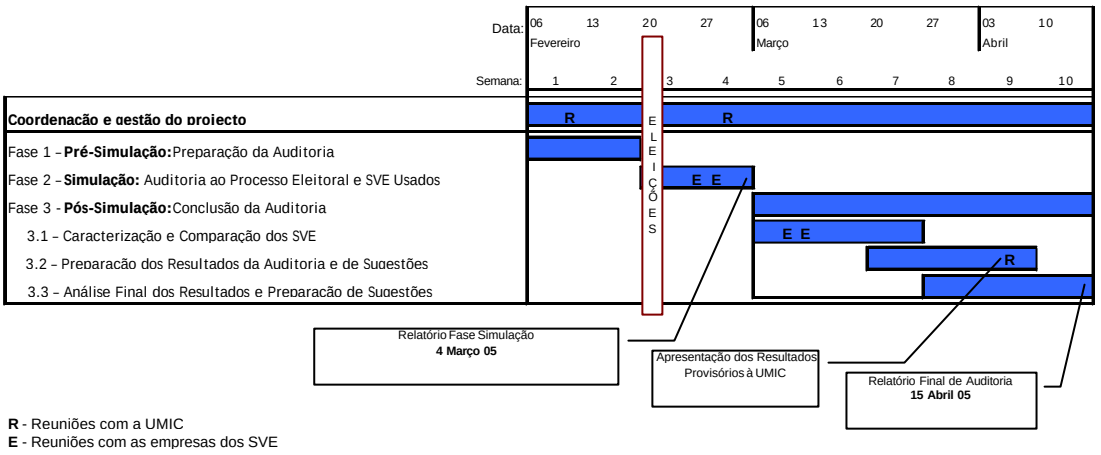

Figura 1 – Plano de actividades da auditoria da FEUP.

Considerando que a FEUP tinha por responsabilidade a auditoria aos 4 sistemas já referidos, distribuídos geograficamente por 5 freguesias em Lisboa, em Loures e na Covilhã[2], bem com a auditoria ao sistema de voto pela Internet cujo serviço estava igualmente centralizado em Lisboa, foram constituídas 4 comissões, designadas Comissões de Auditoria aos Sistema de Votação Electrónica (CASVE), cada uma delas com vários investigadores doutorados em áreas relevantes (com a constituição indicada na secção seguinte e Currículos breves em Anexo A). Para assegurar o conhecimento cruzado de pelo menos dois sistemas diferentes por cada auditor foi definido de forma adequada um plano de reuniões com as empresas e de visitas no dia das eleições. Para além disso recorreu-se à experiência dos relatores das auditorias à anterior experiência de voto electrónico para o Parlamento Europeu [FEUP 2004f], garantindo-se que os anteriores relatores seriam agora relatores para um outro sistema. A Figura 7, da secção 2.2 apresenta o plano das reuniões e visitas efectuadas, bem como da participação na elaboração dos relatórios de auditoria.

[2] Esta escolha de freguesias foi determinada pela UMIC para permitir que o Presidente da República e os líderes dos quatro principais partidos políticos experimentassem votar electronicamente.

O objectivo de cada uma destas comissões era estudar em detalhe cada um destes sistemas e acompanhar o processo eleitoral desde o seu início até ao final, incluindo a observação nos locais de voto, desde a inicialização dos sistemas até ao seu encerramento.

Como não era viável que todos os elementos da equipa da FEUP observassem todos os sistemas em operação, dada a distância a que alguns se encontravam, e para facilitar e promover a coerência no processo de auditoria, foi usada uma grelha de apoio à avaliação baseada nos requisitos de segurança, transparência, usabilidade e acessibilidade que se pretendia auditar. O Anexo B define todos os aspectos considerados e o Anexo C apresenta a grelha utilizada pelas Comissões.

Para além da grelha, foi ainda definido que haveria, no essencial, 8 momentos de auditora distintos, após a recepção das empresas ou da UMIC de informação técnica sobre os sistemas a serem utilizados:

- Elaboração dos pedidos de esclarecimento a enviar às empresas e reuniões prévias com as empresas.
- Realização das visitas aos locais de voto no dia das eleições.
- Redacção dos 4 Relatórios Intercalares de Síntese (RIS) de Auditoria aos Sistema de Votação Electrónica, excluindo o capítulo de Conclusões e Recomendações, e envio à UMIC (2005-03-05).
- Apresentação pública dos resultados preliminares da auditoria (2005-03-09).
- Após reuniões de avaliação e comparação das várias experiências, redacção do capítulo de Conclusões e Recomendações de cada um dos RIS.
- Envio à UMIC e às empresas dos RIS provisórios para apreciação (2005-04-10) e recepção de comentários.
- Redacção da versão final de cada RIS.
- Redacção do Relatório Final de Auditoria (o presente relatório) e seu envio à UMIC.

Foram assim elaborados 4 Relatórios Intercalares de Síntese, cada um deles com duas versões, as primeiras das quais foram disponibilizadas logo após as eleições, e cujas versões finais seguem como anexos separados a este Relatório Final de Auditoria. Foi ainda preparada uma apresentação dos resultados preliminares (cópia igualmente em anexo separado a este documento).

1.2 Constituição da Comissão de Auditoria

A comissão de auditoria da FEUP foi coordenada globalmente pelo Prof. Doutor João Falcão e Cunha, por indicação do Director da FEUP, Professor Doutor Carlos Albino Veiga da Costa, e nela participaram 16 investigadores e especialistas da FEUP, cujos currículos podem ser vistos no Anexo A.

Participaram no processo de auditoria directa aos SVE os seguintes colaboradores:

Prof. Doutor João Falcão e Cunha – Gestão e Sistemas de Informação
Prof. Doutor Mário Jorge Leitão – Telecomunicações
Prof. Doutor Gabriel David – Sistemas de Informação e Segurança
Prof. Doutor João Pascoal Faria - Sistemas de Informação
Prof. Doutor António Pimenta Monteiro – Informática
Prof. Doutor João Correia Lopes – Informática
Prof. Doutor António Carvalho Brito – Informática
Prof. Doutor José Magalhães Cruz – Informática e Segurança
Prof. Doutor Sérgio Reis Cunha – Telecomunicações
Prof. Doutor Raul Moreira Vidal – Informática
Profª. Doutora Henriqueta Nóvoa - Sistemas de Informação
Engenheiro João Vila Verde – Telecomunicações
Engenheiro Miguel Gonçalves – Informática
Engenheiro Luís Miguel Silva – Informática e Segurança

Na definição detalhada do processo de avaliação e comparação nos critérios e sub-critérios dos vários SVE, e no apoio a esse processo participaram ainda:

Prof. Doutor José Fernando Oliveira – Investigação Operacional
Profª. Doutora Maria Antónia Carravilla – Investigação Operacional

Com os objectivos referidos na secção anterior foram constituídas quatro equipas ou comissões, designadas Comissões de Auditoria aos Sistema de Votação Electrónica (CASVE), cada uma delas com pelo menos 3 investigadores doutorados da FEUP em áreas técnicas relevantes.

CASVE A – Sistema de Votação Electrónica da UNISYS

Freguesia de S. Sebastião da Pedreira - Lisboa

Freguesia de Santos-o-Velho – Lisboa

Prof. Doutor António Pimenta Monteiro – relator
Prof. Doutor António Carvalho Brito
Engenheiro Isidro Vila Verde
Prof. Doutor João Correia Lopes

Engenheiro Miguel Barbosa Gonçalves
Prof. Doutor Raul Moreira Vidal
Prof. Doutor Gabriel David

CASVE B – Sistema de Voto Electrónico da INDRA

Freguesia da Conceição - Covilhã

Freguesia da Coração de Jesus - Lisboa

Prof. Doutor Mário Jorge Leitão – relator
Prof.ª Doutora Maria Henriqueta Nóvoa
Prof. Doutor José Magalhães Cruz
Prof. Doutor João Correia Lopes
Prof. Doutor João Pascoal Faria
Engenheiro Miguel Barbosa Gonçalves
Prof. Doutor Sérgio Reis Cunha

CASVE C –Sistema de Voto Electrónico da MULTICERT

Freguesia da Santa Iria de Azóia - Loures

Prof. Doutor João Pascoal Faria – relator
Prof. Doutor Raul Moreira Vidal
Engenheiro Miguel Barbosa Gonçalves
Prof. Doutor Gabriel David
Prof. Doutor Mário Jorge Leitão
Prof. Doutor António Carvalho Brito
Prof.ª Doutora Maria Henriqueta Nóvoa
Prof. Doutor António Pimenta Monteiro
Prof. Doutor Sérgio Reis Cunha

CASVE D –Sistema de Voto Electrónico da NOVABASE

Europa e Resto do Mundo

Prof. Doutor Gabriel David – relator
Prof. Doutor Sérgio Reis Cunha
Prof. Doutor José Magalhães Cruz
Engenheiro João Isidro Vila Verde

2 Descrição da metodologia utilizada para comparação de sistemas de voto electrónico (SVE)

Com base na experiência do processo anterior de auditoria foram fixados quatro critérios para avaliação dos SVE e para cada um destes critérios um conjunto de sub-critérios, como se pode ver de seguida e nos Anexos B e C com mais detalhe.

Relativamente aos critérios e sub-critérios, antes do dia do processo eleitoral, foi realizada uma sessão de trabalho para fazer a aferição da sua avaliação pelos auditores. Nessa sessão de trabalho, com a participação de todos os auditores, foi também utilizada a metodologia AHP ([Saaty 1980], [Saaty 1987]) para atribuição da ponderação de cada sub-critério em cada critério ([Canter 1997]).

Em reuniões realizadas após o processo eleitoral, em que também participaram todos os auditores, foram então comparados os diversos SVE segundo cada um dos sub-critérios, sendo-lhes atribuída uma classificação numa escala de 1 a 5.

O produto interno das ponderações dos sub-critérios com as classificações obtidas por cada um dos SVE permitiu então obter uma classificação de cada SVE para cada critério.

2.1 Análise e atribuição de ponderações aos sub-critérios

Como já se referiu foram previamente definidos 4 critérios para avaliação dos SVE, nomeadamente Acessibilidade, Segurança, Transparência e Usabilidade, com os respectivos sub-critérios, que corresponderam a um refinamento relativamente ao processo anterior de auditoria [FEUP 2004f].

2.1.1 Aferição de entendimento acerca dos sub-critérios

A aferição de todos os sub-critérios foi feita numa reunião de preparação da auditoria, já referida, com a presença de todos os auditores. Nessa reunião, cada auditor explicitou verbalmente o que entendia por cada um dos sub-critérios, tendo-se chegado a um entendimento geral, que permitiu que, no dia das eleições, todas as avaliações fossem feitas de forma única e consistente. Foram também definidas formas de "medir" os sub-critérios e condições a cumprir por cada um dos Sistemas de Voto Electrónico para terem num determinado sub-critério uma avaliação intermédia (3) e máxima (5).

2.1.2 Detecção de sub-critérios enquadrados em critérios não adequados

Durante essa reunião foram também detectados alguns sub-critérios mal enquadrados, tais como "escalabilidade do sistema", anteriormente incluído no critério Segurança, e "viabilidade (custo/benefício)", anteriormente incluído no critério Acessibilidade, e que passaram a ser alvo de um tratamento independente.

2.1.3 Ponderação de cada sub-critério em cada critério

Depois de concluída a fase de explicitação e reorganização de sub-critérios, passou-se à fase de obtenção de ponderações para cada sub-critério associado a um determinado critério. Para obter essas ponderações recorreu-se à metodologia AHP, que se descreve sucintamente a seguir. As grelhas AHP foram preenchidas por cada avaliador, permitindo obter um vector de ponderações para cada critério/avaliador. O vector de ponderações final de cada critério foi obtido calculando a média dos vectores de todos os avaliadores.

Breve descrição da metodologia AHP

A metodologia AHP baseia-se na estruturação hierárquica de critérios e sub-critérios, de uma forma similar à utilizada pelo cérebro humano na estruturação do conhecimento.

A aplicação do AHP, exige que cada um dos critérios complexos seja subdividido num conjunto de sub-critérios não correlacionados e que descrevam totalmente o critério em causa. Relativamente a cada sub-critério, a metodologia AHP permite determinar as ponderações com que este contribui para o critério respectivo, com base em comparações entre pares de sub-critérios i e j (p_{ij}), seguindo a seguinte escala verbal:

$p_{ij} = p_{ji} = 1$ se sub-critérios i e j têm igual importância;
$p_{ij} = 2$ ou $p_{ji} = 1/2$ situação intermédia;
$p_{ij} = 3$ ou $p_{ji} = 1/3$ se sub-critério i é moderadamente mais importante do que sub-critério j;
$p_{ij} = 4$ ou $p_{ji} = 1/4$ situação intermédia;
$p_{ij} = 5$ ou $p_{ji} = 1/5$ se sub-critério i é bastante mais importante do que sub-critério j;
$p_{ij} = 6$ ou $p_{ji} = 1/6$ situação intermédia;
$p_{ij} = 7$ ou $p_{ji} = 1/7$ se sub-critério i é muito mais importante do que sub-critério j;
$p_{ij} = 8$ ou $p_{ji} = 1/8$ situação intermédia;
$p_{ij} = 9$ ou $p_{ji} = 1/9$ se sub-critério i é extremamente mais importante do que sub-critério j.

Preenchimento das grelhas por cada avaliador

Para este processo de auditoria foram definidos 4 critérios, Acessibilidade, com 5 sub-critérios, Segurança, com 14 sub-critérios, Transparência, com 15 sub-critérios e Usabilidade, com 5 sub-critérios. Para cada um dos critérios foram criadas grelhas para

comparação de todos os pares de sub-critérios respectivos (ver Figura 2 a Figura 5), que foram preenchidas pelos avaliadores tendo em conta a escala verbal apresentada na secção anterior.

Acessibilidade	1 - conveniência	2 - direito de voto	3 - documentação para eleitor	4 - flexibilidade	5 - mobilidade
1 - conveniência	1,00				
2 - direito de voto		1,00			
3 - documentação para eleitor			1,00		
4 - flexibilidade				1,00	
5 - mobilidade					1,00

Figura 2 – Grelha para comparação de todos os pares de sub-critérios para o critério ACESSIBILIDADE.

Segurança	1 - auditabilidade	2 - autenticação do operador	3 - certificabilidade	4 - fiabilidade	5 - detectabilidade	6 - disponibilidade do sistema	7 - imunidade a ataques	8 - integridade dos votos	9 - invulnerabilidade	10 - rastreabilidade	11 - recuperabilidade	12 - tolerância a falhas	13 - isolamento	14 - segurança das comunicações
1 - auditabilidade	1,00													
2 - autenticação do operador		1,00												
3 - certificabilidade			1,00											
4 - fiabilidade				1,00										
5 - detectabilidade					1,00									
6 - disponibilidade do sistema						1,00								
7 - imunidade a ataques							1,00							
8 - integridade dos votos								1,00						
9 - invulnerabilidade									1,00					
10 - rastreabilidade										1,00				
11 - recuperabilidade											1,00			
12 - tolerância a falhas												1,00		
13 - isolamento													1,00	
14 - segurança das comunicações														1,00

Figura 3 – Grelha para comparação de todos os pares de sub-critérios para o critério SEGURANÇA.

Transparência	1 - anonimato	2 - atomicidade	3 - autenticidade (método de autenticação do	4 - confiabilidade	5 - documentação técnica	6 - integridade do pessoal	7 - integridade do sistema	8 - não-coercibilidade	9 - precisão do sve	10 - privacidade	11 - singularidade (não reutilização)	12 - transparência do processo	13 - transparência do sistema	14 - verificabilidade	15 - separação de papeis
1 - anonimato	1,00														
2 - atomicidade		1,00													
3 - autenticidade (método de autenticação do utilizador)			1,00												
4 - confiabilidade				1,00											
5 - documentação técnica					1,00										
6 - integridade do pessoal						1,00									
7 - integridade do sistema							1,00								
8 - não-coercibilidade								1,00							
9 - precisão do sve									1,00						
10 - privacidade										1,00					
11 - singularidade (não reutilização)											1,00				
12 - transparência do processo												1,00			
13 - transparência do sistema													1,00		
14 - verificabilidade														1,00	
15 - separação de papeis															1,00

Figura 4 – Grelha para comparação de todos os pares de sub-critérios para o critério TRANSPARÊNCIA

Usabilidade	1 - facilidade de uso	2 - rapidez de uso	3 - clareza da linguagem na interface	4 - localização da interface	5 - satisfação emocional
1 - facilidade de uso	1,00				
2 - rapidez de uso		1,00			
3 - clareza da linguagem na interface			1,00		
4 - localização da interface				1,00	
5 - satisfação emocional					1,00

Figura 5 – Grelha para comparação de todos os pares de sub-critérios para o critério USABILIDADE.

Agregação da informação

O tratamento dos dados recolhidos e a agregação da informação, feita com base na média das contribuições dos auditores, permitiu obter vectores de ponderações de sub-critérios para cada um dos 4 critérios. Esses vectores estão representados de seguida na Figura 6.

SEGURANCA (S)		100,00%
S1	Auditabilidade	10,29%
S2	Autenticação do Operador	4,43%
S3	Certificabilidade	9,02%
S4	Fiabilidade	9,77%
S5	Detectabilidade	4,59%
S6	Disponibilidade do Sistema	5,44%
S7	Imunidade a Ataques	8,13%
S8	Integridade dos Votos	14,39%
S9	Invulnerabilidade	9,28%
S10	Rastreabilidade	3,82%
S11	Recuperabilidade	5,30%
S12	Tolerância a Falhas	4,59%
S13	Isolamento	2,58%
S14	Segurança das comunicações	8,35%

TRANSPARÊNCIA (T)		100,00%
T1	Anonimato	11,25%
T2	Atomicidade	7,00%
T3	Autenticidade (método autenticação utilizador)	11,46%
T4	Confiabilidade	6,22%
T5	Documentação técnica	2,16%
T6	Integridade do Pessoal	2,83%
T7	Integridade do Sistema	5,96%
T8	Não-Coercibilidade	10,48%
T9	Precisão do SVE	7,61%
T10	Privacidade	7,57%
T11	Singularidade (Não Reutilização)	10,75%
T12	Transparência do Processo	3,46%
T13	Transparência do Sistema	3,93%
T14	Verificabilidade	6,46%
T15	Separação de papéis	2,87%

USABILIDADE (U)		100,00%
U1	Facilidade de uso	38,39%
U2	Rapidez de uso	10,06%
U3	Clareza da Linguagem na Interface	23,38%
U4	Localização da Interface	11,13%
U5	Satisfação emocional	17,04%

ACESSIBILIDADE (A)		100,00%
A1	Conveniência	14,42%
A2	Direito de Voto	46,96%
A3	Documentação para eleitor	7,63%
A4	Flexibilidade	11,86%
A5	Mobilidade	19,13%

Figura 6 – Vectores de ponderação de sub-critérios.

2.1.4 Observações relativamente aos sub-critérios

Durante a análise dos sub-critérios detectaram-se algumas correlações que deverão ser eliminadas em processos futuros de auditoria. A aplicabilidade da metodologia AHP exige por um lado que todos os sub-critérios associados a um critério sejam não correlacionados e por outro lado que caracterizem na totalidade esse critério.

2.2 Método de comparação dos sistemas de voto electrónico

A comparação dos sistemas de voto electrónico (SVE) é feita de forma tanto mais robusta quanto mais auditores os conhecerem e avaliarem. Nesse sentido foi construído um plano de visitas e reuniões, ver Figura 7, por forma a aumentar por um lado o número de auditores que conhecem cada sistema e também a aumentar o número de sistemas conhecidos por cada auditor.

	INDRA							UNISYS							MULTICERT				NOVABASE	UMIC CNE	Reunião ou Reuniões	Relatório
	Europeias 2004	Covilhã			Coração de Jesus			Europeias 2004	Santos o Velho			S. Seb. da Pedreira			Europeias 2004	Santa Iria			Internet	Apuramento		
		Abertura	Fecho	Visita	Abertura	Fecho	Visita		Abertura	Fecho	Visita	Abertura	Fecho	Visita		Abertura	Fecho	Visita				
SRC		x													o				x		Novabase, Multicert	Novabase
JMC			x					o											x			Indra
MJL					x										o			x			Indra	Indra (rel.)
HN						x												x				Indra
JCL	o						x		x												Indra	Unisys
MG							x			x					o						Multicert	Multicert
ACB												x			o			x			Novabase, Unisys	Unisys
APM	o												x					x				Unisys (rel.)
JPF	o						x										x				Multicert	Multicert (rel.)
RMV											x					x					Multicert	Multicert
GTD								o								x			x		Novabase, Unisys	Novabase (rel.)
LMS																x			x			Novabase
IVV								o			x								x		Novabase, Unisys	Novabase
JFC							x				x			x				x		x		Final (rel.)

Figura 7 – Plano de contactos e visitas dos auditores da FEUP.

O preenchimento das grelhas de avaliação dos SVE foi feito por todos os avaliadores em conjunto. A análise foi feita sub-critério a sub-critério, para todos os SVE. Para cada sub-critério foram apresentadas, negociadas e finalmente atribuídas as classificações dos SVE (ver secção 3.2.4).

			Tipo de SVE					
			SVE					
SEGURANÇA (S)		100,00%	**2,94**					
S1	**Auditabilidade**	10,29%	x					1
S2	**Autenticação do Operador**	4,43%		x				2
S3	**Certificabilidade**	9,02%			x			3
S4	**Fiabilidade**	9,77%				x		4
S5	**Detectabilidade**	4,59%					x	5
S6	**Disponibilidade do Sistema**	5,44%			x			3
S7	**Imunidade a Ataques**	8,13%			x			3
S8	**Integridade dos Votos**	14,39%			x			3
S9	**Invulnerabilidade**	9,28%			x			3
S10	**Rastreabilidade**	3,82%			x			3
S11	**Recuperabilidade**	5,30%			x			3
S12	**Tolerância a Falhas**	4,59%			x			3
S13	**Isolamento**	2,58%			x			3
S14	**Segurança das comunicações**	8,35%			x			3
TRANSPARÊNCIA (T)		100,00%	**2,81**					
T1	**Anonimato**	11,25%	x					1
T2	**Atomicidade**	7,00%		x				2
T3	**Autenticidade** (método autenticação utilizador)	11,46%			x			3
T4	**Confiabilidade**	6,22%				x		4
T5	**Documentação técnica**	2,16%					x	5
T6	**Integridade do Pessoal**	2,83%			x			3
T7	**Integridade do Sistema**	5,96%			x			3
T8	**Não-Coercibilidade**	10,48%			x			3
T9	**Precisão do SVE**	7,61%			x			3
T10	**Privacidade**	7,57%			x			3
T11	**Singularidade (Não Reutilização)**	10,75%			x			3
T12	**Transparência do Processo**	3,46%			x			3
T13	**Transparência do Sistema**	3,93%			x			3
T14	**Verificabilidade**	6,46%			x			3
T15	**Separação de papéis**	2,87%			x			3
USABILIDADE (U)		100,00%	**2,58**					
U1	**Facilidade de uso**	38,39%	x					1
U2	**Rapidez de uso**	10,06%		x				2
U3	**Clareza da Linguagem na Interface**	23,38%			x			3
U4	**Localização da Interface**	11,13%				x		4
U5	**Satisfação emocional**	17,04%					x	5
ACESSIBILIDADE (A)		100,00%	**2,74**					
A1	**Conveniência**	14,42%	x					1
A2	**Direito de Voto**	46,96%		x				2
A3	**Documentação para eleitor**	7,63%			x			3
A4	**Flexibilidade**	11,86%				x		4
A5	**Mobilidade**	19,13%					x	5
A6	**Viabilidade (Custo/Beneficio)**							x
S15	**Escalabilidade do Sistema**					x		4

Figura 8 – Exemplo de atribuição de classificações a um SVE nos sub-critérios definidos

O cálculo do produto interno entre as classificações de um SVE, representadas para um caso fictício na Figura 8, e as ponderações obtidas pelo AHP, permitirá por fim obter

uma classificação para cada par SVE/Critério (ver secção 3.4 para os vários sistemas auditados).

2.3 Observação geral

Como se pode verificar ao longo da apresentação da metodologia, todo o processo foi aplicado aos 2 sistemas de voto presencial da INDRA e da UNISYS, ao sistema de voto presencial com mobilidade da MULTICERT e também ao sistema de voto não presencial pela Internet apresentado pela NOVABASE. É no entanto claro para todos os auditores da equipa que os três tipos de sistemas não são directa e globalmente comparáveis, porque as condições de utilização são diferentes e porque os sistemas que pretendem substituir também são diferentes. Optou-se, no entanto, por avaliar todos os sistemas em conjunto, para aumentar a troca de opiniões.

3 Apreciação dos sistemas de voto electrónico

3.1 Resultados do inquérito aos eleitores

De acordo com os resultados do inquérito realizado aos eleitores após o voto electrónico, [UMIC 2004b], a experiência obteve um grau de satisfação notável e de abertura a um processo eleitoral real com meios electrónicos.

Os resultados obtidos nas mesas de voto que a equipa da FEUP auditou, também estão muito próximos dos obtidos na votação tradicional, embora este resultado não tenha qualquer significado estatístico.

Do ponto de vista de apreciação final, referem-se em seguida os principais resultados do inquérito realizado [OSIC 2005] (p. 4) aos eleitores que aceitaram participar na experiência piloto do voto electrónico presencial:

- *99,2% dos eleitores que participaram no projecto-piloto e responderam ao inquérito gostaram da experiência de voto electrónico presencial e 98,1% revelam-se dispostos a votar electronicamente em futuros actos eleitorais;*
- *Os eleitores que votaram electronicamente consideram que o sistema é Rápido (98,2), Simples/Fácil (97,8%) e que facilita a identificação dos candidatos (90,2%);*
- *63% consideram que o novo sistema de voto Facilita o acto de voto dos cidadãos com dificuldades visuais/motoras;*
- *80,5% dos eleitores inquiridos confia na Segurança do sistema. Os eleitores que declaram não considerar o sistema seguro (3%), classificam sobretudo a garantia de Inalterabilidade do Voto (31,7%) e de Anonimato (30,1%) como sendo "pouco seguras";*
- *84,5% dos eleitores que votaram electronicamente numa máquina com registo do voto em papel, consideraram importante que o seu voto tenha sido impresso e automaticamente inserido na urna;*
- *86,3% dos eleitores inquiridos consideram que a implementação desta nova forma de votar, a permitir a mobilidade do votante contribuirá para a diminuição da abstenção eleitoral;*
- *Na possibilidade de recurso a tecnologias alternativas que permitam o voto à distância, 62,4% das preferências dos eleitores inquiridos recai sobre o voto pela Internet, seguindo-se o voto através da rede ATM (54,2%). O voto por SMS (42,9%) e por Telefone (42,4%) surgem no fim da lista das preferências, sendo cerca de metade dos eleitores inquiridos pouco receptivos a estas duas tecnologias;*
- *Quanto mais elevado é o nível de escolaridade (concluído) dos eleitores inquiridos maior é a sua receptividade à introdução do voto por Internet e através da rede ATM;*
- *A discordância relativamente ao recurso à Internet e à rede ATM reside, em particular, nos indivíduos do escalão etário mais elevado e nos que possuem níveis de escolaridade mais baixos para os quais o voto por telefone (com auxílio do teclado) é o que reúne maior número de preferências. Para 41,3% dos indivíduos com 65 ou mais anos, 51,3% dos que não sabem*

ler/escrever e 47,1% dos que não concluíram o 1.º Ciclo do Ensino básico, esta é a alternativa mais viável para o seu possível exercício de voto à distância.

Do ponto de vista dos eleitores recenseados no estrangeiro que exerceram o seu direito de voto pela Internet obteve-se a seguinte apreciação [UMIC 2005]:

- *99,2% dos eleitores que participaram no projecto-piloto gostaram da experiência de voto electrónico pela Internet e 98,3% revelam-se dispostos a votar desta forma em futuros actos eleitorais;*
- *Os eleitores que votaram consideram que o sistema é Rápido (98,9%), Simples/Fácil (98,1%).*
- *57,8% dos eleitores inquiridos considera esta forma de votar Segura, 7,9% considera que não é Segura e 34,3 não sabem ou não respondem.*
- *Relativamente ao nível de segurança do sistema de voto pela Internet apenas 1,7% dos eleitores o classificam como totalmente seguro no que respeita à sua resistência a ataques de piratas informáticos, enquanto 54,3% não sabe ou não responde.*
- *90,8% dos eleitores que participaram no projecto-piloto dispõem de ligação à Internet em casa, e 81,7% encontrava-se em casa quando votou.*
- *73,3 dos eleitores inquiridos consideram que a implementação desta nova forma de votar contribuirá para a diminuição da abstenção eleitoral da comunidade portuguesa residente no estrangeiro.*

É de realçar que estes resultados abrangem unicamente a opinião dos eleitores que votaram de facto electronicamente. Não foram recolhidas opiniões dos eleitores que apenas votaram pela forma tradicional.

3.2 Descrição dos sistemas utilizados

Os sistemas de voto electrónico da UNISYS, INDRA, MULTICERT e NOVABASE bem como a respectiva caracterização face aos requisitos de segurança, transparência, usabilidade e acessibilidade, são apresentados em detalhe nos relatórios de auditoria a cada um dos sistemas[3].

De acordo com as informações prestadas pelas empresas, e pelo que foi dado observar aos auditores da FEUP, apresenta-se de seguida uma descrição muito sucinta de como cada um dos sistemas opera.

Do ponto de vista de organização podemos considerar que em todos os casos havia dois sistemas em operação:

[3] Juntamente com o presente relatório seguem as versões finais dos relatórios de auditoria a cada um dos sistemas (UNISYS: [FEUP 2005a], INDRA: [FEUP 2005b], MULTICERT: [FEUP 2005c] e NOVABASE: [FEUP 2005d]).

- **Sistema de Gestão do Caderno Eleitoral** (SGCE), dando as permissões para acesso ao voto e contabilizando quem ia votando. **Em todas as assembleias de voto tratava-se de um sistema desenvolvido pela empresa MULTICERT**. Na freguesia de Santa Iria de Azóia a versão do sistema era diferente da versão em todos os outros locais, para permitir a gestão da mobilidade de eleitores. Na freguesia de Coração de Jesus o SGCE não funcionou, pelo que a gestão do caderno eleitoral foi realizada da forma tradicional.

- **Sistema de Voto Electrónico** (SVE) propriamente dito, onde o eleitor escolhia o partido em que iria votar (ou em que podia também escolher votar em branco ou mesmo não votar) e que permitia apurar localmente os resultados da votação no encerramento das urnas. Após o SGCE aceitar o eleitor, era-lhe entregue um dispositivo electrónico (em substituição do tradicional boletim de voto em papel) que permitia usar o equipamento de votação. No monitor deste equipamento aparecia o boletim de voto com as opções possíveis. Após confirmar a opção de voto desejada, o eleitor retirava o dispositivo electrónico e regressava à mesa onde o devolvia, terminando assim o processo. Cada um dos SVE apresentava alternativas neste processo. No caso da INDRA e da UNISYS o voto era contabilizado no equipamento de votação, mas no caso da MULTICERT o voto era também transportado com o dispositivo e transferido para uma urna electrónica na mesa. No final do dia e após o fecho da votação, no caso da INDRA cada equipamento transmite o total de votos ao centro de contagem por linha telefónica analógica. No caso da UNISYS há no final da eleição uma recolha de votos de cada equipamento de votação para um sistema central na assembleia que de seguida transmite os totais para o centro de contagem de votos por linha telefónica analógica (no caso da freguesia de S. Sebastião da Pedreira não foi possível estabelecer a comunicação de dados). No caso da MULTICERT o sistema da assembleia de voto encerra contando os totais e haveria uma ligação segura pela Internet a um servidor onde seriam registadas as contagens locais (mas tal não sucedeu).

3.2.1 Sistema de Voto Electrónico da UNYSIS

Os postos de votação da Unisys são unidades autónomas, dotadas de um ecrã táctil em que estes apresentam uma orientação ligeiramente inclinada relativamente à horizontal, para evitar reflexos. Além disso, fazem parte destas unidades palas de protecção laterais, posterior e superior, que garantem uma total privacidade no momento da votação. A montagem dos postos não necessita de qualquer material adicional, dispondo de suportes reguláveis em altura. Na Figura 9 pode ver-se o seu aspecto exterior e na Figura 11 o seu aspecto interior. Um dos postos estava equipado com auscultadores destinando-se o seu uso aos eleitores com necessidades especiais. Estava disponível

apenas para demonstração um sistema com uma impressora para registo de votos em papel.

Figura 9 – Postos de votação do sistema representado pela Unisys

Adicionalmente aos postos de votação existe um outro dispositivo (computador) operado pela mesa, e também com uma interface táctil, que tem como principal função preparar as "chaves de votação pessoal" (*Personal Electronic Ballots* – PEBs) que autorizam a votação nos postos (ver Figura 10). Estas chaves devem ser transportadas pelos eleitores até um dos postos, e após inserção na ranhura própria aí existente, desencadeiam a visualização dos ecrãs de votação. Após uma utilização, cada PEB necessita de ser regenerado no computador da mesa já referido, para que possa ser novamente utilizado por um novo eleitor (Figura 11). É a posse destes PEB, devidamente preparados e validados na mesa, que garante a autorização de votação do eleitor e que este só efectua uma única votação.

Os ecrãs de votação permitem a escolha da preferência do eleitor e a sua correcção no caso de engano, usando o ecrã táctil. A sessão termina, validando a escolha final do eleitor, quando este pressiona um botão físico, marcado com a palavra "VOTE", e existente na parte superior do equipamento. Durante todo este processo um PEB válido terá de estar inserido na ranhura correspondente, à esquerda do ecrã. A contagem dos votos assim concluídos vai sendo acumulada no posto de votação e armazenada de forma redundante. Na Figura 12 pode observar-se o interior de um posto de votação, onde se vê um cartaz com a indicação que é clara do local de colocação do PEB que permite a votação.

Se um eleitor retirar o seu PEB prematuramente antes de concluir toda a sessão com o pressionar do botão "VOTE", o posto deveria ficar inoperacional até à intervenção de um operador munido de PEB especial (o PEB de supervisão)[4]. Este PEB permite efectuar outras operações privilegiadas que não a votação, apresentadas num menu. Entre essas operações está a que permite validar a última opção do eleitor anterior (que não havia concluído a votação) ou invalidá-la.

Figura 10 – Chave ou PEB de supervisão. O PEB de votação tem aspecto idênticomas com outra cor.

Figura 11 – Regeneração de um PEB no computador de supervisão na mesa.

Após a conclusão do período de votação todos os postos deverão ser encerrados. Essa operação de encerramento necessita do PEB de supervisão. Cada posto que vai sendo encerrado transfere os totais de votos aí acumulados para a memória do PEB de supervisão que os vai totalizando. Quando todos os postos estiverem encerrados, usando o mesmo PEB de supervisão, este conterá os totais de todos os postos.

[4] Na realidade observou-se que a inserção do mesmo PEB que foi retirado prematuramente, depois de devidamente regenerado, permitia a continuação da sessão de votação interrompida.

Figura 12 – Interior dos postos de votação com a indicação do local de inserção do PEB

Faltará então apenas a impressão e transmissão destes resultados para um computador da autoridade eleitoral. Novamente colocando o PEB de supervisão, já com os dados recolhidos no encerramento dos postos de votação, num outro computador dotado de impressora e modem, será impressa uma acta indicando os totais apurados por posto e os totais gerais. A partir de uma ligação à rede telefónica e utilizando o modem incluído os resultados poderão ser transmitidos para um outro computador totalizador, geralmente pertencente à autoridade eleitoral.

Figura 13 – Contagem de votos na UMIC.

3.2.2 Sistema de Voto Electrónico da INDRA

Arquitectura do SVE

O SVE da Indra objecto de auditoria é constituído pelos seguintes elementos utilizados na secção de voto:

- Postos de Votação Electrónica (PVE): equipamento isolado especialmente desenhado para o efeito, baseado numa plataforma PC - Windows NT, leitor de cartões electrónicos (*smart cards*, ver Figura 14) e ecrã táctil (Figura 15), equipado com protecções que tornavam difícil a sua visualização sem ser pela pessoa que estivesse na sua frente. Um dos postos estava equipado com auscultadores e rato, destinando-se o seu uso aos eleitores com necessidades especiais. Um outro dispunha de uma impressora colocada sobre uma urna de recolha de votos impressos (Figura 16), os quais poderiam ser visualizados pelo eleitor, mas não retirados da impressora.
- *Smart cards* para os votantes: conjunto de cartões *smart card* fornecidos igualmente pela empresa INDRA, usados para a votação (em substituição dos boletins de voto). Os cartões disponibilizados encontravam-se já prontos a usar (uma única vez cada cartão) nos postos de votação.
- *Smart cards* para os administradores dos postos de votação: cartões usados pela mesa para o arranque e encerramento dos postos de votação.

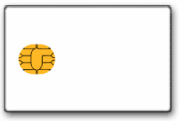

Figura 14 – *Smart card* sem qualquer desenho.

Figura 15 – Postos de Votação Electrónica

Figura 16 – Postos de Votação Electrónica com impressora

No final da votação, cada PVE imprime um relatório com o resultado da eleição, sendo ligado directamente a uma linha telefónica analógica, para transmissão dos resultados para um centro de apuramento, neste caso localizado na UMIC.

Procedimentos do SVE

Para a abertura da mesa e dos postos de votação, o presidente da Mesa da Secção de Voto, apoiado por técnicos da INDRA, efectua a inicialização dos postos de votação utilizando, para o efeito, uma chave normal que permite o acesso físico ao equipamento, um *smart card* de administração e o conhecimento de um código de administração de 8 dígitos (PIN do cartão) que dá acesso ao Menu de Administração. Através dele

imprime-se um relatório em papel que apresenta o estado da máquina (nomeadamente a contagem de votos a zero) e, não havendo irregularidades, a máquina é colocada em funcionamento normal ficando pronta a aceitar votos.

O computador que dá acesso ao Caderno Eleitoral é iniciado por um procedimento semelhante, utilizando também para autenticação os três cartões electrónicos (*smart card*) previamente distribuídos aos três membros da mesa. O processo de votação consiste:

- na verificação da inscrição do eleitor nos cadernos eleitorais em formato electrónico;
- na entrega ao eleitor de um cartão electrónico (*smart card* de voto), ainda não utilizado durante o acto eleitoral;
- na votação propriamente dita, em que o eleitor se dirige a um PVE livre e segue as indicações apresentadas no ecrã:
    - pedido de introdução do *smart card* numa ranhura da máquina;
    - pedido de escolha de um dos partidos apresentados no ecrã (boletim de voto electrónico), ou de "voto em branco", o que é efectuado tocando o ecrã com um dedo no item escolhido, ou no quadrado correspondente, no qual irá surgir a marca da votação (um X);
    - pedido de confirmação da opção escolhida;
    - mensagem de "votação concluída" e pedido de remoção do cartão que, após efectuada, origina a emissão de um breve sinal sonoro.

É de notar que o eleitor pode alterar a sua escolha de voto até ao momento em que confirma a votação. É também de salientar, que o eleitor pode em qualquer momento desistir de votar, apenas por remoção do *smart card* da ranhura onde estava semi-inserido. Neste caso, aparecia uma mensagem no ecrã indicadora do facto de a votação não estar concluída.

O processo de votação continua:

- com a devolução à Mesa do cartão de voto utilizado (e electronicamente marcado, por forma a não poder servir novamente na eleição) e com a recuperação dos documentos de identificação do eleitor;
- com a colocação, por um elemento da Mesa, do cartão de voto usado numa caixa separada da que continha os cartões novos;
- com a indicação no caderno eleitoral electrónico, por outro elemento da Mesa, de que o eleitor exerceu o seu direito de voto.

No final do acto eleitoral, mediante um sistema de autenticação idêntico ao utilizado na abertura da Mesa, o caderno eleitoral electrónico é encerrado, um registo de encerramento é produzido (contendo, nomeadamente, o número de votantes assinalados), uma cópia dos registos é salvaguardada em disquete e toda a aplicação de manuseamento do caderno eleitoral, assim como o próprio Caderno, é eliminada do disco do computador.

Em cada um dos PVE, o presidente da mesa ou um seu representante, de forma autenticada idêntica à efectuada na abertura, obtém das máquinas os registos de votação, faz a ligação a uma linha telefónica analógica e transmite os resultados à central de apuramento, procedendo de seguida ao encerramento do posto. Todos os registos em papel são assinados pela Mesa e juntos aos produzidos na abertura e à acta do decurso global da votação na Secção de Voto em questão.

Nos PVE que têm acoplados uma impressora que regista em papel o voto dos eleitores (por forma a que eles pudessem efectuar uma última constatação da sua votação), procede-se no final do acto eleitoral à contagem dos votos em papel assim produzidos, por forma a verificar se coincidem com os registados electronicamente. Os resultados desta operação são também lançados na Acta elaborada pela Mesa.

Figura 17 – Local na UMIC para contagem de votos.

3.2.3 Sistema de Voto Electrónico da MULTICERT

Sistema de Gestão do Caderno Eleitoral

Para suportar a mobilidade dos eleitores na experiência de voto electrónico entre os 7 locais de voto na freguesia de Santa Iria de Azóia, a empresa MULTICERT disponibilizou um Sistema de Gestão do Caderno Eleitoral (SGCE) em arquitectura cliente-servidor, baseado num servidor central onde residia a base de dados do caderno eleitoral (contendo a lista dos eleitores recenseados e a indicação dos eleitores que já votaram), ao qual acediam por UMTS ou ADSL as aplicações clientes localizadas nas várias Mesas de Voto (Figura 18).

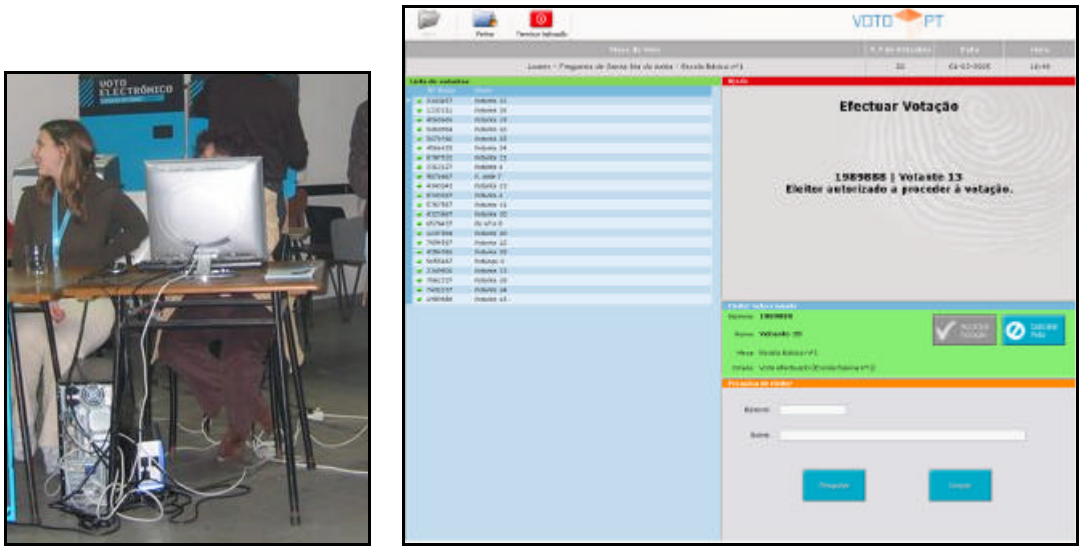

Figura 18 – Imagens de um sistema cliente do caderno eleitoral electrónica (à esquerda) e da aplicação cliente que executa no sistema cliente (à direita).

Sistema de Voto Electrónico propriamente dito

No caso do SVE da MULTICERT, o dispositivo electrónico entregue ao eleitor para permitir a utilização dos equipamentos de votação era um *i-button* (Figura 19). Em cada local de voto existiam cerca de 6 a 8 *i-buttons* reutilizáveis.

Figura 19 – Dispositivo *i-button*.

Os equipamentos de votação (também designados cabines de voto electrónico) eram sistemas comuns equipados com ecrã táctil, leitor de *i-buttons* e impressora com depósito vedado (Figura 20). Depois de obter da mesa um *i-button* contendo uma

autorização de voto, o eleitor devia dirigir-se a uma cabine livre e inserir o *i-button* no leitor respectivo, sendo-lhe então apresentado um boletim com as opções de voto. Depois do eleitor seleccionar e confirmar a sua opção de voto no ecrã táctil, esta era gravada no *i-button* e era impresso um talão comprovativo que o eleitor podia visualizar por breves momentos mas não retirar. No entanto, o voto (em formato electrónico) não ficava gravado na própria cabine.

Para concluir o seu processo de votação, o eleitor devia dirigir-se de novo à mesa, onde devia descarregar o seu voto para uma urna electrónica, encostando o *i-button* ao leitor respectivo (Figura 21). O sistema da urna electrónica era um computador de secretária comum (não visível na figura), equipado com um monitor (não visível na figura) e um leitor de *i-buttons*, sendo este colocado junto à ranhura de uma urna de forma tradicional (visível na figura), para tornar mais evidente a sua função. Quando um voto era descarregado na urna electrónica, o *i-button* era imediatamente regenerado (limpo e carregado com uma nova autorização de voto), ficando pronto a seu usado por outro eleitor.

Figura 20 – Cabina de voto com dispositivo de leitura e escrita para o *i-button* e uma impressora protegida à sua direita.

Figura 21 – Urna electrónica com leitor de *i-buttons* (não se vê o computador a que o mesmo está ligado).

Após o encerramento da urna electrónica em cada local de votação, os resultados ficavam imediatamente disponíveis localmente no monitor respectivo, mas não foram transmitidos para um centro de apuramento.

A Multicert, em parceria com a PT Inovação, desenvolveu também um protótipo de um sistema de votação por telemóvel, pensado para eleitores com necessidades especiais. A cada eleitor interessado em votar por esta via era fornecido um envelope fechado contendo um PIN de 4 dígitos (código de votação), depois de identificar e autorizar o eleitor no SGCE da mesma forma que os restantes eleitores. Ligando para um número de telefone previamente definido, e indicando este PIN, estabelecia-se um diálogo que permitia ao eleitor efectuar a sua votação.

3.2.4 Sistema de Voto Electrónico da NOVABASE

O SVE pela Internet desenvolvido pela empresa Novabase destinou-se a suportar a votação electrónica dos círculos de emigrantes, Europa e Fora da Europa. Por essa razão, a fonte de inspiração e a referência para comparações com a metodologia em vigor é o voto por correspondência.

O processo de voto

O processo seguido pelo SVE pela Internet consiste nas seguintes etapas:

1. Geração de credenciais individuais de acesso ao SVE.
2. Registo dos cadernos eleitorais.
3. Envio das credenciais ao eleitor.
4. Geração das chaves de encriptação.
5. Abertura da votação.

6. Preenchimento do boletim.
7. Registo do voto e descarga no caderno eleitoral.
8. Fecho da votação.
9. Apuramento dos resultados dos círculos internacionais.

Descrevem-se em seguida os aspectos essenciais de cada uma destas etapas.

1. Geração de credenciais individuais de acesso ao SVE

Os Cadernos Eleitorais são enviados pelo STAPE, através da UMIC, à Novabase, em formato electrónico. O SVE executa o programa de Geração de Credenciais. Este lê os Cadernos Eleitorais e produz e imprime, para cada eleitor, uma credencial, um código único de 12 caracteres, correspondendo a um nome de utilizador de 6 caracteres e a uma senha de outros 6 caracteres.

2. Registo dos cadernos eleitorais

A informação de cada eleitor é registada com a respectiva credencial no sistema central, no *Active Directory*. O *Active Directory* vai funcionar como caderno eleitoral, durante a votação. A BD nesse sistema é também preparada com uma tabela contendo todas as credenciais emitidas, pelo que pode ser vista como uma segunda versão simplificada do Caderno Eleitoral, e uma tabela por círculo eleitoral, para registar os votos que vierem a ser recebidos.

3. Envio das credenciais ao eleitor

As credenciais são entregues à empresa que irá enviar a correspondência (empresa de *mailing*), através da UMIC, juntamente com o nome e a morada do eleitor, para o respectivo envio, em conjunto com informação sobre o processo de votação, em particular o URL do sítio do SVE. Da informação entregue à empresa não faz parte o número de eleitor, impedindo que quem tenha acesso a esta informação possa realizar votos indevidamente.

4. Geração das chaves de encriptação

Existe uma operação de geração de um par de chaves de encriptação, sendo a chave pública entregue à Novabase para a colocar na BD. A chave privada é dividida em sete partes, as quais são gravadas em CD, uma para cada partido representado na CNE e uma para a CNPD (ver Figura 22). Desta forma, garante-se que os votos só podem ser desencriptados com a anuência das sete partes envolvidas.

Figura 22 – As caixas representadas contêm os CD com as 7 partes da chave privada de encriptação. O CD à vista tem uma cópia da base de dados com os votos encriptados.

5. Abertura da votação

A abertura da votação consiste em activar o SVE e permitir os acessos dos navegadores da Internet ao URL do sítio do SVE (no caso das eleições legislativas de 2005, baseado num sistema instalado na própria NOVABASE).

6. Preenchimento do boletim

Para votar, o eleitor que recebeu a credencial por correio indica ao navegador Web que estiver a utilizar o URL do Voto Electrónico/Info e, após seguir as ligações "Voto electrónico não presencial" e "Área de Votação", chega ao formulário de autenticação, onde lhe é solicitado o código na credencial e o Número de Eleitor. No caso de ambos estarem correctos e de a informação no *Active Directory* do SVE sobre o eleitor indicar que este ainda não votou, é-lhe apresentado o formulário do boletim de voto correspondente ao círculo em que se encontra recenseado, segundo o *Active Directory*. O eleitor pode então escolher uma e uma só opção no boletim, isto é, um dos concorrentes ou a opção de voto em branco e enviar o formulário. Em seguida, aparece um ecrã onde se pede para confirmar que a opção escolhida é a pretendida. Após esta confirmação, que corresponde a enviar o voto electrónico, o eleitor é convidado a responder a um inquérito sobre o projecto.

7. Registo do voto e descarga no caderno eleitoral

O voto confirmado e enviado ao servidor Web do SVE é codificado e registado numa das tabelas de votos da BD. Os votos são registados de forma encriptada, usando um sistema de chave dupla. A chave pública é usada para encriptar; a chave privada para desencriptar.

Na mesma transacção, regista-se que o eleitor já exerceu o seu direito de voto na tabela das credenciais e no registo do eleitor no *Active Directory*, após o que se notifica o eleitor do sucesso da operação.

8. Fecho da votação

No momento do encerramento do período de votação, o sítio de votação do SVE é desactivado e a informação de caderno eleitoral no *Active Directory* impressa, para envio à CNE. O *Active Directory* é então apagado, na presença de elementos da CNPD, para eliminar do SVE a informação de Caderno Eleitoral. É efectuada para CD uma cópia do conteúdo da BD, a qual é selada informaticamente com MD5 e entregue à UMIC.

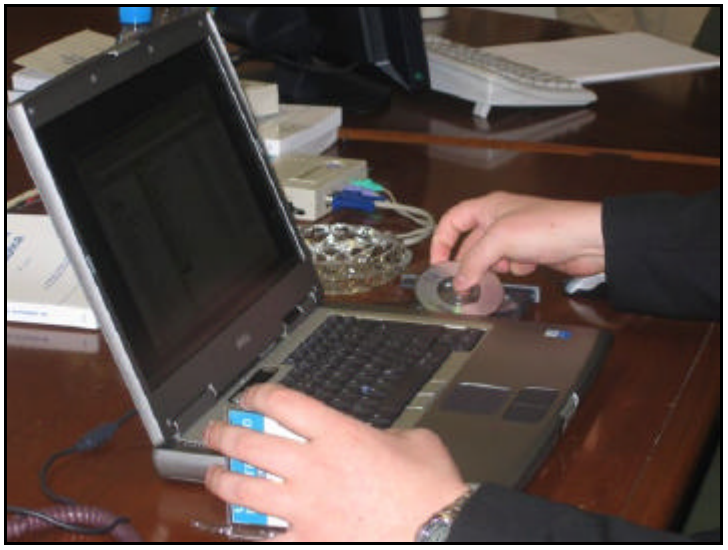

Figura 23 – CD com os votos a ser carregado para o PC que vai efectuar a contagem.

Figura 24 – Sala na CNE onde se realizou a contagem de votos.

9. Apuramento dos resultados dos círculos internacionais

O apuramento dos resultados é efectuado com um programa de contagem de votos. Como os votos estão encriptados, é necessário reunir as sete partes em que foi dividida a chave privada. Numa primeira fase, o conteúdo do CD com a cópia da informação da votação é carregado na BD (ver Figura 23). Na fase seguinte, o programa de contagem desencripta os votos, usando a chave reconstruída, e produz a contagem (ver exemplo na Figura 25).

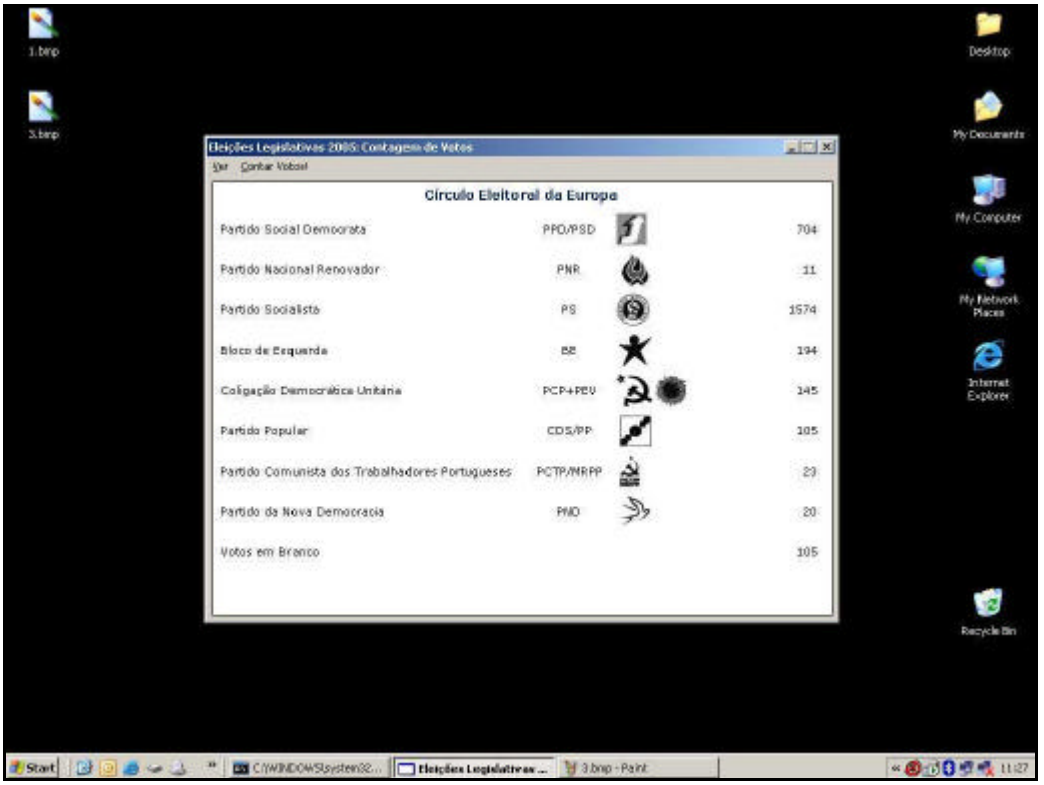

Figura 25 – Resultado da contagem de votos pela Internet no círculo eleitoral da Europa.

Arquitectura do SVE

O SVE adopta a arquitectura cliente servidor habitual nos sistemas que utilizam o serviço www da Internet. Do ponto de vista lógico existem um sítio Web de Voto Electrónico (URL: http://www.votoelectronico.pt) e Eleitores, distribuídos na Internet.

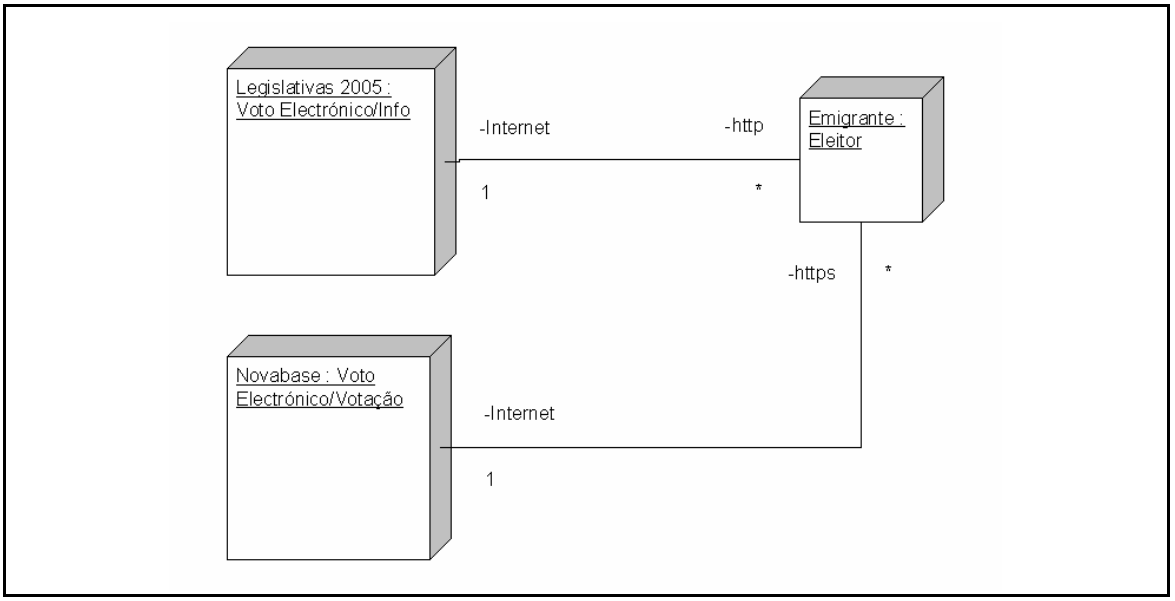

Figura 26 – Arquitectura do SVE da Novabase.

Do ponto de vista técnico, os Eleitores recorrem a um vulgar navegador Web que interprete HTML e algum JavaScript e que aceite *cookies*. O Eleitor pode executar o navegador Web em qualquer máquina com acesso à Internet.

O sítio Web está repartido por dois nós. O primeiro, aqui designado por Voto Electrónico/Info, está sob a responsabilidade da UMIC e é acessível por uma ligação http; responde no URL http://www.votoelectronico.pt/ publicitado aos eleitores e contém informação sobre o projecto e os seus objectivos, o modo de votar e esclarecimento de dúvidas; redirecciona para o segundo nó na ligação "Área de Votação".

O segundo nó, Voto Electrónico/Votação, está sob a responsabilidade da Novabase, instalado na sua infra-estrutura das Amoreiras e é acessível por uma ligação segura https. Responde no URL http://voto.votoelectronico.pt/ e contém os formulários correspondentes ao processo de votação, os cadernos eleitorais e regista os votos.

A arquitectura interna deste nó contém dois sub-nós, um *Frontend* para os servidores Web e um *Backend* para as bases de dados. Cada sub-nó corresponde a uma máquina real, na qual foram definidas várias máquinas virtuais.

Todo o software foi desenvolvido em plataformas Microsoft, em ambiente .Net, sendo as linguagens de programação utilizadas C# e HTML com JavaScript.

3.3 Resumo de vantagens e desvantagens dos vários tipos de sistemas

De seguida resumem-se os aspectos mais e menos positivos de cada uma das abordagens ao voto electrónico que foram objecto de ensaio nas eleições legislativas de 20 de Fevereiro. Referem-se também as oportunidades e ameaças a cada alternativa. Este resumo aplica-se a qualquer sistema do tipo mencionado. Na secção seguinte referem-se as vantagens e desvantagens específicas a cada um dos sistemas utilizados.

3.3.1 Sistemas de voto electrónico presencial

Nesta categoria estão incluídas as versões dos SVE utilizados pela UNISYS e pela INDRA. Ambas as empresas afirmaram que podiam ter disponibilizado sistemas para permitir graus de mobilidade do eleitor, mas tal não aconteceu nas eleições pois não estava nos requisitos definidos.

Pontos Fortes

- Satisfação dos eleitores.
- Contagem rápida e fiável.

- Possibilidade de registo do voto em papel.
- Voto branco explícito e voto nulo inexistente.

Pontos Fracos

- Informação técnica detalhada não disponibilizada.
- O desconhecimento da relação custo-benefício actual para a realização de uma eleição nacional vinculativa.

Oportunidades

- Acessibilidade.
- Difusão da sociedade digital.

Ameaças

- Dependência de empresas informáticas externas ao actual processo eleitoral. Esta ameaça pode ser compensada com procedimentos fiáveis de auditoria e certificação.
- Procedimentos, usabilidade e deficiências técnicas podem provocar discrepância entre número de votantes e votos contados.

3.3.2 Sistemas de voto electrónico presencial com mobilidade

Nesta categoria está incluída a versão do SVE em desenvolvimento MULTICERT com o apoio da PT Inovação. O sistema demonstrado permitia a um eleitor votar em qualquer assembleia de voto da freguesia de Santa Iria de Azóia.

Pontos Fortes

- Satisfação dos eleitores.
- Mobilidade dos eleitores.
- Contagem rápida e fiável.
- Voto branco explícito e voto nulo inexistente.

Pontos Fracos

- O desconhecimento da relação custo-benefício actual para a realização de uma eleição nacional vinculativa.
- Dificuldades com a possibilidade de registo do voto em papel para eleitores que votem em assembleias de voto distintas das da sua origem. Em eleições com boletins de voto diferentes de local para local, a existência de um único eleitor em mobilidade podia permitir identificar qual a sua opção de voto no registo em papel.

Oportunidades

- Acessibilidade.
- Difusão da sociedade digital.

Ameaças

- Informação técnica detalhada não disponibilizada.
- Dependência de empresas informáticas externas ao actual processo eleitoral.
- Procedimentos, usabilidade e deficiências técnicas podem provocar discrepância entre número de votantes e votos contados.

3.3.3 Sistemas de voto electrónico não presencial pela Internet

Nesta categoria está incluída a versão do SVE em desenvolvimento pela NOVABASE. O sistema demonstrado permitia a um eleitor recenseado na Europa ou no Resto do Mundo votar pela Internet.

Pontos Fortes

- Mobilidade.
- Satisfação dos eleitores.
- Contagem rápida.
- Voto branco explícito e voto nulo inexistente.

Pontos Fracos

- Impossível impressão em papel de cada voto para verificação final.
- Impossível garantir não coercibilidade (tal como no voto por correspondência).

Oportunidades

- Acessibilidade, maior participação, conveniência.
- Se o voto por correspondência viesse a ser totalmente substituído por esta forma de votar, seria possível encerrar o processo de votação dos círculos de emigração no mesmo momento que a votação nacional, e determinar a composição total da assembleia de imediato.

Ameaças

- Acesso desigual dos votantes à Internet, devido a aspectos sociais e económicos (incluindo a iliteracia informática).
- Falta de percepção de confiança no processo baseado na Internet.
- Possibilidades variadas de ataques à segurança.

3.4 Resumo de vantagens e desvantagens dos vários sistemas

De seguida resumem-se as vantagens e desvantagens específicas a cada um dos sistemas utilizados. Os relatórios de auditoria específicos a cada um dos sistemas apresentam uma análise muito mais completa.

É também de salientar que os SVE da UNISYS e da INDRA são produtos comerciais com experiência passada de utilização em eleições noutros países.

O SVE da MULTICERT foi desenvolvido especificamente para a presente eleição sob requisitos definidos pela UMIC em relação à possibilidade de mobilidade do eleitor. Resultou da evolução de um sistema anterior testado nas eleições para o Parlamento Europeu de 2004. Este SVE recorreu a uma infra-estrutura variada de telecomunicações para manter o acesso de um caderno eleitoral centralizado. A MULTICERT também disponibilizou o Sistema de Gestão do Caderno Eleitoral para todas as assembleias de voto, em duas versões.

O SVE da NOVABASE foi igualmente desenvolvido especificamente para a presente eleição, sob requisitos definidos pela UMIC e CNPD.

Nas secções seguintes apresentam-se os vários sistemas, incluindo as classificações atribuídas a cada um deles nos vários sub-critérios pela equipa de auditoria. Incluem-se também explicações sobre os melhores e piores resultados obtidos.

3.4.1 Sistema de Gestão do Caderno Eleitoral da MULTICERT (utilizado em todas as experiências piloto presenciais)

Como já foi referido, a principal vantagem deste sistema é o de vir a permitir a disponibilização futura dos cadernos eleitorais de uma forma integrada para todos as assembleias eleitorais.

A principal desvantagem é o facto de, devido a ser um sistema novo, desenvolvido em muito pouco tempo, não estar ainda devidamente documentado e testado.

Do ponto de vista de usabilidade o sistema também pode ser melhorado. De facto, relativamente à experiência de voto electrónico de 2004, foi constatado que foram introduzidas melhorias no sistema. Em particular na presente eleição foram utilizadas duas versões:

- Uma versão utilizada com os SVE da UNISYS e da INDRA; esta versão é idêntica à versão que foi usada nas eleições de 2004.

- Uma versão utilizada com o SVE da própria MULTICERT; esta versão permite a gestão da mobilidade do eleitor e assegura a comunicação com o caderno

eleitoral centralizado. Corresponde ainda a uma melhoria de filosofia significativa face à versão anterior utilizada nas Eleições Europeias [FEUP 2004d] que funcionava integrada no mesmo equipamento SVE que contava os votos expressos electronicamente. Nesta versão o sistema é autónomo do SVE não restando dúvidas sobre a separação do processo de voto do processo de identificação do eleitor[5].

[5] No entanto, para um suporte completo de mobilidade à escala nacional, não é possível manter uma separação completa, pois será necessário passar a identificação do círculo eleitoral de origem do eleitor do SGCE para o SVE propriamente dito.

3.4.2 Sistema de Voto Electrónico Presencial da UNISYS

			Unisys					
SEGURANÇA (S)		100,00%				**4,22**		
S1	**Auditabilidade**	10,29%			x			3
S2	**Autenticação do Operador**	4,43%					x	5
S3	**Certificabilidade**	9,02%				x		4
S4	**Fiabilidade**	9,77%			x			3
S5	**Detectabilidade**	4,59%					x	5
S6	**Disponibilidade do Sistema**	5,44%					x	5
S7	**Imunidade a Ataques**	8,13%				x		4
S8	**Integridade dos Votos**	14,39%					x	5
S9	**Invulnerabilidade**	9,28%					x	5
S10	**Rastreabilidade**	3,82%			x			3
S11	**Recuperabilidade**	5,30%					x	5
S12	**Tolerância a Falhas**	4,59%				x		4
S13	**Isolamento**	2,58%					x	5
S14	**Segurança das comunicações**	8,35%				x		4
TRANSPARÊNCIA (T)		100,00%				**4,22**		
T1	**Anonimato**	11,25%					x	5
T2	**Atomicidade**	7,00%		x				2
T3	**Autenticidade** (método autenticação utilizador)	11,46%					x	5
T4	**Confiabilidade**	6,22%					x	5
T5	**Documentação técnica**	2,16%			x			3
T6	**Integridade do Pessoal**	2,83%				x		4
T7	**Integridade do Sistema**	5,96%			x			3
T8	**Não-Coercibilidade**	10,48%					x	5
T9	**Precisão do SVE**	7,61%					x	5
T10	**Privacidade**	7,57%					x	5
T11	**Singularidade (Não Reutilização)**	10,75%				x		4
T12	**Transparência do Processo**	3,46%			x			3
T13	**Transparência do Sistema**	3,93%			x			3
T14	**Verificabilidade**	6,46%				x		4
T15	**Separação de papéis**	2,87%			x			3
USABILIDADE (U)		100,00%				**4,23**		
U1	**Facilidade de uso**	38,39%				x		4
U2	**Rapidez de uso**	10,06%				x		4
U3	**Clareza da Linguagem na Interface**	23,38%					x	5
U4	**Localização da Interface**	11,13%				x		4
U5	**Satisfação emocional**	17,04%				x		4
ACESSIBILIDADE (A)		100,00%				**3,69**		
A1	**Conveniência**	14,42%					x	5
A2	**Direito de Voto**	46,96%				x		4
A3	**Documentação para eleitor**	7,63%			x			3
A4	**Flexibilidade**	11,86%				x		4
A5	**Mobilidade**	19,13%		x				2
A6	**Viabilidade (Custo/Beneficio)**							x
S15	**Escalabilidade do Sistema**					x		4

Figura 27 – Avaliação do Sistema de Voto Electrónico da UNISYS

Como já foi referido, as principais vantagens deste sistema parecem ser a segurança, usabilidade e acessibilidade que lhe advêm de já ter sido utilizado em eleições

electrónicas vinculativas. Trata-se de um sistema estável, testado e certificado em outros países, com boas características de transparência.

O dispositivo electrónico (*Personal Electronic Ballot* – PEB) que o eleitor utiliza para aceder ao sistema de voto e o processo de voto associado, parece ser muito intuitivo e simples. É de salientar que a introdução de uma seta nesse dispositivo melhorou a sua usabilidade. A referida seta não existia no caso das eleições de 2004 [FEUP 2004e], o que provocava alguma confusão sobre o sentido de inserção do dispositivo no equipamento de voto.

A baixa pontuação em atomicidade deve-se à possibilidade de o eleitor levantar o PEB e aparentar votar electronicamente sem o fazer. Por si não é grave, pois tal facto pode ser considerado uma abstenção, mas a possibilidade de estas situações mascararem perturbações no sentido contrário é grave. Se por engano se entregar a um eleitor que já tenha votado um novo PEB (por exemplo, em dúvida se o eleitor votou de facto), permite-se que o número de votos contados seja superior ao que foi registado no caderno eleitoral, correspondente aos que se apresentaram para votar.

A baixa pontuação em mobilidade deve-se a não ter sido disponibilizado um sistema que o permitisse fazer. No entanto o sistema central que permite regenerar os PEB na mesa tornaria viável a mobilidade, permitindo a colocação no PEB de informação sobre a origem do eleitor.

Embora disponível para testes, não foi usado de forma integrada a impressão do voto em papel.

Não foram cedidas à equipa de auditoria as fontes dos programas utilizados pelo sistema da UNISYS.

3.4.3 Sistema de Voto Electrónico Presencial da INDRA

			Indra					
SEGURANÇA (S)		100,00%			**4,14**			
S1	**Auditabilidade**	10,29%			x			3
S2	**Autenticação do Operador**	4,43%					x	5
S3	**Certificabilidade**	9,02%				x		4
S4	**Fiabilidade**	9,77%			x			3
S5	**Detectabilidade**	4,59%				x		4
S6	**Disponibilidade do Sistema**	5,44%					x	5
S7	**Imunidade a Ataques**	8,13%			x			3
S8	**Integridade dos Votos**	14,39%					x	5
S9	**Invulnerabilidade**	9,28%					x	5
S10	**Rastreabilidade**	3,82%			x			3
S11	**Recuperabilidade**	5,30%					x	5
S12	**Tolerância a Falhas**	4,59%					x	5
S13	**Isolamento**	2,58%					x	5
S14	**Segurança das comunicações**	8,35%				x		4
TRANSPARÊNCIA (T)		100,00%			**4,32**			
T1	**Anonimato**	11,25%					x	5
T2	**Atomicidade**	7,00%		x				2
T3	**Autenticidade** (método autenticação utilizador)	11,46%					x	5
T4	**Confiabilidade**	6,22%					x	5
T5	**Documentação técnica**	2,16%			x			3
T6	**Integridade do Pessoal**	2,83%				x		4
T7	**Integridade do Sistema**	5,96%			x			3
T8	**Não-Coercibilidade**	10,48%					x	5
T9	**Precisão do SVE**	7,61%					x	5
T10	**Privacidade**	7,57%					x	5
T11	**Singularidade (Não Reutilização)**	10,75%				x		4
T12	**Transparência do Processo**	3,46%				x		4
T13	**Transparência do Sistema**	3,93%			x			3
T14	**Verificabilidade**	6,46%					x	5
T15	**Separação de papéis**	2,87%			x			3
USABILIDADE (U)		100,00%			**3,89**			
U1	**Facilidade de uso**	38,39%				x		4
U2	**Rapidez de uso**	10,06%				x		4
U3	**Clareza da Linguagem na Interface**	23,38%				x		4
U4	**Localização da Interface**	11,13%			x			3
U5	**Satisfação emocional**	17,04%				x		4
ACESSIBILIDADE (A)		100,00%			**3,35**			
A1	**Conveniência**	14,42%				x		4
A2	**Direito de Voto**	46,96%				x		4
A3	**Documentação para eleitor**	7,63%			x			3
A4	**Flexibilidade**	11,86%				x		4
A5	**Mobilidade**	19,13%	x					1
A6	**Viabilidade (Custo/Beneficio)**							x
S15	**Escalabilidade do Sistema**					x		4

Figura 28 – Avaliação do Sistema de Voto Electrónico da INDRA

Como já foi referido, a principal vantagem deste sistema parece ser a transparência que lhe advém de já ter sido utilizado em eleições electrónicas vinculativas. Trata-se de um

sistema estável, testado e certificado em outros países, com boas características de segurança, usabilidade e acessibilidade.

O sistema demonstrou a possibilidade de manter um registo anónimo em papel da votação realizada, permitindo em caso de dúvidas vir a recontar os votos por meios tradicionais.

O cartão electrónico (do tipo *smartcard*) que o eleitor utiliza para aceder ao sistema de voto e o processo de voto associado, cria algumas dificuldades a alguns eleitores. Ao contrário dos cartões bancários habituais, apenas se introduz parcialmente no equipamento de votação.

A baixa pontuação em atomicidade deve-se à possibilidade de o eleitor levantar o cartão electrónico e aparentar votar electronicamente sem o fazer. Por si não é grave, pois tal facto pode ser considerado uma abstenção, mas a possibilidade de estas situações mascararem perturbações no sentido contrário é grave. Se por engano se entregar a um eleitor que já tenha votado um novo cartão electrónico (por exemplo, em dúvida se o eleitor votou de facto), permite-se que o número de votos contados seja superior ao que foi registado no caderno eleitoral, correspondente aos que se apresentaram para votar.

A baixa pontuação em mobilidade deve-se a não ter sido disponibilizado um sistema que o permitisse fazer, e à arquitectura e processo apresentada não permitir suporte à mobilidade. No entanto, com um sistema em que cada eleitor tivesse o seu cartão electrónico pessoal previamente programado para o seu local de recenseamento, tal seria possível. Essa solução exigia uma norma nacional para os cartões de voto electrónico semelhante à que existiria para um cartão de identificação nacional electrónico.

Não foram cedidas à equipa de auditoria as fontes dos programas utilizados pelo sistema da INDRA.

3.4.4 Sistema de Voto Electrónico Presencial com Mobilidade da MULTICERT

			Multicert					
SEGURANÇA (S)		100,00%			**2,57**			
S1	**Auditabilidade**	10,29%			x			3
S2	**Autenticação do Operador**	4,43%				x		4
S3	**Certificabilidade**	9,02%			x			3
S4	**Fiabilidade**	9,77%		x				2
S5	**Detectabilidade**	4,59%			x			3
S6	**Disponibilidade do Sistema**	5,44%		x				2
S7	**Imunidade a Ataques**	8,13%				x		4
S8	**Integridade dos Votos**	14,39%		x				2
S9	**Invulnerabilidade**	9,28%		x				2
S10	**Rastreabilidade**	3,82%		x				2
S11	**Recuperabilidade**	5,30%		x				2
S12	**Tolerância a Falhas**	4,59%		x				2
S13	**Isolamento**	2,58%		x				2
S14	**Segurança das comunicações**	8,35%			x			3
TRANSPARÊNCIA (T)		100,00%			**3,15**			
T1	**Anonimato**	11,25%			x			3
T2	**Atomicidade**	7,00%	x					1
T3	**Autenticidade** (método autenticação utilizador)	11,46%					x	5
T4	**Confiabilidade**	6,22%		x				2
T5	**Documentação técnica**	2,16%	x					1
T6	**Integridade do Pessoal**	2,83%				x		4
T7	**Integridade do Sistema**	5,96%		x				2
T8	**Não-Coercibilidade**	10,48%					x	5
T9	**Precisão do SVE**	7,61%		x				2
T10	**Privacidade**	7,57%				x		4
T11	**Singularidade (Não Reutilização)**	10,75%		x				2
T12	**Transparência do Processo**	3,46%				x		4
T13	**Transparência do Sistema**	3,93%			x			3
T14	**Verificabilidade**	6,46%				x		4
T15	**Separação de papéis**	2,87%			x			3
USABILIDADE (U)		100,00%			**2,68**			
U1	**Facilidade de uso**	38,39%		x				2
U2	**Rapidez de uso**	10,06%			x			3
U3	**Clareza da Linguagem na Interface**	23,38%			x			3
U4	**Localização da Interface**	11,13%		x				2
U5	**Satisfação emocional**	17,04%				x		4
ACESSIBILIDADE (A)		100,00%			**3,50**			
A1	**Conveniência**	14,42%				x		4
A2	**Direito de Voto**	46,96%				x		4
A3	**Documentação para eleitor**	7,63%			x			3
A4	**Flexibilidade**	11,86%		x				2
A5	**Mobilidade**	19,13%			x			3
A6	**Viabilidade (Custo/Beneficio)**							x
S15	**Escalabilidade do Sistema**					x		4

Figura 29 – Avaliação do Sistema de Voto Electrónico da MULTICERT

Como já foi referido, a principal vantagem deste sistema em conjunto com o sistema MULTICERT para gestão do caderno eleitoral é a de vir a possibilitar que os eleitores votem em qualquer assembleia de voto. Além disso salienta-se a total disponibilidade da

empresa em prestar esclarecimentos à equipa da FEUP, com as vantagens que isso representa de audibilidade.

Sendo um sistema novo, desenvolvido em muito pouco tempo, não está ainda num estado de maturidade adequada sendo necessário resolver vários problemas tecnológicos e de processo.

Os procedimentos de segurança precisam de ser melhorados: não existem mecanismos apropriados de armazenamento redundante e recuperação de falhas no servidor do caderno eleitoral electrónico, o que é crítico num cenário de mobilidade à escala nacional; os votos são guardados nas urnas electrónicas de forma não cifrada nem assinada, o que pode permitir a contagem dos votos antes de terminado o período eleitoral (por não serem cifrados), e a alteração indevida dos votos (por não serem assinados); o sistema de impressões dos votos não é suficientemente fiável para permitir uma recontagem totalmente independente dos votos; não se verificou uma alta disponibilidade do sistema, devida não só a causas externas ao sistema (problemas de conectividade da rede UMTS), como a dificuldade de recuperação do sistema e no arranque de diversos equipamentos.

A usabilidade do dispositivo electrónico (*i-button*) para permitir ao eleitor aceder ao sistema de voto e transportar o voto para a urna electrónica parece ser complicada e originou vários problemas. Houve um número significativo de situações percepcionadas pelos eleitores e pela mesa como de erro e de dúvidas sobre se o processo de voto se tinha concluído com sucesso. A localização dos leitores de *i-button* foi feita de modo artesanal. Nas anteriores eleições de 2004 foi usado um cartão electrónico (do tipo *smartcard*), que também apresentava problemas [FEUP 2004d], em particular de tempo de leitura.

A muito baixa pontuação em atomicidade deve-se à possibilidade de o eleitor levantar o *i-button* e aparentar votar electronicamente sem o fazer. Por si não é grave, pois tal facto pode ser considerado uma abstenção, mas a possibilidade de estas situações mascararem perturbações no sentido contrário é grave. Se por engano se entregar a um eleitor que já tenha votado um novo *i-button* (por exemplo, em dúvida se o eleitor votou de facto), permite-se que o número de votos contados seja superior ao que foi registado no caderno eleitoral, correspondente aos que se apresentaram para votar. Nas eleições realizadas houve em geral bastante mais votos expressos do que eleitores que se apresentaram para votar.

A localização dos postos de voto e a facilidade com que qualquer pessoa conseguia ver o monitor do computador onde se realizava a votação, não permitia por vezes o anonimato do voto. Este problema é de fácil correcção e já tinha sido referido pela auditoria às anteriores eleições.

Embora a disponibilidade para prestar esclarecimentos tenha sido total, o sistema não tem documentação do ponto de vista técnico, ou esta não foi cedida à equipa de auditoria.

Não foram cedidas à equipa de auditoria as fontes dos programas utilizados pelos sistemas da MULTICERT.

3.4.5 Sistema de Voto Electrónico à Distância pela Internet da NOVABASE

			Novabase					
SEGURANÇA (S)		100,00%			**3,63**			
S1	**Auditabilidade**	10,29%				x		4
S2	**Autenticação do Operador**	4,43%					x	5
S3	**Certificabilidade**	9,02%			x			3
S4	**Fiabilidade**	9,77%			x			3
S5	**Detectabilidade**	4,59%		x				2
S6	**Disponibilidade do Sistema**	5,44%				x		4
S7	**Imunidade a Ataques**	8,13%			x			3
S8	**Integridade dos Votos**	14,39%				x		4
S9	**Invulnerabilidade**	9,28%				x		4
S10	**Rastreabilidade**	3,82%				x		4
S11	**Recuperabilidade**	5,30%				x		4
S12	**Tolerância a Falhas**	4,59%				x		4
S13	**Isolamento**	2,58%		x				2
S14	**Segurança das comunicações**	8,35%				x		4
TRANSPARÊNCIA (T)		100,00%			**3,03**			
T1	**Anonimato**	11,25%			x			3
T2	**Atomicidade**	7,00%					x	5
T3	**Autenticidade** (método autenticação utilizador)	11,46%	x					1
T4	**Confiabilidade**	6,22%				x		4
T5	**Documentação técnica**	2,16%	x					1
T6	**Integridade do Pessoal**	2,83%			x			3
T7	**Integridade do Sistema**	5,96%			x			3
T8	**Não-Coercibilidade**	10,48%	x					1
T9	**Precisão do SVE**	7,61%					x	5
T10	**Privacidade**	7,57%			x			3
T11	**Singularidade (Não Reutilização)**	10,75%					x	5
T12	**Transparência do Processo**	3,46%			x			3
T13	**Transparência do Sistema**	3,93%				x		4
T14	**Verificabilidade**	6,46%		x				2
T15	**Separação de papéis**	2,87%		x				2
USABILIDADE (U)		100,00%			**3,76**			
U1	**Facilidade de uso**	38,39%				x		4
U2	**Rapidez de uso**	10,06%					x	5
U3	**Clareza da Linguagem na Interface**	23,38%			x			3
U4	**Localização da Interface**	11,13%			x			3
U5	**Satisfação emocional**	17,04%				x		4
ACESSIBILIDADE (A)		100,00%			**3,63**			
A1	**Conveniência**	14,42%					x	5
A2	**Direito de Voto**	46,96%			x			3
A3	**Documentação para eleitor**	7,63%				x		4
A4	**Flexibilidade**	11,86%		x				2
A5	**Mobilidade**	19,13%					x	5
A6	**Viabilidade (Custo/Beneficio)**							x
S15	**Escalabilidade do Sistema**						x	5

Figura 30 – Avaliação do Sistema de Voto Electrónico da NOVABASE

A principal vantagem deste sistema é a de vir a possibilitar que os eleitores votem em qualquer local onde tenham acesso a um computador ligado à Internet. A conveniência

de tal situação seria sem dúvida grande. A NOVABASE disponibilizou um sistema funcional em muito pouco tempo e com usabilidade global muito positiva.

O sistema tem alguns problemas ao nível da garantia da autenticidade e anonimato, e a metodologia de operação do sistema que foi utilizada só é admissível para uma eleição não vinculativa. Por exemplo não seria possível ter os servidores Internet nas instalações da NOVABASE, que operou o sistema em todas as fases.

Do ponto de vista de segurança, os aspectos que mais preocupações levantam são a detectabilidade de eventuais tentativas de intrusão, a imunidade a ataques e o isolamento. Existe a necessidade de estudar melhor as questões de segurança na Internet, tentando prevenir a actuação de software malicioso nos clientes (por exemplo, com soluções que combinassem teclados virtuais com o https) e os ataques *man-in-the-middle*.

A baixa classificação em autenticidade é característica de qualquer sistema de voto não presencial. No entanto seria possível fazer melhor a este nível. A solução para a distribuição de credenciais e para a autenticação do eleitor deve ser revista no sentido de aumentar a autenticidade e de tornar mais transparente a garantia de anonimato.

O ficheiro resultante da exportação dos dados no fecho da votação deveria ter um formato aberto e neutro.

Embora a disponibilidade para prestar esclarecimentos tenha sido total, o sistema desenvolvido pela NOVABASE não tem documentação do ponto de vista técnico. O prazo de desenvolvimento curto não possibilitou a preparação desses elementos.

Os aspectos mais positivos incluem ainda a facilidade de autenticação dos operadores, a singularidade dos votos e o fornecimento sem reservas do código fonte do SVE com as vantagens que isso representa em termos de auditabilidade e certificabilidade.

3.4.6 Quadro de Avaliação dos 4 SVE

O quadro da Figura seguinte representa as grelhas de avaliação dos 4 sistemas usados. Tal como se referiu anteriormente, a comparação entre os três tipos de sistema não pode ser feita exclusivamente com base nesta informação. Por exemplo, qualquer sistema de voto pela Internet não permite garantir a não-coercibilidade: é sempre possível provar (mostrando) a outra pessoa em quem se votou. Num sistema que permita a mobilidade do eleitor não é simples, e pode não ser possível, efectuar a contagem de registos de voto em papel garantindo sempre o anonimato do voto. Por exemplo se num local de voto houver um único eleitor de uma dada freguesia de origem, o seu registo em papel terá de incluir uma referência a essa freguesia.

			SVE presencial										SVE presencial com mobilidade						SVE não presencial pela Internet					
			Unisys						Indra				Multicert						Novabase					
SEGURANÇA (S)		100,00%	**4,22**						**4,14**				**2,57**						**3,63**					
S1	**Auditabilidade**	10,29%			x			3			x			3			x			3				x		4
S2	**Autenticação do Operador**	4,43%					x	5					x	5					x	4					x	5
S3	**Certificabilidade**	9,02%				x		4				x		4				x		3			x			3
S4	**Fiabilidade**	9,77%			x			3			x			3			x			2			x			3
S5	**Detectabilidade**	4,59%					x	5					x	4				x		3		x				2
S6	**Disponibilidade do Sistema**	5,44%					x	5					x	5			x			2					x		4
S7	**Imunidade a Ataques**	8,13%				x		4				x		3					x	4				x		3
S8	**Integridade dos Votos**	14,39%					x	5					x	5			x			2					x		4
S9	**Invulnerabilidade**	9,28%					x	5					x	5			x			2					x		4
S10	**Rastreabilidade**	3,82%			x			3				x		3			x			2					x		4
S11	**Recuperabilidade**	5,30%					x	5					x	5			x			2					x		4
S12	**Tolerância a Falhas**	4,59%				x		4					x	5			x			2					x		4
S13	**Isolamento**	2,58%					x	5					x	5			x			2			x				2
S14	**Segurança das comunicações**	8,35%				x		4				x		4				x		3					x		4
TRANSPARÊNCIA (T)		100,00%	**4,22**						**4,32**				**3,15**						**3,03**					
T1	**Anonimato**	11,25%					x	5					x	5				x		3				x		3
T2	**Atomicidade**	7,00%		x				2			x			2		x				1					x	5
T3	**Autenticidade** (método autenticação utilizador)	11,46%					x	5					x	5					x	5		x				1
T4	**Confiabilidade**	6,22%					x	5					x	5			x			2					x		4
T5	**Documentação técnica**	2,16%			x			3				x		3			x			1			x			1
T6	**Integridade do Pessoal**	2,83%				x		4				x		4					x	4				x		3
T7	**Integridade do Sistema**	5,96%			x			3				x		3			x			2				x		3
T8	**Não-Coercibilidade**	10,48%					x	5					x	5					x	5		x				1
T9	**Precisão do SVE**	7,61%					x	5					x	5			x			2					x		5
T10	**Privacidade**	7,57%					x	5					x	5					x	4				x		3
T11	**Singularidade (Não Reutilização)**	10,75%				x		4				x		4			x			2					x		5
T12	**Transparência do Processo**	3,46%			x			3				x		4					x	4				x		3
T13	**Transparência do Sistema**	3,93%			x			3			x			3				x		3					x		4
T14	**Verificabilidade**	6,46%				x		4					x	5					x	4		x				2
T15	**Separação de papéis**	2,87%			x			3			x			3				x		3		x				2
USABILIDADE (U)		100,00%	**4,23**						**3,89**				**2,68**						**3,76**					
U1	**Facilidade de uso**	38,39%				x		4				x		4			x			2				x		4
U2	**Rapidez de uso**	10,06%				x		4				x		4				x		3					x	5
U3	**Clareza da Linguagem na Interface**	23,38%					x	5				x		4				x		3			x			3
U4	**Localização da Interface**	11,13%				x		4			x			3			x			2			x			3
U5	**Satisfação emocional**	17,04%				x		4				x		4					x	4				x		4
ACESSIBILIDADE(A)		100,00%	**3,69**						**3,35**				**3,50**						**3,63**					
A1	**Conveniência**	14,42%					x	5				x		4					x	4					x	5
A2	**Direito de Voto**	46,96%				x		4				x		4					x	4				x		3
A3	**Documentação para eleitor**	7,63%			x			3			x			3				x		3				x		4
A4	**Flexibilidade**	11,86%				x		4				x		4			x			2			x			2
A5	**Mobilidade**	19,13%		x				2		x				1				x		3					x	5
A6	**Viabilidade (Custo/Beneficio)**							x						x						x						x
S15	**Escalabilidade do Sistema**					x		4				x		4					x	4					x	5

Figura 31 – Resultados de Avaliação dos 4 SVE

Globalmente a apreciação da equipa da FEUP indica que o SVE da UNYSIS está bem classificado relativamente ao SVE da INDRA no aspecto da segurança, usabilidade e acessibilidade devido às seguintes razões, quase todas associadas ao PEB: é mais difícil de «falsificar» a sua utilização, por ser um dispositivo proprietário e pouco vulgar, mas ainda assim com uma utilização que parece ser mais simples para o eleitor do que a do cartão electrónico da INDRA. Os sistemas da INDRA requerem a sua instalação em mesas existentes nos locais de voto, o que parece menos apropriado do que no caso da UNISYS em que o equipamento já vem com a sua própria mesa regulável em altura. O SVE da INDRA parece melhor do ponto de vista de transparência devido à transparência do processo e à verificabilidade. Nestes aspectos a existência em funcionamento da impressão em papel do registo do voto foi determinante para a apreciação ser mais positiva do que a do SVE da UNISYS (que só mostrou um demonstrador desligado do processo).

Embora não esteja reflectido na pontuação atribuída, do ponto de vista de escalabilidade na contagem final de votos o sistema da UNISYS é melhor que o da INDRA. Cada assembleia de voto no caso da UNISYS transmite numa única chamada telefónica de dados todos os resultados, que foram entretanto recolhidos dos vários equipamentos, enquanto que no caso da INDRA cada equipamento na assembleia de voto efectua uma chamada telefónica de dados para transmitir os resultados.

A justificação global da apreciação do SVE da MULTICERT, em geral menos positiva comparativamente, tem a ver com os requisitos muito exigentes e variados que lhe foram colocados, comparativamente com os outros sistemas, que originam um sistema mais complexo (hardware e software) a conceber, desenvolver e implementar no dia das eleições, incluindo toda a logística de distribuição de equipamentos, treino e formação de operadores e técnicos. Tudo isto foi efectuado num prazo muito curto e o demonstrador funcionou bem globalmente em todos os aspectos, embora com problemas apontados que podem ser corrigidos, desde que sejam feitos os investimentos adequados.

A justificação global da apreciação do SVE da NOVABASE, comparativamente mais positiva nuns aspectos e menos em outros, resulta quer da complexidade relativamente mais baixa do sistema a conceber, desenvolver e implementar para as eleições (face aos da MULTICERT, INDRA e UNISYS), quer das características positivas e negativas do próprio meio e processo de votação pela Internet.

Também será justo afirmar que existe uma apreciação de nível excelente relativamente ao trabalho e empenho colocados por todos os técnicos das 4 empresas envolvidos no projecto (bem como das restantes pessoas envolvidas). Esta apreciação estará parcialmente traduzida nas grelhas, mas é relevante referir aqui pois não foi explicitamente avaliada.

4 Conclusões e recomendações

4.1 Conclusões

Globalmente a experiência piloto foi um grande sucesso do ponto de vista de adesão e satisfação dos eleitores, do funcionamento dos sistemas, e do conhecimento e experiência adicional que todos os agentes envolvidos obtiveram, tendo em vista a futura realização de eleições electrónicas vinculativas em Portugal.

Os sistemas da **INDRA** e da **UNISYS** têm filosofias de funcionamento semelhantes, embora recorram a tecnologias e processos diferentes. Trata-se de sistemas já testados e certificados internacionalmente com equipamentos concebidos com o único objectivo de serem utilizados em eleições. Uma vez assegurado um ambiente de utilização adequado, de quem gere a assembleia de voto e de informação prévia aos eleitores, estes sistemas já estão em condições de assegurar a realização de testes em eleições electrónicas vinculativas.

Considerando o estado actual de evolução desses dois sistemas, e do conhecimento presente na população de eleitores, será essencial garantir em eleições vinculativas uma adequada informação prévia aos eleitores, nomeadamente a possibilidade de experimentarem o sistema antes de votar. Será também essencial a preparação prévia das pessoas que gerem a assembleia de voto e a participação de técnicos com conhecimentos sobre os sistemas, para apoio a qualquer eventualidade.

Esta preparação prévia e apoio técnico são essenciais para garantir por exemplo que com os sistemas usados não se verifiquem discrepâncias sistemáticas entre a contagem de votantes, tal como registados no sistema de gestão do caderno eleitoral (electrónico ou em papel), e a contagem de votos expressos nos equipamentos de voto electrónico. Devido à forma como os sistemas actualmente garantem (ou não garantem) que o eleitor vota, e tornam esse facto óbvio para o eleitor e para as pessoas na mesa de voto, pode haver diferenças entre o número de votos expressos contados e o número de eleitores que exerceram o direito de voto. Para evitar o aparecimento de votos em excesso é importante uma grande atenção e disciplina dos elementos da assembleia de voto, no sentido de não autorizarem a mesma pessoa a repetir o voto. Não deveria haver dúvidas de ninguém sobre o exercício efectivo do voto nos equipamentos disponíveis. Melhorias nos sistemas e procedimentos, e maior conhecimento e experiência das pessoas envolvidas, permitem garantir tal problema não se verifique.

Os sistemas da **MULTICERT** foram desenvolvidos especificamente para as eleições legislativas de 20 Fevereiro de 2005, sob requisitos da UMIC. Tais desenvolvimentos

foram realizados num prazo muito curto e os sistemas resultantes assentam em computadores de uso corrente com software e periféricos específicos para o acto eleitoral. Os sistemas da MULTICERT que gerem o caderno eleitoral e o sistema de voto electrónico têm um grande potencial para vir a assegurar o voto em mobilidade, desde que sejam ultrapassados os problemas que foram detectados. Os problemas existentes nas versões usadas têm de ser resolvidos e novas versões melhoradas devem submeter-se de novo a testes não vinculativos satisfatórios.

É essencial uma versão melhorada do sistema de gestão de caderno eleitoral, baseada num melhor sistema de comunicações subjacente. O sistema de gestão de caderno eleitoral deve ser mais resistente a falhas de comunicação, e o sistema de comunicações deve ser mais fiável.

É também essencial um sistema de votação electrónica mais seguro, mais equilibrado do ponto de vista de transparência e mais fácil de usar. Em particular verificaram-se demasiados erros devido a dúvidas dos eleitores e das pessoas nas mesas de voto sobre a conclusão efectiva do voto. Esta dúvida permitiu que um número significativo de pessoas fosse autorizada a votar de novo, tendo-se verificado no final que houve mais votos do que votantes registados no caderno eleitoral.

O sistema de voto pela Internet da **NOVABASE** foi desenvolvido especificamente para as eleições legislativas de 20 Fevereiro de 2005, sob requisitos da UMIC. Tais desenvolvimentos foram realizados num prazo muito curto. Uma vez resolvidos alguns problemas existentes pode vir a ser uma alternativa real para o voto por correspondência. É essencial rever o processo de distribuição de credenciais e de autenticação do eleitor para aumentar a autenticidade e tornar mais transparente a garantia de anonimato. É também importante estudar melhor as questões de segurança na Internet, tentando prevenir a possibilidade de actuação de software malicioso nos clientes.

Dado o conhecimento actual dos eleitores recenseados no estrangeiro, a disponibilidade muito variável que têm de acessos à Internet fará com que a opção vinculativa de voto pela Internet só seja desejável como opção a par de outras. De facto os inquéritos realizados indicam que praticamente todos os eleitores que votaram pela Internet dispunham de um PC com acesso a partir de casa, o que não será ainda o caso para todos estes eleitores: 90,8% dos eleitores que participaram no projecto-piloto dispõem de ligação à Internet em casa, e 81,7% encontrava-se em casa quando votou.

Os meios de votação electrónica podem e devem contribuir para que os cidadãos confiem e participem nos actos eleitorais, e nessa medida estes sistemas devem ser aperfeiçoados, experimentados e utilizados. Estes novos sistemas têm ainda a vantagem

de vir a permitir aos cidadãos portadores de deficiências tornarem-se eleitores anónimos com maior autonomia.

A grande mais valia de um sistema de voto electrónico confiável parece também ser o de vir a permitir um processo de votação descentralizado e assim um maior conforto e satisfação, traduzidos talvez numa maior afluência de cidadãos aos actos eleitorais. A modernização do processo eleitoral parece essencial para tornar atractivas as eleições, em particular junto do cidadão eleitor mais jovem, cada vez mais habituado às novas tecnologias.

As novas tecnologias disponíveis na Sociedade de Informação podem contribuir para actos eleitorais mais rápidos, ou até mais frequentes, e mais confortáveis para todos, melhorando assim globalmente a produtividade e a satisfação emocional com as eleições.

Talvez o objectivo a longo prazo mais importante com a introdução dos sistemas de voto electrónico deve ser o de aumentar a participação política de todos os cidadãos. A evolução das tecnologias pode ser usada para envolver mais e melhor todas as pessoas nos processos de decisão mais relevantes, contribuindo assim para melhorar o governo democrático. Uma maior aproximação entre o eleitor e quem governa e decide pode ser usado para o aprofundamento da democracia.

Conclusões e recomendações mais específicas e detalhadas estão disponíveis nos relatórios de auditoria da FEUP a cada um dos sistemas (UNISYS: [FEUP 2005a], INDRA: [FEUP 2005b], MULTICERT: [FEUP 2005c] e NOVABASE: [FEUP 2005d]).

4.2 Recomendações

A equipa de auditoria da FEUP assume como prioritárias as seguintes três orientações para o desenvolvimento dos sistemas de voto electrónico, que deverão ser objecto de próximas experiências futuras:

- **Permitir aos eleitores o exercício do voto presencial em qualquer assembleia de voto**. Para tal é necessária a integração e disponibilização global de uma base de dados nacional de eleitores, e a possibilidade de, em qualquer assembleia de voto, ser apresentado ao eleitor o boletim de voto apropriado. Este último requisito é particularmente exigente no caso de eleições locais. Este objectivo de permitir a mobilidade pode ser atingido de forma faseada, disponibilizando

algumas assembleias de voto espalhadas pelo país onde tal seja possível ou permitindo aos eleitores que solicitem antecipadamente tal possibilidade.

- **Garantir a possibilidade de re-contagem dos votos de forma independente**, e de preferência por parte de não especialistas de informática, sempre que haja dúvidas sobre a correcção dos sistemas de voto electrónico ou para auditar uma amostra dos resultados obtidos por via electrónica nos sistemas em utilização.

- **Divulgar publicamente, com suficiente antecipação, todos os detalhes dos sistemas e processos em uso pelos sistemas de voto electrónico**, com preferência para os sistemas abertos e aplicações baseadas em sistemas abertos, não proprietários, e seguindo normas nacionais ou internacionais do domínio público.

No sentido de melhorar os sistemas e os processos de voto electrónico, a equipa de auditores da FEUP recomenda de forma mais específica o seguinte:

- Melhorar a informação sobre o processo de voto electrónico, permitindo por exemplo ao eleitor o acesso a um sistema de voto electrónico para teste ou para treino no local de voto, e antes de votar vinculativamente ou não.

- Manter a impressão do voto em papel, garantindo assim a possibilidade de verificação pelo eleitor de que a sua opção de voto é registada da forma tradicional e garantindo ainda a possibilidade de contagem final pela mesa de voto. No caso de se permitir o voto presencial em mobilidade esta opção afigura-se mais complicada. Numa fase de maior maturidade pode vir a ser dispensável esta garantia, mas para introdução de forma vinculativa do voto electrónico parece ser uma medida de aumentar a confiança.

- Melhorar os sistemas e processos para garantir uma melhor percepção pelo eleitor e pelos elementos da mesa de voto sobre a ocorrência do exercício efectivo do voto. Deve ser possível ao eleitor não votar, mas não deve haver a mínima dúvida quando de facto o eleitor votou.

- Definir procedimentos rigorosos para todas as fases do processo e melhorar o conhecimento e experiência dos elementos da mesa de voto sobre o sistema a utilizar, em particular sobre os procedimentos que permitam eliminar discrepâncias entre o número de votantes e de votos expressos (isto é, para se saber sem dúvida se um eleitor votou de facto).

- No caso do voto pela Internet, melhorar o processo de distribuição de credenciais e considerar alternativas à utilização do código de eleitor para

confirmar a sua identificação. Melhorar a informação para evitar software malicioso nos clientes.

- No caso do voto em mobilidade, para se permitir ao eleitor votar presencialmente em local diferente de onde está recenseado, considerar alternativas ao modelo do processo testado nestas eleições, para permitir a sua disponibilização a nível nacional de forma faseada, por exemplo recorrendo a um pedido prévio dos eleitores que optem por votar nessas condições[6].

- Aprofundar as soluções de apoio à acessibilidade, garantindo a inclusão de cidadãos com deficiências visuais ou com défice de literacia. No caso Internet, oferecer alternativas de acesso, por exemplo disponibilizando equipamentos em locais apropriados. Seria possível até para a eleição do Presidente da República o voto pela Internet presencial, em equipamentos disponíveis em mesas de voto.

Embora os processos de votação não presenciais, tais como as votações pela Internet, pelo telemóvel ou pelo Multibanco não garantam satisfatoriamente alguns dos requisitos enunciados, seria interessante continuar a efectuar experiências neste domínio para aferir da receptividade real junto dos eleitores e para comparar com os resultados obtidos por meios tradicionais. Os resultados dos inquéritos efectuados aos eleitores que participaram nas experiências piloto parecem indicar que, na Sociedade de Informação mais habituada às novas tecnologias e aos processos sociais de comunicação mediados por meios informáticos, tais processos possam vir a ser aceites com níveis de Confiança elevados.

Seria também relevante envolver os grupos existentes nos centros de investigação nacionais e estrangeiros, procurando incentivar o aparecimento e teste de propostas inovadoras. As possibilidades das novas tecnologias são imensas. Propostas inovadoras de formas de votar com elevada segurança, transparência, usabilidade e acessibilidade, podem até ser completadas com formas atractivas do ponto de vista emocional. Por exemplo seria interessante avaliar até que ponto a disponibilização de imagens de assembleias reais na Internet, com pessoas conhecidas a votar, de comunidades virtuais, ou de outras experiências virtuais, podia afectar a participação eleitoral.

A equipa de auditores da FEUP considera que é essencial e urgente definir objectivos concretos em relação ao voto electrónico, ao mais alto nível nacional dos vários poderes

[6] No caso da demonstração de viabilidade para voto em mobilidade seria necessário que uma experiência não vinculativa demonstrasse a possibilidade de um eleitor votar numa região do país diferente daquela onde está recenseado, em particular podendo usar o boletim de voto desse local. Seria interessante testar a disponibilização de alguns sistemas para experiência de voto em mobilidade, por exemplo nas regiões autónomas, e Porto, Lisboa e Faro.

legislativos e executivos, com um horizonte mínimo do final do próximo ciclo eleitoral completo, que se inicia com a próxima eleição para Presidente da República (ver Figura 32).

A definição de tais objectivos deve ser feita de forma inclusiva com as várias tendências políticas representadas na Assembleia da República. Os conhecimentos e as experiências já adquiridas a nível nacional pelas várias instituições e pessoas envolvidas nos testes realizados, deve ser aproveitada na definição desses objectivos, por forma a que as estratégias e acções a desenvolver para os atingir se possam concretizar com sucesso no horizonte estipulado. Um projecto com uma missão clara, gerido com sabedoria e apoio político, e com uma equipa experiente e empenhada será certamente essencial. Tal projecto deve envolver também a modernização de todos os processos necessários para a realização de consultas aos eleitores, que permita uma maior qualidade, flexibilidade e satisfação.

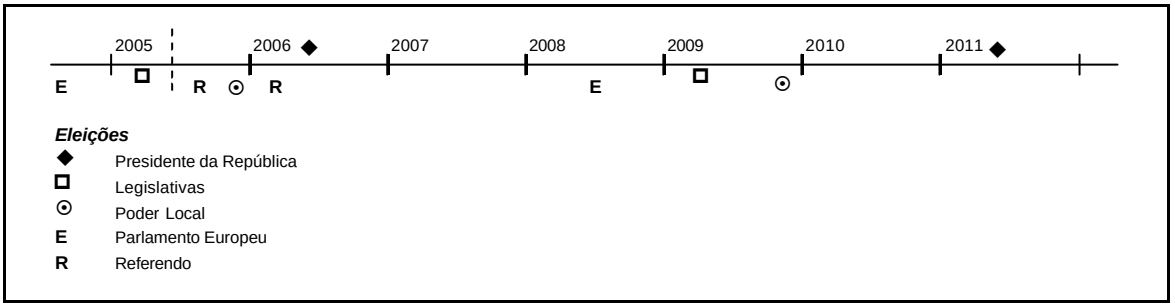

Figura 32 – Calendário de eleições e referendos em Portugal (aproximado)

Tal como se referiu no início deste relatório, o projecto deverá envolver a realização de uma análise de viabilidade das várias alternativas, incluindo os seus custos e benefícios. De facto, para se evoluir para um sistema global de voto electrónico há muitos cenários possíveis que podem ser considerados e que requerem um estudo adequado. Refere-se por exemplo que o sistema pode ou não ser exclusivo para eleições, com equipamentos que são reutilizados para outros fins depois das eleições. Mesmo sendo exclusivos para eleições, há muitas eleições onde se podem aplicar, nem todas de carácter nacional. Eventualmente os sistemas ou soluções podem até ter aplicações ao nível dos inquéritos que as empresas realizam aos seus clientes. Esta utilização seria até uma forma de tornar mais acessíveis os equipamentos, diminuindo a dificuldade com a sua operação em eleições. Também é relevante pensar se é possível e desejável aumentar o ritmo ou a profundidade das consultas públicas, mesmo que não vinculativas.

A disponibilidade para os processos de consulta pública de um sistema de voto electrónico flexível de elevada qualidade é sem dúvida um requisito relevante para a nossa sociedade em rápida evolução e para aproximar eleitores e governantes.

5 Referências e bibliografia

[ACM 2004] «Should computer-based electronic voting systems provide a physical record so voters can inspect permanent records of their ballots before they are cast and so meaningful recounts may be conducted?», Association for Computing Machinery, Member Opinion Poll, 2004-07-07 (https://campus.acm.org/polls/poll.cfm#position).

[Bederson & Herrnson 2004]: Ben Bederson, Paul Herrnson: «Expert Review Plan of Voting Machines», Research Report, Human-Computer Interaction Lab and Center for American Politics and Citizenship, University of Maryland, EUA, 2004.

[Braun 2004] Nadja Braun: «E-Voting: Switzerland's projects and their legal framework – in a European context», (http://www.e-voting.at/main.php?l=E 2005-04-23), [IWEVE 2004].

[Camp *et al* 2004] Jean Camp, Allan Friedman, Warigia Bowman (ed.): «Electronic Voting Best Practices - A Summary», Voting, Vote Capture & Vote Counting Symposium, Kennedy School of Government, Harvard University, 2004-06, 23 p.

[Canter 1997] Larry W. Canter: «Environmental Impact Assessment», McGraw-Hill, 2nd edition, 1997, p. 557-563.

[FEUP 2004a] João Falcão e Cunha (relator): «Voto Electrónico para um Portugal Moderno – Algumas Perguntas Preliminares», FEUP, 2004-05-31, 4 p.

[FEUP 2004b] João Falcão e Cunha (relator): «Voto Electrónico para um Portugal Moderno – Relatório Preliminar – Fase de Pré-Simulação». 2004-06-07, 14 p.

[FEUP 2004c] João Correia Lopes (relator), João Pascoal Faria, António Pimenta Monteiro: «Voto Electrónico para um Portugal Moderno – Relatório de Auditoria ao Sistema de Votação Electrónica – Fase de Simulação: Freguesia de Mangualde» (SVE MULTICERT-INDRA), Relatório Intercalar de Síntese 2004-06-21: 11 p, 2004-07-12: 20 p.

[FEUP 2004d] Mário Jorge Leitão (relator), Sérgio Reis Cunha, António Carvalho Brito, Miguel Gonçalves: «Voto Electrónico para um Portugal Moderno – Relatório de Auditoria ao Sistema de Votação Electrónica – Fase de Simulação: Freguesia de Paranhos» (SVE MULTICERT-MULTICERT), Relatório Intercalar de Síntese 2004-06-21, 9 p, 2004-07-26, 17 p.

[FEUP 2004e] Gabriel Torcato David (relator), José Magalhães Cruz, João Vila Verde: «Voto Electrónico para um Portugal Moderno – Relatório de Auditoria ao Sistema de Votação Electrónica – Fase de Simulação: Freguesia de S. Sebastião – Setúbal» (SVE MULTICERT-UNISYS), Relatório Intercalar de Síntese 2004-06-21, 13 p, 2004-07-27, 19 p.

[FEUP 2004f] J. Falcão e Cunha (relator): «Relatório Final de Auditoria – Fase de Pós-Simulação; Experiência piloto de voto electrónico decorrida nas Freguesias de Mangualde, Paranhos e São Sebastião nas Eleições para o Parlamento Europeu de 2004-06-13», Relatório apresentado à UMIC no âmbito do projecto «Voto Electrónico para um Portugal Moderno», 2004-08-04, FEUP, Porto, 28 p.

[FEUP 2005a] António Pimenta Monteiro (relator), António Carvalho Brito, Isidro Vila Verde, João Correia Lopes, Miguel Barbosa Gonçalves, Raul Moreira Vidal, Gabriel David: «Auditoria ao Projecto de Voto Electrónico, Eleições Legislativas de 2005-02-20, Relatório sobre o Sistema de Voto Electrónico Presencial da Empresa UNISYS » Relatório de Síntese 2005-04-15, 47 p.

[FEUP 2005b] Mário Jorge Leitão (relator), Maria Henriqueta Nóvoa, José Magalhães Cruz, João Correia Lopes, João Pascoal Faria, Miguel Barbosa Gonçalves, Sérgio Reis Cunha: «Auditoria ao Projecto de Voto Electrónico, Eleições Legislativas de 2005-02-20, Relatório sobre o Sistema de Voto Electrónico Presencial da Empresa INDRA», Relatório de Síntese 2005-04-15, 35 p.

[FEUP 2005c] João Pascoal Faria (relator), Raul Moreira Vidal, Miguel Barbosa Gonçalves, Gabriel David, Mário Jorge Leitão, António Carvalho Brito, Maria Henriqueta Nóvoa, António Pimenta Monteiro, Sérgio Reis Cunha: «Auditoria ao Projecto de Voto Electrónico, Eleições Legislativas de 2005-02-20, Relatório sobre o Sistema de Voto Electrónico Presencial com Mobilidade da Empresa MULTICERT», Relatório de Síntese 2005-04-15, 65 p.

[FEUP 2005d] Gabriel Torcato David (relator), Sérgio Reis Cunha, José Magalhães Cruz, Isidro Vila Verde: «Auditoria ao Projecto de Voto Electrónico, Eleições Legislativas de 2005-02-20, Relatório sobre o Sistema de Voto Electrónico Não Presencial pela Internet da Empresa NOVABASE», Relatório de Síntese 2005-04-15, 36 p.

[FEUP 2005e] João Falcão e Cunha (relator): «Auditoria ao Projecto de Voto Electrónico nas Eleições Legislativas de 2005-02-20», Apresentação pública de resultados preliminares da equipa de auditora da FEUP, UMIC, 2005-03-09, Hotel Corinthia Alfa, Lisboa, 22 p.

[FEUP 2005f] Maria Antónia Carravilla, José Fernando Oliveira: «Descrição da metodologia usada para comparação dos Sistemas de Voto Electrónico», Relatório Interno, FEUP, 2005-04-10, 9 p.

[Libbenga 2004] Jan Libbenga: «Dutch e-voting software goes open source», in *The Register* www.theregister.co.uk, published 2004-06-23. (http://www.theregister.co.uk/2004/06/23/open_source_voting_software/)

[Maidou & Polatoglou 2004] Anthoula Maidou, Hariton Polatoglou: «e-Voting and the Architecture of Virtual Space», 2004-07-12 (http://www.e-voting.at/main.php?t=8 2005-04-23) [IWEVE 2004].

[Mercuri 2000] Rebecca Mercuri «Generic Security Assessment Questions» (www.notablesoftware.com).

[IWEVE 2004] The International Workshop on Electronic Voting in Europe, Bregenz, Austria, 7-9.07.2004, (http://www.e-voting.at/main.php?ID=88, 2005-04-23).

[Monteiro *et al* 2001] Américo Monteiro, Natércia Soares, Rosa Maria Oliveira, Pedro Antunes, «Sistemas Electrónicos de Votação» (Relatório de trabalho orientado pelo Prof. Pedro Antunes), DI-FCUL TR–01–9, 2001, Departamento de Informática, Faculdade de Ciências da Universidade de Lisboa, Campo Grande, 1700 Lisboa, Portugal (http://www.di.fc.ul.pt/tech-reports).

[Neumann 1993] Peter G. Neumann: «Security Criteria for Electronic Voting», presented at the 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993 (http://www.csl.sri.com/users/neumann/ncs93.html).

[OSIC 2005] «Voto Electrónico - 2.ª Experiência Piloto de Voto Electrónico Presencial, Resultados», Resultados da análise dos inquéritos aos eleitores que exerceram o seu direito de voto e aceitaram participar na 2.ª experiência piloto do voto electrónico presencial nas Eleições Legislativas de 2005-02-20, OSIC – Observatório da Sociedade da Informação e Conhecimento, 2005-03, 22 p.

[OVSI 1999] Fundación OVSI: «Informe Experiência de Voto Electrónico: Elecciones a las Cortes Valencianas - Municipio de Villena», Fundación OVSI – Oficina Valenciana para la Sociedad de la Información, Alicante, 1999-06-25, 50 p.

[OVSI 2001] Fundación OVSI: «Informe de las Experiência de Voto Electrónico: Generalitat Valenciana 2001-11-06, Universidad de Valencia 2001-11-29», Fundación OVSI – Oficina Valenciana para la Sociedad de la Información, Alicante, 2001-12, 42 p.

[Pinto *et al* 2004] Rui Rocha Pinto, Filipe Simões, Pedro Antunes: «Estudo dos Requisitos para um Sistema de Votação Electrónica» (Relatório de trabalho orientado pelo Prof. Pedro Antunes), DI-FCUL TR–04–2, MARÇO 2004, Departamento de Informática, Faculdade de Ciências da Universidade de Lisboa, Campo Grande, 1700 Lisboa, Portugal (http://www.di.fc.ul.pt/tech-reports).

[Saaty 1980] T. L. Saaty: «The Analytic Hierarchy Process». McGraw-Hill, New York, 1980.

[Saaty 1987] T. L. Saaty: «The Analytic Hierarchy Process: what it is and how it is used», Mathematical Modelling, 9, 1987.

[Selker 2004] Ted Selker: «Fixing the Vote», Scientific American, 2004-09-17, p. 60-67.

[Thompson 1984] Ken Thompson: «Reflections on Trusting Trust», in *Communication of the ACM*, Vol. 27, No. 8, August 1984, p. 761-763.

[UMIC 2004a] «Voto Electrónico para um Portugal Moderno – Processo de Auditoria», Unidade de Missão Inovação e Conhecimento, Maio 2004, 5 p.

[UMIC 2004b] «Inquérito Voto Electrónico – Resultados», UMIC 2004-07-05, 9 p.

[UMIC 2005] «Voto Electrónico - 1.ª Experiência Piloto de Voto Electrónico Não Presencial, Resultados», Resultados da análise dos inquéritos aos eleitores recenseados no estrangeiro que exerceram o seu direito de voto pela Internet nas Eleições Legislativas de 2005-02-20, UMIC, 2005-03, www.votoelectronico.pt.

ANEXO A - Comissão de Auditoria da FEUP

Prof. Doutor João Falcão e Cunha – Coordenador

Doutorado em Engenharia Informática e Computação – Sistemas de Informação, pelo Imperial College London/FEUP, desenvolve actividades de docência e de investigação nas áreas de Sistemas de Informação, Bases de Dados, Interacção Pessoa Computador, Sistemas de Apoio à Decisão, Negócio e Governo Electrónico. A Interacção Pessoa Computador, o Negócio e o Governo Electrónicos constituem o rol de actuais interesses de investigação.

Prof. Doutor Mário Jorge Leitão

Doutorado em Comunicações por Satélite, pela Universidade de Bradford, Reino Unido. Agregação em Engenharia Electrotécnica pela Faculdade de Engenharia da Universidade do Porto. Professor Associado da FEUP onde desenvolve actividades de docência e investigação em Redes de Telecomunicações. Coordenador do Mestrado em Redes e Serviços de Comunicação. Director do INESC entre 1989 e 1995, Director do INESC Porto desde 1998.

Prof. Doutor António Carvalho Brito

Doutorado em Sistemas de Apoio à Decisão, lecciona e investiga actualmente nas áreas de Sistemas de Informação para Gestão, Simulação Visual Interactiva e Comércio Electrónico, que constituem os interesses mais recentes de investigação.

Prof. Doutor Sérgio Reis Cunha

Com o doutoramento em Engenharia Electrotécnica e de Computadores, desenvolve actividades de docência e de investigação nos seguintes domínios: Matemática, Sistemas, Controlo e Programação. A navegação, o controlo e a detecção remota têm composto as prioridades recentes de investigação. Esteve envolvido na concepção, instalação e gestão da rede informática da Faculdade de Engenharia da Universidade do Porto, tendo experiência, entre outras, na área da segurança informática. Foi membro de uma comissão eleitoral onde foi utilizado o sistema de voto electrónico.

Prof. Doutor João Correia Lopes

Com o doutoramento em Ciência de Computadores, desenvolve actividades de docência e de investigação nos seguintes domínios: Bases de Dados e Sistemas de Informação, Aplicações Web, Engenharia de Software e Programação. As Linguagens Persistentes

Ortogonais, a Tecnologia de Bases de Dados, a Orientação por Objectos, a Interoperabilidade e XML, e o Middleware têm composto as prioridades recentes de investigação.

Prof. Doutor Miguel Pimenta Monteiro

Doutorado em Engenharia Electrotécnica e Computadores pela FEUP, exerce actividade docente e de investigação no Departamento de Engenharia Electrotécnica e de Computadores da FEUP, nas áreas de Ciência da Computação, Sistemas Operativos e Distribuição e Integração. Pertence actualmente às Comissões Científicas da Licenciatura de Engenharia Informática e Computação e do Mestrado em Engenharia Informática da FEUP. Os seus interesses mais recentes de investigação, além das áreas genéricas já citadas incluem também e-learning, acesso remoto a serviços de computação intensiva sistemas de processamento e análise de imagem médica.

Prof. Doutor João Pascoal Faria

Doutorado em Engenharia Electrotécnica e de Computadores, pela FEUP, desenvolve actividades de docência, investigação e consultoria nas áreas de Engenharia de Software e Sistemas de Informação, com particular ênfase na integração de métodos formais de especificação e verificação de software com métodos semi-formais e com técnicas de desenvolvimento rápido de aplicações.

Prof. Doutor Gabriel David

Doutorado em Informática pela Universidade Nova de Lisboa, desenvolve actividades de docência e de investigação no Departamento de Engenharia Electrotécnica e Computadores, onde faz parte das comissões de coordenação da Licenciatura em Ciência da Informação e do Mestrado em Gestão de Informação, bem como dirige a equipa de desenvolvimento do SiFEUP (Sistema de Informação da FEUP). É investigador do INESC desde 1985, onde foi o responsável do projecto FCT MetaMedia sobre arquivos multimédia. As áreas de interesse mais recente são os Sistemas de Informação, as Bases de Dados e a Gestão de Informação.

Prof. Doutor José Magalhães Cruz

Doutorado em Engenharia Electrotécnica e de Computadores pela Faculdade de Engenharia da Universidade do Porto, onde é actualmente Professor Auxiliar. Tem leccionado disciplinas, a nível de Licenciatura e de Mestrado, nas áreas de Sistemas Operativos, Sistemas Distribuídos e Segurança Informática. Estas são também as áreas que cobrem os seus interesses actuais em termos de investigação.

Engenheiro João Isidro Vila Verde

Licenciado e Mestrado pela Faculdade de Engenharia da Universidade do Porto, desenvolve actividade de docência nos domínios de Segurança de Redes e Sistemas, Tecnologias XML, Web Services e Programação. É também Sócio Gerente da empresa Serprest, que desenvolve as actividades de desenvolvimento de software de gestão de parques informáticos e presta serviços de outsourcing na área de informática e comunicações. Foi durante 4 anos Director Técnico da Sonae Redes de Dados / Novis com responsabilidade, entre outras, pela área de segurança de redes, sistemas, aplicações e serviços. Entre 1989 e 1998 foi ainda Investigador do Inesc na área de redes, tendo participado em diversos projectos europeus (RACE, LACE, Atlantic, Binet) e nacionais (Atlantis).

Prof. Doutor Raul Moreira Vidal

Doutorado em Engenharia Electrotécnica e Computadores pela U. Manchester/UMIST/FEUP em 1979. Tem como interesses de investigação Sistemas de Informação e Engenharia de Software.

Prof.ª Doutora Henriqueta Nóvoa

Doutorada em Sistemas de Informação para Gestão, lecciona e investiga actualmente nas áreas de Estatística e Sistemas de Informação para Gestão, bem como de Negócio e Governo Electrónico, que constituem os interesses mais recentes de investigação.

Engenheiro Miguel Gonçalves

Licenciado em Engenharia Informática e Computação pela FEUP, esteve integrado no projecto ATLAS do CERN, na área de Sistemas de Informação. Os seus actuais interesses de investigação são Interacção Pessoa Computador, Sistemas de Informação e Segurança de Sistemas/Comunicações.

Prof.ª Doutora Maria Antónia Carravilla

Doutorada em Investigação Operacional e Planeamento da Produção (1996, FEUP), Mestre em Engenharia Electrotécnica e de Computadores, na área de controlo teórico, e Licenciada em Engenharia Electrotécnica, também na FEUP.

É actualmente Professora Auxiliar do Departamento de Engenharia Electrotécnica e de Computadores e Investigadora na Unidade de Sistemas de Produção do INESC-Porto. Em 2003 foi nomeada Pró-Directora da FEUP, responsável pelos Serviços Económico-Financeiros e está também envolvida em vários projectos ligados à gestão

central da FEUP. Nos últimos anos, os seus principais interesses de investigação são os Sistemas de Apoio à Decisão, Logística, re-engenharia de Processos Organizacionais e também Programação por Restrições na resolução de problemas de optimização combinatória

Prof. Doutor José Fernando Oliveira

Doutorado em Engenharia Electrotécnica e de Computadores, pela Faculdade de Engenharia da Universidade do Porto, desenvolve actividades de docência, investigação e consultadoria empresarial nas áreas da Investigação Operacional, Optimização e Apoio à Tomada de Decisão. As correntes áreas de interesse, do ponto de vista da aplicação dos Sistemas de Apoio à Decisão, são a Gestão e Optimização da Utilização de Recursos em Processos Industrias e o Apoio à Decisão na Gestão do Ensino Superior.

ANEXO B - Propriedades de um sistema de votação electrónica[7]

Anonimato

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).

Atomicidade

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)?

Auditabilidade

O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.

Autenticação do Operador

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.

Autenticidade (método de autenticação do utilizador)

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.

Certificabilidade

O sistema deve poder ser testado e certificado por agentes oficiais.

Confiabilidade

O SVE deve funcionar de forma fiável e robusta, tornando-se confiável aos olhos dos diversos actores envolvidos, em particular o eleitor.

[7] Adaptado de [Pinto *et al* 2004] e de [FEUP 2004f].

Conveniência

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.

Detectabilidade

O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.

Direito de Voto

O direito de voto deverá poder ser efectivamente exercido se um eleitor verificar simultaneamente as propriedades de Autenticidade e Singularidade.

Disponibilidade do Sistema

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.

Documentação para eleitor

O eleitor deve ter acesso com a antecedência adequada a informação de compreensão simples sobre o SVE e as suas características.

Documentação técnica

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.

Escalabilidade do Sistema

A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.

Fiabilidade

O SVE deve funcionar de forma fiável, sem perda de votos.

Flexibilidade

Os equipamentos de votação que fazem parte do SVE devem suportar uma variedade de questões relacionadas com o processo de votação, como por exemplo a utilização por pessoas com necessidades especiais, etc.

Imunidade a Ataques

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.

Integridade do Pessoal

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.

Integridade do Sistema

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.

Integridade dos Votos

Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.

Invulnerabilidade

A invulnerabilidade do SVE é a garantia de que não se pode aceder e alterar o sistema indevidamente.

Isolamento

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.

Mobilidade

O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.

Não-Coercibilidade

O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.

Precisão do SVE

O sistema deve garantir que todos votos são adequadamente registados e contabilizados.

Privacidade

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.

Rastreabilidade

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).

Recuperabilidade

O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.

Segurança das comunicações

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.

Separação de papéis

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.

Singularidade (Não Reutilização)

O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.

Tolerância a Falhas

Caso ocorra uma falha no sistema é possível recuperar o estado anterior e o funcionamento regular, assegurando um serviço aceitável.

Transparência do Processo

Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.

Transparência do Sistema

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.

Usabilidade

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.

Verificabilidade

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 p ropriedades como o anonimato ou a privacidade do votante.

Viabilidade (Custo/Beneficio)

O SVE deve ser eficiente e viável economicamente.

ANEXO C – Grelha para apoio à avaliação dos Requisitos de segurança, Transparência, Acessibilidade e Usabilidade

		-				+
SEGURANÇA (S)						
S	**Auditabilidade**					
	O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.					
S	**Autenticação do Operador**					
	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	**Certificabilidade**					
	O sistema deve poder ser testado e certificado por agentes oficiais.					
S	**Fiabilidade**					
	O SVE deve funcionar de forma fiável, sem perda de votos.					
S	**Detectabilidade**					
	O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.					
S	**Disponibilidade do Sistema**					
	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	**Imunidade a Ataques**					
	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	**Integridade dos Votos**					
	Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.					
S	**Invulnerabilidade**					
	A invulnerabilidade do SVE é a garantia de que não se pode aceder e alterar o sistema indevidamente.					
S	**Rastreabilidade**					
	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	**Recuperabilidade**					
	O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.					
S	**Tolerância a Falhas**					
	Caso ocorra uma falha no sistema é possível recuperar o estado anterior e o funcionamento regular, assegurando um serviço aceitável.					
S	**Isolamento**					
	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	**Segurança das comunicações**					
	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.					

		-				+
TRANSPARÊNCIA (T)						
T	**Anonimato**					
	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	**Atomicidade**					
	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	**Autenticidade (método de autenticação do utilizador)**					
	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	**Confiabilidade**					
	O SVE deve funcionar de forma fiável e robusta, tornando-se confiável aos olhos dos diversos actores envolvidos, em particular o eleitor.					
T	**Documentação técnica**					
	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	**Integridade do Pessoal**					
	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	**Integridade do Sistema**					
	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	**Não-Coercibilidade**					
	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	**Precisão do SVE**					
	O sistema deve garantir que todos votos são adequadamente registados e contabilizados.					
T	**Privacidade**					
	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	**Singularidade (Não Reutilização)**					
	O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.					
T	**Transparência do Processo**					
	Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.					
T	**Transparência do Sistema**					
	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	**Verificabilidade**					
	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	**Separação de papéis**					
	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.					

USABILIDADE (U)	-				+
U **Facilidade de uso**					
O sistema deve ser de uso fácil, quer para eleitores quer para operadores (membros da mesa de voto).					
U **Rapidez de uso**					
O sistema deve ser de uso rápido, quer para eleitores quer para operadores (membros da mesa de voto).					
U **Clareza da Linguagem na Interface**					
A interface do SVE (linguagem e 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.					
U **Localização da Interface**					
A localização, orientação e altura do monitor, bem como dos restantes dispositivos de interacção, devem ser apropriadas ao eleitor.					
U **Satisfação emocional**					
O sistema deve ser atraente e agradável de usar.					

ACESSIBILIDADE (A)	-				+
A **Conveniência**					
O sistema só será útil se permitir a todos os votantes exercerem o seu direito de voto de forma rápida, com o mínimo de equipamento, treino e sem necessidades específicas adicionais.					
A **Direito de Voto**					
O direito de voto deverá poder ser efectivamente exercido se um eleitor verificar simultaneamente as propriedades de Autenticidade e Singularidade.					
A **Documentação para eleitor**					
O eleitor deve ter acesso com a antecedência adequada a informação de compreensão simples sobre o SVE e as suas características.					
A **Flexibilidade**					
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, analfabetas, etc.					
A **Mobilidade**					
O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.					

Características transversais e outros aspectos (O)	-				+
O **Viabilidade (Custo/Beneficio)**					
O SVE deve ser eficiente e viável economicamente.					
	-				+
O **Escalabilidade do Sistema**					
A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.					