



Voto Electrónico e Defesa da Privacidade
Auditório da Assembleia da República 2005-12-07

A Segurança do Voto Electrónico

Problemas e Oportunidades

*João Falcão e Cunha **

jfcunha@fe.up.pt

91-254 1104

** Coordenador da equipa de auditoria da FEUP às experiências de Voto Electrónico não vinculativo*

Faculdade de Engenharia da Universidade do Porto



FEUP

Introdução

1. Experiência de Auditoria da FEUP
 - Objectivos, Equipa e Metodologia
2. Problemas do VE
 - Transparência do processo
 - Segurança do processo
 - Custo de criar, manter e gerir o processo de VE
3. Oportunidades do VE
 - Acessibilidade
 - Mobilidade
 - Satisfação e participação dos eleitores
4. Conclusões e Recomendações
 - Experiências de VE não vinculativo são necessárias e relevantes, e Experiências de VE vinculativo são essenciais.
 - Definir objectivos e plano de acções para um ciclo eleitoral.
 - Promover experiências de VE em outros actos eleitorais

1.

Experiência de Auditoria

Objectivos

- Auditar os sistemas de VE, tendo em conta requisitos de:
 - Segurança
 - Transparência
 - Usabilidade
 - Acessibilidade
- Comparar a eficiência e eficácia das diferentes tecnologias.
- Garantir uma avaliação independente e transparente das tecnologias utilizadas.
- Informar e orientar, do ponto de vista técnico, a acção política no domínio do VE, e impulsionar o debate nacional sobre as novas formas de participação electrónica em geral, e sobre o VE em particular.

Equipa de auditoria da FEUP

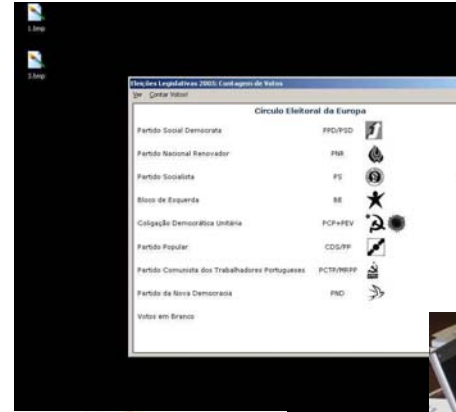
- Prof. Doutor João Falcão e Cunha - Sistemas de Informação
- Prof. Doutor **Mário Jorge Leitão** - Telecomunicações
- Prof. Doutor **Gabriel David** - Sistemas de Informação e Segurança
- Prof. Doutor **João Pascoal Faria** - Sistemas de Informação
- Prof. Doutor **António Pimenta Monteiro** - Informática
- 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
- Prof^a. Doutora Henriqueta Nóvoa - Sistemas de Informação
- Eng^o João Vila Verde - Telecomunicações
- Eng^o Miguel Gonçalves - Informática
- Eng^o Luís Miguel Silva - Informática e Segurança

Apoio à comparação e classificação dos vários sistemas de VE:

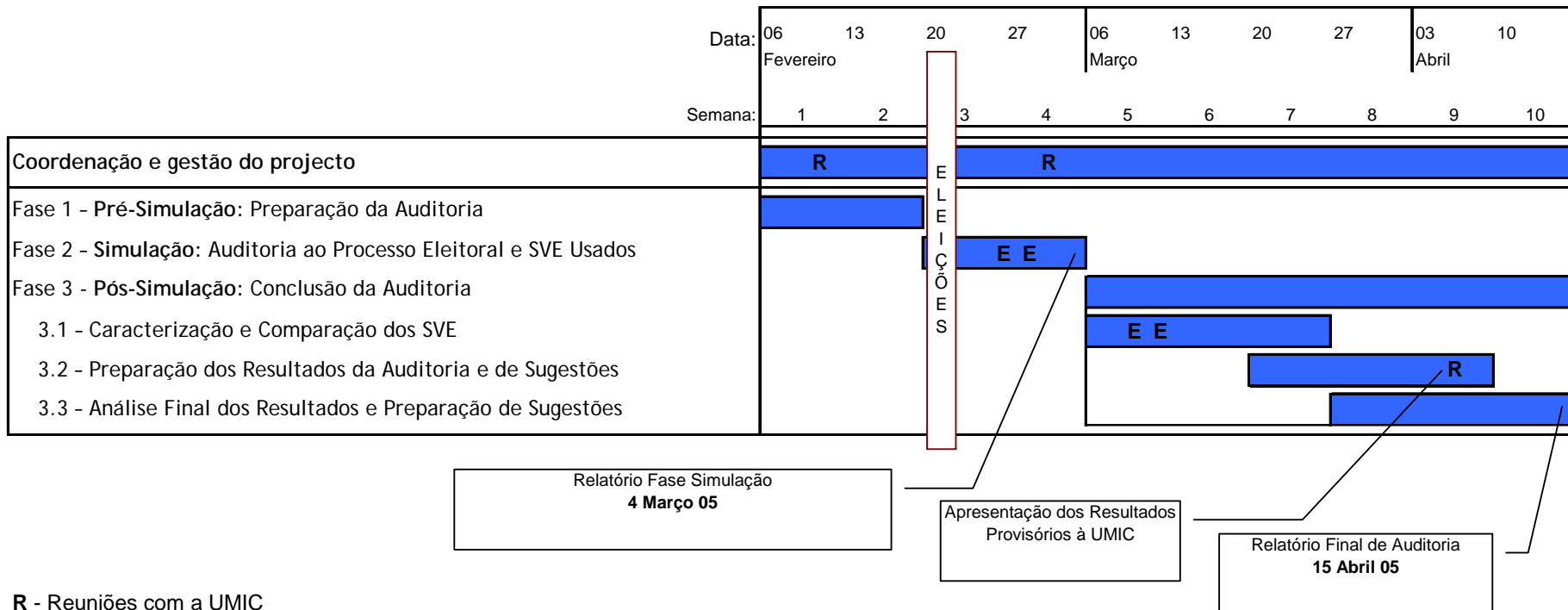
- Prof. Doutor José Fernando Oliveira - Investigação Operacional
- Prof^a. Doutora Maria Antónia Carravilla- Investigação Operacional

Experiências Auditadas

- Voto Presencial
 - Conceição - **Covilhã** (INDRA)
 - Santa Iria de Azóia - **Loures** (MULTICERT)
 - Coração de Jesus - **Lisboa** (INDRA)
 - Santos-o-Velho - **Lisboa** (UNISYS)
 - S. Sebastião da Pedreira - **Lisboa** (UNISYS)
- Voto Não Presencial pela Internet
 - Europa e Resto do Mundo (NOVABASE)



Plano de Auditoria



R - Reuniões com a UMIC
 E - Reuniões com as empresas dos SVE

Principais Tarefas de Auditoria

- Elaboração de pedidos de esclarecimento a enviar às empresas fornecedoras.
- Presença nos locais de voto no dia das eleições, analisando:
 - Abertura das mesas de voto electrónicas
 - Processo de votação electrónica
 - Fecho das mesas de voto electrónicas
 - Contagem / Comunicação / Contagem de votos na UMIC.
- Realização de reuniões com as empresas fornecedoras.
- Redacção dos Relatórios de Auditoria.
- Apresentação e discussão dos resultados intercalares e das sugestões com a UMIC e outros especialistas nacionais ou internacionais.
- Redacção do Relatório Final de Auditoria.

Auditoria no dia das Eleições

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

Metodologia

- Critérios de avaliação e comparação dos SVE:
 - **Segurança** (15 factores).
 - Transparência (14 factores).
 - Usabilidade (5 factores).
 - Acessibilidade (6 factores).
- Definição de um índice de viabilidade tecnológica:
 - Comparação da importância dos critérios - baseado na metodologia AHP [Saaty 1980].
 - Comparação das alternativas de avaliação [Canter 1997].

[Canter 1997] Larry W. Canter: «**Environmental Impact Assessment**», McGraw-Hill, 2nd edition, 1997, p. 557-563.
[Saaty 1980] T. L. Saaty: «**The Analytic Hierarchy Process**». McGraw-Hill, New York, 1980.

Exemplo: 15 factores de Segurança

- Auditabilidade
- Autenticação do Operador
- Certificabilidade
- Detectabilidade de intrusão
- Disponibilidade do Sistema
- Fiabilidade
- Imunidade a Ataques
- Integridade dos Votos
- Invulnerabilidade
- Isolamento
- Rastreabilidade
- Recuperabilidade
- Segurança das comunicações
- Tolerância a Falhas

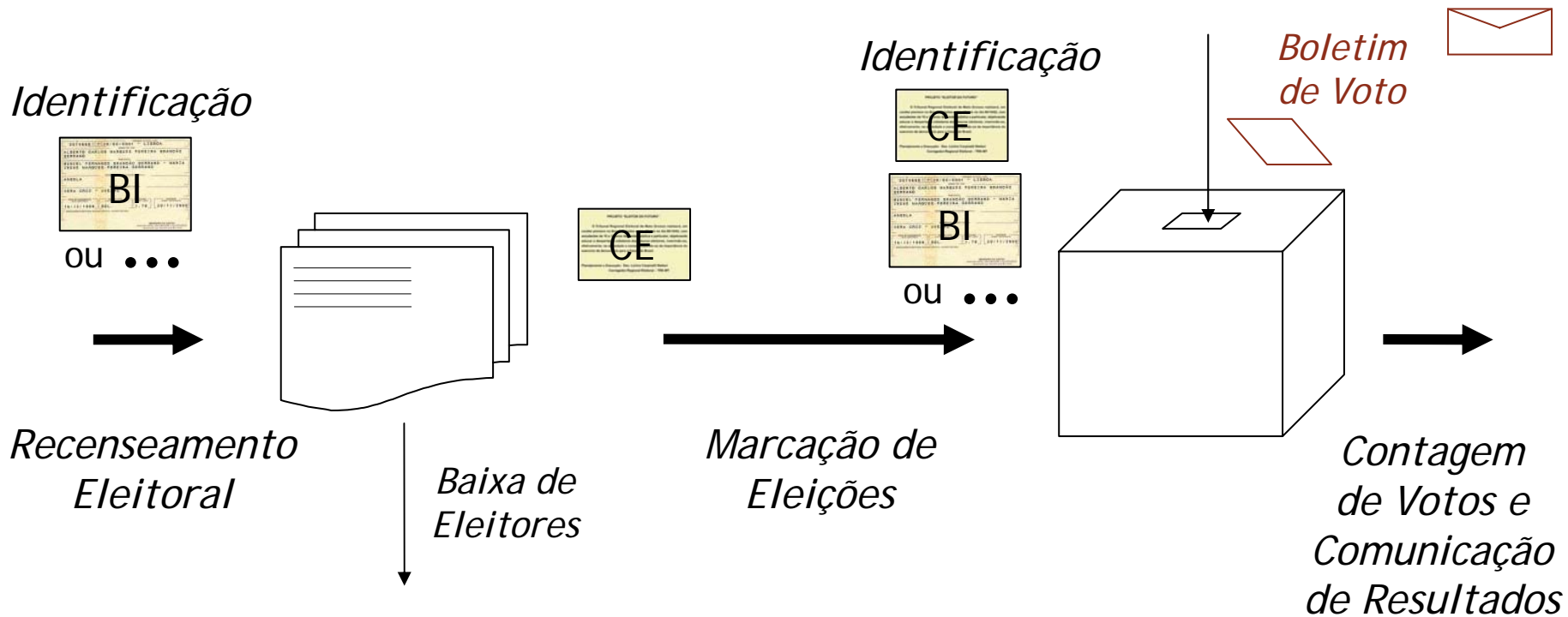
2.

Problemas do VE

Contexto: os processos e os sistemas em Voto Presencial

Gestão do Caderno Eleitoral

Gestão do Acto Eleitoral / Referendo



Satisfação com a transparência e a segurança do processo

- Existe uma elevada satisfação e confiança com o actual processo eleitoral.
- A maior parte dos eleitores não tem conhecimentos e experiências que lhes permitam avaliar a segurança dos sistemas informáticos e de comunicações eventualmente a usar no processo eleitoral.
- É assim necessário um sistema de certificação e auditoria dos sistemas e processos, com alargado reconhecimento social de garantia de transparência e segurança.

Exemplo: ACM - Associação Internacional de Profissionais de Informática

86.30% das respostas a um inquérito da ACM sobre o tema referem forte concordância com a seguinte posição:

«To protect the accuracy and impartiality of the electoral process, ACM recommends that all voting systems - particularly computer-based electronic voting systems - embody careful design, strong safeguards, and rigorous testing in both their design and operation. In addition, voting systems should enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast, and to serve as an independent check on the result produced and stored by the system. Making those records permanent (e.g., not based in computer memory) provides a means by which an accurate recount may be conducted. Ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy. Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by all the electorate»

(ACM <https://campus.acm.org/polls/> 2004-07)

Segurança do Registo em Papel vs. Acessibilidade e Mobilidade

- O registo em papel do VE permite em princípio à maior parte das pessoas verificar os resultados, garantindo uma maior segurança e transparência do processo.
- Mas com esta opção a acessibilidade a pessoas com alguns tipos de deficiência ou dificuldade volta a ser reduzida (não podem p. exemplo ver).
- Essa opção dificulta enormemente a possibilidade de o eleitor votar em qualquer Assembleia de Voto (para eleições com diferentes boletins de voto por região - um único voto impresso de uma determinada origem podia identificar o voto do eleitor).

Segurança do processo: Quantos foram os Votos Electrónicos?

- Votos electrónicos apurados: N_v
- Eleitores que votaram electronicamente: E_v
- Nas eleições não vinculativas passadas sucederam os 3 casos:
 - $N_v > E_v$ (pelo menos um eleitor votou duas vezes)
 - $N_v < E_v$ (pelo menos um eleitor não votou)
 - $N_v = E_v$ (tudo bem ou os dois casos anteriores em igual nº)
- Será um problema dos sistemas ou dos processos?
 - $N_v > E_v$: Pode suceder que ao mesmo eleitor sejam dados dois boletins de voto?
 - $N_v < E_v$: Pode suceder que um eleitor se retire sem colocar o seu boletim de voto na urna?

Segurança - fruto da experiência

- Actualmente os votantes e as pessoas das mesas de voto sabem como o processo de votação se desenrola e conhecem os protocolos.
- A introdução do VE vai requerer muita informação para os votantes e para as pessoas nas mesas de voto, por forma a que sintam segurança no que estão a fazer.
- Será ainda necessário treinar operadores especializados, eventualmente de entre as pessoas das mesas de voto, independentes das empresas fornecedoras, por exemplo para instalarem e fecharem os equipamentos, por forma a que se sintam seguros do que estão a fazer.

Custo de criar, manter e gerir o processo de VE

- Os recursos necessários para gerir o actual processo eleitoral são conhecidos.
- Há muitas arquitecturas TIC possíveis de usar no processo eleitoral, suficientemente seguras e transparentes.
- Cada arquitectura deverá ser avaliada sob diversos critérios, envolvendo nessa análise os custos de investimento e manutenção.

VE Não Presencial - pela Internet

- Em comum com o voto por correspondência, existem os problemas de garantia da autenticidade e do anonimato.
- Há no entanto problemas de segurança adicionais. Por exemplo:
 - Processo de distribuição de credenciais.
 - Software malicioso nos clientes.
 - Tentativas de intrusão.
 - Ataques, por exemplo no percurso da rede.
 - Isolamento dos servidores.

O problema da segurança - conclusões

- Os sistemas de VE podem ser tão seguros quanto desejável.
- A segurança e a transparência são factores «higiénicos» na satisfação e confiança sobre o processo do VE.
- A percepção de segurança requer conhecimento, experiência e autonomia de utilização por parte de todos os intervenientes nos vários papéis desempenhados no processo.

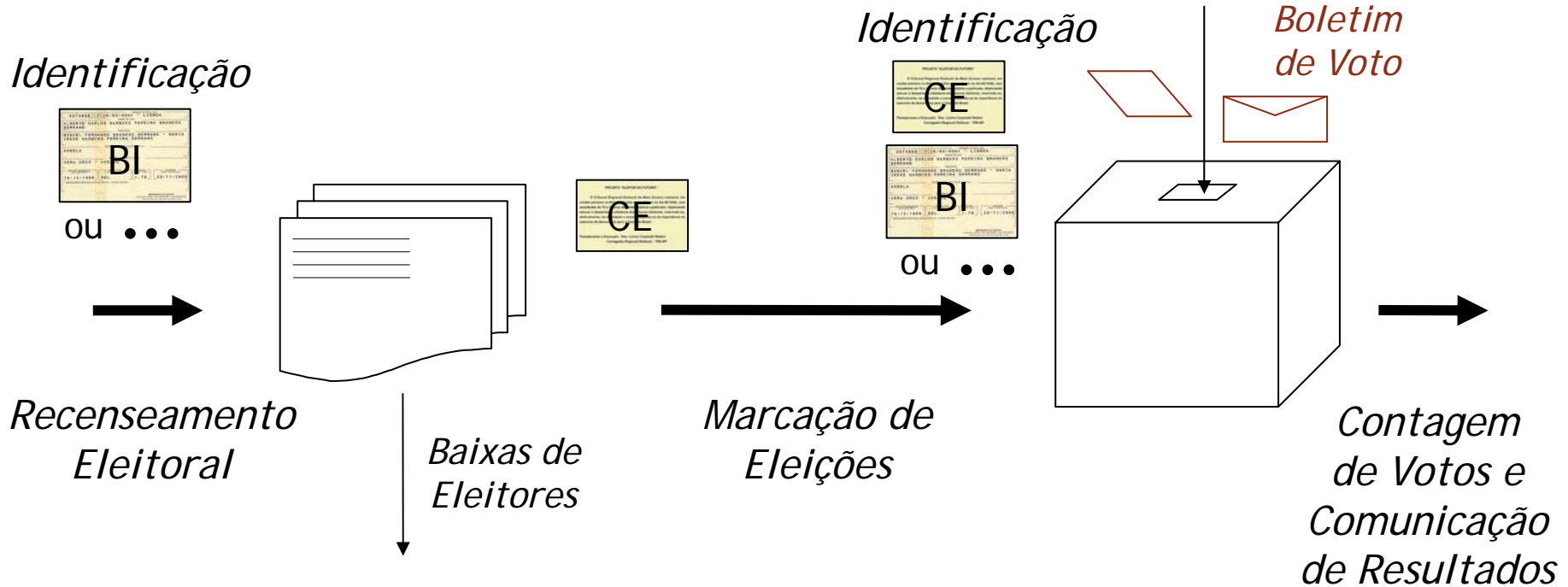
3.

Oportunidades do VE

Contexto: os processos e os sistemas em Voto Presencial

Gestão do Caderno Eleitoral

Gestão do Acto Eleitoral / Referendo



Acessibilidade

- Uma vez garantida a segurança e transparência, o VE pode permitir melhorar a acessibilidade dos eleitores com alguns tipos de deficiência ou dificuldade (p. exemplo de visão).
- O VE pode também permitir ao eleitor exercer o seu direito em qualquer Assembleia de Voto, facilitando assim o acto de votar.

Satisfação e participação dos eleitores

- Os aspectos de acessibilidade e de usabilidade dos SVE terão provavelmente um contributo fundamental positivo para a satisfação do eleitor.

Satisfação dos restantes elementos envolvidos

- É ainda de considerar a satisfação de todos os outros elementos envolvidos no processo eleitoral:
 - Pessoas nas Mesas de Voto.
 - Pessoas nas Autarquias.
 - Pessoas envolvidas na logística do processo eleitoral (transporte seguro de equipamentos e dispositivos).
 - ...

Outros Modelos de VE Não Presencial

- Há outras experiências de VE não presencial:
 - Multibanco / ATM
 - Internet (Simples).
 - Telemóvel / sms / Internet Móvel.
 - Internet com ambiente virtual de assembleia.

3.

Conclusões e Recomendações

Conclusões

(face às experiências realizadas)

- Do ponto de vista técnico, os SVE auditados e os procedimentos de operação associados apresentam um forte potencial para virem a ser usados de forma vinculativa em voto presencial sem mobilidade.
- O voto pela Internet pode ser uma alternativa ao voto por correspondência, numa versão mais madura do SVE utilizado.
- O grau de adopção e satisfação observada numa experiência não vinculativa permite antever o sucesso generalizado destes tipos de votação, uma vez assegurado o envolvimento político e o investimento de recursos adequados.

Recomendações

(face às experiências realizadas)

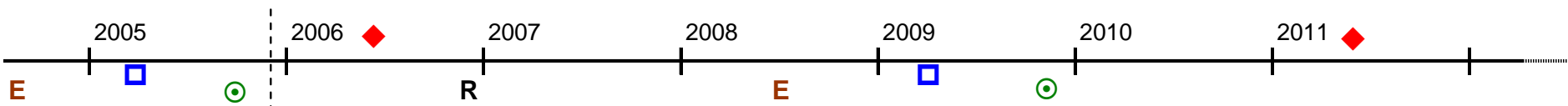
- Avaliar com mais detalhe as soluções de suporte à mobilidade de eleitores.
- Disponibilizar antecipadamente informação detalhada sobre como votar em cada sistema, por exemplo cartazes explicativos e pelo menos um sistema de teste no local de voto.
- Aprofundar as soluções de suporte à acessibilidade - inclusão de cidadãos com deficiências visuais e com défice de literacia.
- Utilizar métodos redundantes de verificação de votação, por exemplo através do registo de voto em papel.
- Melhorar a formação das pessoas envolvidas no processo, em particular dos elementos das mesas de voto.
- No voto pela Internet, assegurar a qualidade do processo de distribuição de credenciais.

Conclusões

- Experiências de VE não vinculativo são necessárias e relevantes - ver excelente resumo de recomendações da CNPD.
- Mas é essencial ter como objectivo as experiências de VE vinculativo:
 - Seguro
 - Transparente
 - Acessível
- Para satisfação e participação dos eleitores

Recomendações

- Definir objectivos e arquitectura dos sistemas de VE a usar.
- Definir um plano de acções para um ciclo eleitoral completo.
- Promover experiências de VE presencial e não presencial em outros actos eleitorais (Universidades, Sindicatos, ...).



Eleições

- ◆ Presidente da República
- Legislativas
- ⊙ Poder Local
- E Parlamento Europeu
- R Referendo



Mensagem Final

De tudo, ficaram três coisas:

A certeza de que estamos sempre começando...

A certeza de que precisamos continuar...

A certeza de que seremos interrompidos antes de terminar...

Portanto devemos:

Fazer da interrupção, um caminho novo...

Da queda, um passo de dança...

Do medo, uma escada...

Do sonho, uma ponte...

Da procura, um encontro...

Fernando Pessoa