Projecto de Avaliação de Sistemas de Votação Electrónica – Definição do Contexto e Critérios de Avaliação

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

VERSÃO 1.4

2 DE JUNHO DE 2004

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

SUMÁRIO

1. INTRODUÇÃO

Os Sistemas de Votação Electrónica (SVE) são sistemas que, quer pelas suas características e limitações quer pelo seu impacto social, estão actualmente em estudo e desenvolvimento intensivos em todo o mundo, encontrando-se já em utilização em alguns países, contudo com algumas limitações.

São de certo modo nobres os objectivos que levam ao desenvolvimento de SVE, sobretudo após um decréscimo significativo do interesse na participação em processos eleitorais que se tem vindo a verificar nas democracias ocidentais.

Proporcionar um aumento das oportunidades de voto, redução de votos nulos não intencionais, maior rapidez e exactidão na contagem dos votos, etc., são alguns dos objectivos de um SVE.

No entanto, o sucesso dos SVE requer a confiança dos eleitores e do público em geral em todo o processo de introdução desta tecnologia.

A questão fundamental está em identificar qual a combinação óptima entre tecnologia e processos sociais que garanta um conjunto muito vasto de propriedades que a sociedade considera como adquiridas relativamente ao processo eleitoral. Os desafios são inúmeros, desde a necessidade de garantir que um SVE funciona em grande escala, sem problemas de fiabilidade e segurança que coloquem uma votação em causa; que o sistema seja capaz de garantir o anonimato e a integridade dos votos; que o sistema seja acessível e utilizável por uma imensa diversidade de pessoas; não esquecendo também que o sistema e processos eleitorais devem continuar a ser facilmente compreensíveis para os utilizadores comuns e entidades administrativas e políticas.

1.1. OBJECTIVOS

O objectivo fundamental deste documento consiste em clarificar todo o processo que leva a uma avaliação cuidada de um SVE, realizada por peritos em sistemas informáticos.

O cumprimento deste objectivo envolve, num primeiro passo, a especificação de todos os componentes que constituem um SVE – não apenas físicos, mas também lógicos, processuais ou documentais – e a identificação de todos os critérios de avaliação.

Num segundo passo é construída uma grelha que permite avaliar as correlações entre os componentes do SVE e os critérios de avaliação.

Finalmente, apresenta-se uma lista aberta de recomendações sobre o desenvolvimento e utilização de SVE, que serve de base para a avaliação das correlações acima referidas.

2. ENQUADRAMENTO DA AVALIAÇÃO

Entende-se a avaliação de um SVE como sendo constituída por três actividades fundamentais:

1. Definição do contexto e critérios de avaliação.
2. Análise do software, documentação, processos, produtos, interfaces com o mundo não electrónico, equipamento, micro-código e circuitos especiais utilizados, previamente e posteriormente ao acto eleitoral; assim como observação directa do funcionamento dos SVE durante o acto eleitoral.
3. Análise dos dados recolhidos e avaliação dos SVE de acordo com os critérios estabelecidos.

O presente documento cumpre os objectivos da primeira actividade acima referida.

3. OBJECTO DA AVALIAÇÃO

O objecto da avaliação é o SVE. Sendo este um sistema socio-técnico bastante complexo, é conveniente discriminar as seguintes três perspectivas complementares sobre o SVE:

- **Processo eleitoral** – Componente social da operação e funcionamento do SVE. O processo eleitoral pode ser fragmentado em diversos sub-processos, incluindo os sub-processos de recenseamento, votação e contagem.
- **Produto** – O SVE perspectivado como uma caixa negra, apresentando-se com um conjunto de atributos, funcionalidades e restrições.
- **Sistema** – Visão aberta do SVE, identificando os seus diversos dispositivos, componentes, interfaces e infraestruturas de comunicação.

Esta divisão do SVE em três perspectivas deverá ser sistematicamente utilizada no processo avaliação.

Seguidamente são pormenorizadas as referidas perspectivas.

3.1. PROCESSO ELEITORAL

Consideram-se três sub-processos fundamentais que compõem o processo eleitoral:

- **Recenseamento eleitoral**
- **Votação**
- **Contagem dos votos**

O processo de recenseamento eleitoral realiza o registo prévio dos eleitores – pessoas que perfazem as condições de serem eleitoras. Este registo é obrigatório sendo fornecido ao eleitor recenseado um mecanismo de comprovação da identidade, que pode se instanciado de diversas formas, perante o SVE ou membro da mesa eleitoral que opere o SVE.

O processo de votação deve permitir a identificação do eleitor, validação das condições de votação e disponibilização de um mecanismo com o qual o eleitor possa escolher a sua opção de voto. No contexto deste projecto considera-se que o processo de votação será realizado exclusivamente num ambiente presencial e em recinto controlado, à semelhança do que hoje acontece, mas substituindo o voto em papel por outro em formato electrónico.

No âmbito deste processo, os eleitores terão que se identificar junto de um membro da mesa eleitoral, ao qual compete verificar a identidade do eleitor e confirmar a sua condição de eleitor. A verificação da identidade dos eleitores pode em alternativa ser realizada pelo SVE, não sendo de momento conhecida qual a alternativa que será avaliada.

Depois de verificados todos os requisitos, é disponibilizado ao eleitor um boletim de voto electrónico que este preenche e entrega. No contexto deste projecto serão cuidadosamente analisadas todas as formas de interacção com o boletim (e.g. audíveis, tácteis, visuais), tendo em atenção os potenciais problemas de acessibilidade.

O processo de contagem tem como finalidade o apuramento e contagem de votos, bem como a publicação e divulgação dos seus resultados. Os resultados apurados são agrupados em resultados parciais (e.g. uma mesa eleitoral) e totais (e.g. todos os círculos eleitorais) segundo parâmetros previamente estabelecidos (totais por freguesia/concelhos/distritos, partidos, eleitos, etc.). O apuramento de resultados pode envolver comunicação de dados entre os diversos componentes distribuídos do SVE, sendo nesse caso necessário avaliar os potenciais problemas relacionados com a infraestrutura de comunicações do SVE (disponibilidade, tolerância a faltas, etc.).

3.2. PRODUTO

Relativamente a esta perspectiva, identificam-se os seguintes elementos que serão objecto de avaliação:

- **Software** – Documentos de especificação da análise, desenho, codificação, teste e manutenção do software
- **Hardware** – Documentos de especificação da análise, desenho, codificação, teste e manutenção do hardware (incluindo firmware)
- **Manuais** de instalação, manutenção e utilização
- **Planos** e resultados de testes/utilizações do produto
- **Certificados** do cumprimento de normas internacionais, em particular normas de qualidade aplicadas ao desenvolvimento de hardware e software

3.3. SISTEMA

Considera-se que um SVE é constituído pelos seguintes componentes principais:

- **Servidores** – Onde está armazenada a informação eleitoral
    - Servidor de eleitores – Armazena os dados referentes aos eleitores e permite fazer a gestão dessa mesma informação, designadamente a verificação das condições de eleitor
    - Servidor de votação – Armazena e gere a informação relativa ao processo de votação, como por exemplo a lista de candidatos
    - Servidor de resultados – Armazena e disponibiliza os resultados do processo de votação
- **Urna** – Onde é realizado o voto
    - Subsistema de supervisão – Destina-se a gerir e supervisionar o processo de votação
    - Subsistema de votação – É o dispositivo que permite ao eleitor votar
    - Subsistema de contagem parcial
- **Gestor de resultados** – Onde são apurados os resultados globais do processo eleitoral
    - Subsistema de contagem global
    - Subsistema de apresentação de resultados
- **Interfaces –** Agrupamentos de componentes, gráficos e outros, que interagem com os diversos utilizadores do sistema
    - Interface de votação – Utilizada pelo eleitor para preencher e confirmar o boletim de voto

    - Interface de supervisão – Utilizada pelo membro da mesa eleitoral para dar início à votação, verificar e gerir o direito de voto, terminar a votação e apurar resultados
    - Interface de manutenção – Utilizada para ligar, manter, verificar e desligar os componentes do sistema
    - Interface de inspecção – Utilizada para auditar o funcionamento dos componentes do sistema
- **Infraestrutura de comunicação** – Destinada a interligar todos os restantes componentes do sistema
    - Rede de cliente – Destinada a interligar componentes locais do sistema, como sejam a urna e a interface de votação
    - Rede de serviço – Destinada a interligar componentes locais e globais do sistema, como sejam a urna e o gestor de resultados
    - Rede pública – Destinada à divulgação dos resultados

4. CRITÉRIOS DE AVALIAÇÃO

Um SVE deve garantir, além dos critérios inerentes ao processo eleitoral tradicional, mais um conjunto de critérios justificados pela utilização de sistemas electrónicos e informáticos.

O que se apresenta em seguida é uma lista exaustiva dos critérios que têm sido identificados pela literatura científica que aborda os SVE.

4.1. CRITÉRIOS GERAIS

Autenticidade

Autenticar o indivíduo é o meio pelo qual a identificação de um eleitor é validada e confirmada. Apenas os eleitores autorizados devem poder votar.

Singularidade

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

Direito de Voto

O Direito de voto será atribuído a um eleitor sempre que ele verifique simultaneamente as propriedades de autenticidade e singularidade. Será sempre necessário verificar o direito de voto de um eleitor antes de ele poder votar.

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).

Integridade dos Votos

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

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.

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.

4.2. CRITÉRIOS RELACIONADOS COM O PROCESSO ELEITORAL

Confiabilidade

O sistema deve funcionar de forma robusta, sem perda de votos, tornando-se confiável ao olhos dos diversos actores que nele participam.

Disponibilidade

O sistema deve estar sempre disponível durante o período eleitoral, para que o processo decorra normalmente.

Precisão

As eleições podem ser decididas por apenas um voto. O sistema não pode tolerar margens estatísticas de erro durante a sua operação, seja na fase de votação ou contagem dos votos. Até os erros involuntários dos eleitores, provocados por processos ou equipamentos inadequados, podem inverter ou modificar o resultado eleitoral.

Verificabilidade

O sistema deve permitir a verificação de 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.

Transparência do Processo

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

4.3. CRITÉRIOS DE SEGURANÇA

Detectabilidade

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

Tolerância a Ataques

A principal característica que diferencia um SVE de outros sistemas de alto risco é que este poderá ser alvo privilegiado de ataques mal intencionados. Medidas de defesa

contra fraudes, inclusive vindas dos próprios agentes que projectaram e desenvolveram o sistema, devem ser rigorosas e redundantes.

Tolerância a Faltas

É desejável a existência de métodos de detecção de faltas no equipamento. A troca de um bit num total de um candidato pode ser a diferença entre ganhar ou perder a eleição.

Autenticação do Operador

Os utilizadores autorizados a operar o sistema devem estar sujeitos a 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.

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

O SVE deve poder ser posto à prova, depois de validado e certificado por auditores externos.

Invulnerabilidade

A invulnerabilidade do SVE é garantida se se verificarem sempre as condições de autenticidade e singularidade.

Recuperabilidade

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

4.4. CRITÉRIOS DE QUALIDADE

Auditabilidade

O sistema deverá poder ser auditado, quer por observadores externos – através por exemplo da análise do registo de "logs", quer pelo próprio sistema – com a confrontação dos diversos dados.

Certificabilidade

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

Documentação

Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema devem estar documentados, devendo não conter ambiguidades e ser coerentes.

Transparência do Sistema

Todo o software, documentação, equipamento, micro-código e circuitos especiais devem poder ser abertos para inspecção e auditoria a qualquer instante.

Rastreabilidade

O SVE deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir "logs" de entrada e saída de utilizadores, bem como registos do envio e recepção de dados, que obviamente não comprometam as restantes propriedades (anonimato e privacidade).

4.5. CRITÉRIOS DE USABILIDADE

Usabilidade

O SVE deve ser de fácil uso quer para eleitores quer para operadores.

Conveniência

O SVE 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.

Acessibilidade

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

Mobilidade

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

Viabilidade

O SVE deve ser eficiente e viável economicamente.

5. GRELHA DE AVALIAÇÃO

	Gerais							Processo					Segurança								Qualidade					Usabilidade				
	Autenticidade	Singularidade	Direito de voto	Anonimato	Integridade dos votos	Privacidade	Não-coercibilidade	Confiabilidade	Disponibilidade	Precisão	Verificabilidade	Transparência do processo	Detectabilidade	Tolerância a ataques	Tolerância a faltas	Autenticação do operador	Integridade do pessoal	Integridade do sistema	Invulnerabilidade	Recuperabilidade	Auditabilidade	Certificabilidade	Documentação	Transparência do sistema	Rastreabilidade	Usabilidade	Conveniência	Acessibilidade	Mobilidade	Viabilidade
Processo eleitoral																														
Recenseamento	■	■	■	■	■	■	■	■	■	■	■	■																		
Votação	■	■	■	■	■	■	■	■	■	■	■	■																		
Contagem	■	■	■	■	■	■	■	■	■	■	■	■																		
Produto																														
Software																					■	■	■	■	■					
Hardware																					■	■	■	■	■					
Manuais																					■	■	■	■	■					
Testes																					■	■	■	■	■					
Certificados																					■	■	■	■	■					
Sistema																														
Servidores																														
Eleitores	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Votação	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Resultados	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Urna																														
Supervisão	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Votação	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Contagem parcial	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Gestor de resultados																														
Contagem	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Apresentação	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Interfaces																														
Votação																										■	■	■	■	■
Supervisão																										■	■	■	■	■
Manutenção																										■	■	■	■	■
Inspecção																										■	■	■	■	■
Infraestrutura de comunicação																														
Rede de cliente	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Rede de serviço	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										
Rede pública	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■										

Esta grelha resulta do cruzamento entre o objecto da avaliação, discriminado nos seus diversos componentes, e os critérios de avaliação e destina-se a sistematizar o processo de avaliação. Cada célula desta grelha avalia o grau de correlação entre um componente do SVE e um critério de avaliação. Apenas as células marcadas correspondem a correlações que à partida justificam uma avaliação. Seguindo uma abordagem corrente em avaliações deste tipo, serão utilizados os valores 0, 1, 3 e 9 (nenhuma, fraca, média e forte, respectivamente) para medir essa correlação.

A utilização de valores numéricos permitirá, a partir desta grelha, ordenar os diferentes SVE que forem avaliados. Deve no entanto ser ressalvado que, apesar da grelha, nem todos os critérios de avaliação possuem o mesmo grau de importância (por exemplo, os critérios gerais são mais importantes que os restantes), pelo que os resultados da avaliação não poderão ser meramente resumidos às pontuações globais obtidas por cada SVE.

Para a obtenção dos valores apropriados para cada célula desta grelha serão realizadas diversas perguntas relevantes sobre o SVE. Por exemplo:

A urna tem alguma fonte de energia alternativa (UPS, por exemplo)?

Existem cópias de segurança da informação?

Caso tenha que se reiniciar a urna, está prevista a recuperação do sistema e da informação no ponto exacto?

Está algum cabo (alimentação, conexão, etc.) acessível aos votantes?

O código fonte do produto é auditável (código aberto)?

O produto inclui bases de dados? O modelo de dados é auditável?

Como é feita a "inseminação" das bases de dados? Nomeadamente como e quem insere os candidatos no sistema?

Como é garantida a selagem das bases de dados?

Os votos são guardados em claro ou codificados? Que técnica de criptografia é utilizada?

Quais os níveis de segurança para os vários utilizadores (administrador, operador, eleitor, etc.)?

É feito o registo de todas as ocorrências (logs)? Em que tipo de suporte?

O conjunto de perguntas relevantes é deixado em aberto, tendo em vista dar liberdade aos avaliadores, diversificando e variando as formas de aquisição de dados e, por este meio, aumentando a qualidade do próprio processo de avaliação.

6. RECOMENDAÇÕES

O conjunto de recomendações que a seguir se apresentam resultam de uma colectânea exaustiva das melhores práticas que têm sido seguidas no desenvolvimento de SVE em particular e sistemas socio-técnicos complexos em geral.

Este conjunto de recomendações destina-se a auxiliar os avaliadores na construção das perguntas relevantes sobre o SVE, organizadas de acordo com a grelha anteriormente apresentada.

6.1. SOBRE O PROCESSO ELEITORAL

- A exagerada complexidade de determinados processos de segurança, nomeadamente os que garantam a autenticação dos operadores, pode colocar em causa a transparência ou mesmo a viabilidade do sistema
- Devem existir regras que garantam a integridade do pessoal que opera o sistema
- Deve existir legislação que regule o período de preservação dos dados eleitorais, incluindo os resultados e todos os dados necessários à auditoria dos sistemas
- Devem existir instruções que expliquem claramente o processo eleitoral

6.2. SOBRE O SISTEMA

- Deve existir legislação que penalize as tentativas de ataque ao sistema
- Devem existir regras que garantam a correcção dos dados eleitorais atribuídos a cada urna, assim como a sua distribuição e posterior verificação
- Devem existir regras que regulem a vida dos dados do sistema, identificando que dados dever ser eliminados ou preservados após a votação
- Pela sua natureza, os SVE são particularmente apetecíveis a tentativas de ataque, que podem ter origens internas (quem desenhou ou opera o sistema, por exemplo) ou externas
- O número de operadores privilegiados do sistema deve ser minimizado e controlado
- O sistema deve garantir que os operadores privilegiados do sistema não se possam aproveitar desses privilégios para acções indevidas
- O sistema deve ter mecanismos de autenticação não triviais dos operadores privilegiados
- O sistema deve restringir o acesso a operadores por níveis de acesso e componentes
- Deve existir legislação que regule e sancione os operadores privilegiados do sistema
- Os métodos de ataque electrónico ao sistema englobam: “hacking”, software malicioso, negação de serviço, redirecção de mensagens na rede de comunicação
- Os métodos de ataque não electrónico ao sistema englobam: compra, venda ou coerção de votos; roubo ou falsificação de mecanismos de identificação dos eleitores
- O sistema deve garantir que todos os eventos relevantes são registados de forma persistente por mais de um dispositivo de armazenamento de dados
- O sistema deve garantir que o registo de eventos relevantes não possa ser modificado ou reinicializado
- O sistema deve garantir o acesso dos auditores à lista de eventos relevantes

- O sistema deve ter um relógio que permita registar os eventos relevantes segundo a sua ordem temporal
- A partição do sistema em diversos componentes estanques aumenta a tolerância a ataques

6.3. SOBRE A URNA

- Deve existir um procedimento de selagem da urna
- Os dispositivos de ligação da urna a outros periféricos devem ser selados antes do acto eleitoral e permanecer selados até ao fim do acto eleitoral
- A urna deve ser ensaiada antes do acto eleitoral. O ensaio deve ser realizado como se de uma votação se tratasse, e não através de qualquer procedimento especial que ponha em dúvida o processo de ensaio
- A cada componente de software utilizado pelo SVE deve estar associada uma assinatura digital
- Deve existir um procedimento para garantir que o sistema operativo da urna não foi modificado, por exemplo com a inclusão de um vírus ou "Cavalo de Tróia"
- Deve existir um procedimento para instalação de software em cada urna
- Deve existir um procedimento para garantir que cada urna é configurada com os dados correspondentes à eleição e mesa eleitoral que lhe foram atribuídas
- Devem existir urnas de substituição em número suficiente face à probabilidade de falha de cada urna
- A urna deve ter um mecanismo de bloqueio que garanta a singularidade do voto
- A urna deve ter um mecanismo de desbloqueio no caso de o eleitor desistir de votar
- A utilização de recibos em papel, que permitam confirmar a contagem dos votos de uma urna, tem sido considerada importante para a transparência do sistema. Estes recibos devem ser obrigatoriamente colocados numa urna
- A separação física entre os mecanismos de identificação dos eleitores e os mecanismos de votação tem sido considerada importante para garantir o anonimato dos votantes
- A urna não deve estar ligada nem à rede de serviço nem à rede pública durante o acto eleitoral
- A urna deve possuir fonte de energia alternativa
- A urna deve possuir um mecanismo de preservação dos dados no caso de reinicialização do sistema
- Devem existir procedimentos de operação da urna em caso de ataques, falhas do sistema ou eventos da natureza
- A urna deve ter um mecanismo de diagnóstico do seu funcionamento
- A existência de um contador, visível para o público, que indique o número de votos que já foram introduzidos na urna é considerada benéfica para o aumento da transparência do sistema
- Deve existir um procedimento para votação de emergência, eventualmente em papel, no caso de a urna falhar e não existir urna de substituição
- A urna deve mostrar todas as mensagens críticas do sistema, designadamente as que reportam interrupções, falhas de componentes ou serviços, erros de software ou erros de transmissão
- A urna deve fornecer um relatório de operação depois de terminada a votação

6.4. SOBRE AS INTERFACES

- As interfaces devem suportar utilizadores com necessidades especiais, nomeadamente utilizando canais alternativos de voz ou tácteis
- As interfaces devem suportar mecanismos adequados de retorno ("feedback") para os utilizadores, em particular que indiquem qual o voto que realizaram e que o voto foi armazenado na urna
- As interfaces de votação devem suportar a confirmação do voto dos eleitores
- As interfaces de votação devem confirmar que os votos dos eleitores foram recebidos pelo sistema, sem no entanto colocarem em causa a não-coercibilidade do voto
- As interfaces de votação devem suportar votos em branco e nulos
- As interfaces de votação não devem privilegiar algumas opções de votação em desprimor das outras, nomeadamente por razões de gestão do espaço disponível nos dispositivos
- A urna electrónica elimina os erros de contagem dos votos mas introduz erros na selecção e confirmação dos votos pelos votantes, que podem ser devidos a falhas nas interfaces
- As interfaces devem minimizar a probabilidade de ocorrência de erros dos utilizadores
- É desejável que as interfaces sejam multi-língua
- As mensagens de erro das interfaces devem ser compreensíveis pelos utilizadores

6.5. SOBRE OS SERVIDORES

- Os servidores de votação não devem nunca associar os eleitores aos respectivos votos, mesmo que tal informação se encontre cifrada e o algoritmo de cifra seja extremamente robusto
- A replicação de servidores é uma forma de garantir tolerância a faltas e recuperabilidade do sistema
- Deve existir um procedimento para limpeza e inseminação dos servidores antes do acto eleitoral
- Os servidores devem ser selados antes do acto eleitoral
- A informação nos servidores deve ser cifrada e os algoritmos de cifra devem ser conhecidos e não triviais
- Os servidores devem possuir mecanismos de validação da escrita ou modificação dos dados

6.6. SOBRE A INFRAESTRUTURA DE COMUNICAÇÃO

- A separação da infraestrutura de comunicação em diversas redes com diferentes níveis de segurança aumenta a invulnerabilidade do sistema
- Todas as mensagens trocadas pela infraestrutura de comunicação devem ser cifradas e os algoritmos de cifra devem ser conhecidos e não triviais
- A infraestrutura de comunicação deve fornecer mecanismos de tolerância a faltas relacionados com perda de mensagens
- Devem existir mecanismos de teste da infraestrutura de comunicação

6.7. SOBRE O SOFTWARE

- Deve existir uma descrição das formas de interacção dos utilizadores com o sistema (casos de uso)
- Deve existir uma descrição dos dados geridos, armazenados e transmitidos pelo sistema
- Deve existir uma descrição dos componentes do sistema
- Deve existir uma descrição exaustiva das medidas de segurança desenvolvidas no sistema, seja na fase de análise, design, codificação e teste do sistema
- Devem existir evidências de boas práticas na produção do software, designadamente gestão de versões, gestão da configuração, inspecção, revisão, verificação, validação e teste
- Considera-se que a utilização de código aberto é benéfica para a transparência do sistema, mesmo que em detrimento da invulnerabilidade do sistema
- Considera-se que a utilização de linguagens de programação de alto nível, nomeadamente orientadas a objectos, são benéficas para aumentar a auditabilidade do software