Auditoria ao Projecto de Voto Electrónico

Eleições Legislativas de 20 de Fevereiro de 2005

Relatório Final

Sistema NOVABASE

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

Auditoria ao Projecto de Voto Electrónico

Conteúdos

Página

1 Introdução

O sistema de voto electrónico via Internet, destinado aos círculos de emigração, é de natureza substancialmente diferente dos sistemas presenciais experimentados na outra componente do projecto de Voto Electrónico Legislativas 2005. No entanto, por razões de homogeneidade e facilidade de leitura, optou-se por adoptar a mesma estrutura para todos os relatórios de auditoria, adaptando onde necessário.

1.1 Comissões de auditoria envolvidas

A comissão de auditoria foi constituída por:

- Gabriel David, Professor Associado (relator)
- Sérgio Reis Cunha, Professor Auxiliar
- José Magalhães Cruz, Professor Auxiliar
- João Isidro Vila Verde, Mestre

As observações do acto eleitoral foram efectuadas na Internet, entre os dias 2005-02-16 e 2005-03-04.

1.2 Fontes de informação

As fontes de informação a que tivemos acesso foram:

- Sítio Web do projecto Voto Electrónico Legislativas 2005 [http://www.votoelectronico.pt/]
- Sítio Web da votação via Internet [http://voto.votoelectronico.pt/]
- Reunião com a equipa do projecto na empresa de desenvolvimento Novabase, no dia 2005-02-19, entre as 15H30 e as 19H (FEUP: Gabriel David, Sérgio Reis Cunha, Isidro Vilaverde, Raul Vidal, António Brito, Luís Miguel Silva; Novabase: Nuno Carvalho, Valter Santos, António Cardoso, outro elemento; CNPD: Fernando Silva)
- Reunião com a equipa do projecto na empresa de desenvolvimento Novabase, no dia 2005-02-20, entre as 12H00 e as 13H30 (FEUP: Gabriel David, Isidro Vilaverde, João Correia Lopes, Luís Miguel Silva; Novabase: Diogo Assunção, Nuno Carvalho, Valter Santos, outro elemento)

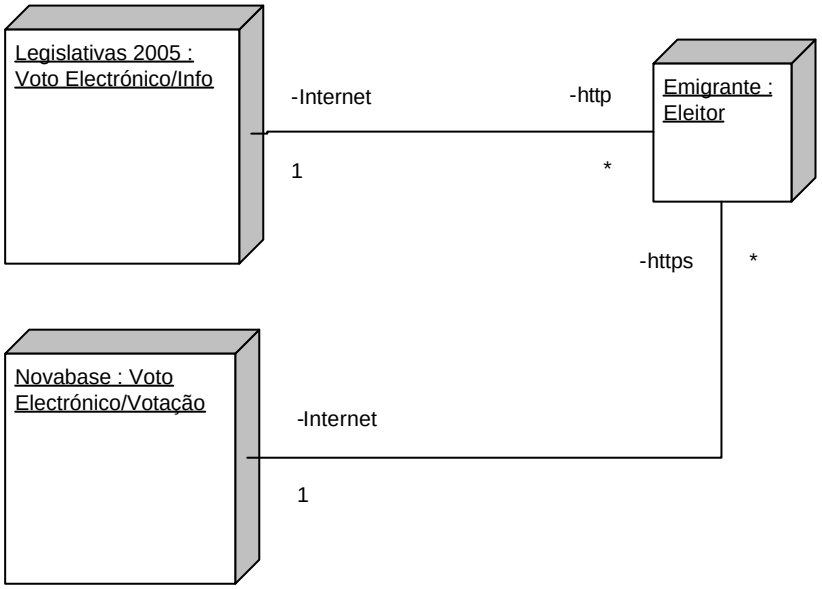
- CD fornecido pela Novabase com o software utilizado e a documentação de especificação
- Sessão de contagem de votos em 2005-03-04 (FEUP: Falcão e Cunha)

2 Apresentação do SVE – Sistema de Voto Electrónico

Apresenta-se o sistema de voto electrónico pela Internet desenvolvido pela empresa Novabase, o parceiro seleccionado pela UMIC para desenvolver o software e assegurar a operação do SVE não presencial do projecto Voto Electrónico Legislativas 2005. Alguns aspectos de detalhe são deixados para a secção de Apreciação do SVE, para não tornar a apresentação demasiado pesada.

2.1 Arquitectura do SVE

O subsistema não presencial do SVE adopta a arquitectura cliente servidor habitual nos



sistemas que utilizam o serviço World Wide Web da Internet. Do ponto de vista lógico existem um sítio Web de Voto Electrónico (URL: http://www.votoelectronico.pt) e Eleitores, distribuídos na Internet.

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, em sua casa, no local de trabalho, num serviço público ou num cibercafé.

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 infraestrutura 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.

O Frontend é um monoprocessador com 2GB de RAM, a correr MS Windows 2003 Server, com Virtual Server 2005. Estão instaladas nele duas máquinas virtuais com o servidor Web MS IIS e equilíbrio de carga.

O Backend é um biprocessador Xeon a 2.8 GHertz, com 4GB de RAM, e 3x146 GB de disco, montados em RAID5, a correr MS Windows 2003 Server, com Virtual Server 2005. Estão instaladas nele quatro máquinas virtuais: dois controladores de domínio com Active Directory; e dois servidores de base de dados (BD) MS SQLServer montados em cluster e a partilhar os discos.

Recorreu-se a um terceiro nó para o processo de contagem dos votos, sendo a informação respectiva transportada do nó Voto Electrónico/Votação em CD.

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

2.2 Procedimentos do SVE

Os procedimentos do SVE não presencial acompanharam os da votação por correspondência, os quais incluem:

1. Fixação dos Cadernos Eleitorais;
2. Impressão das etiquetas com as moradas dos eleitores;
3. Envio, através de uma empresa de mailing, de cartas com os boletins de voto e envelopes para garantir o anonimato do voto na recepção;
4. Preenchimento do boletim;
5. Recepção das cartas com os envelopes com os votos;
6. Apuramento dos resultados dos círculos internacionais.

Os procedimentos do SVE são descritos abaixo.

O passo 1 de fixação dos Cadernos Eleitorais é comum ao SVE.

2.2.1 Abertura da mesa e dos postos de votação

Os Cadernos Eleitorais são enviados pelo STAPE à UMIC, que os envia para a Novabase, em formato electrónico. No correspondente ao passo 2 acima, o SVE executa o programa de Geração de Credenciais. Este lê os Cadernos Eleitorais, produz e imprime 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) para cada eleitor e regista o eleitor e a respectiva credencial no Backend, no Active Directory.

O Active Directory funciona como Caderno Eleitoral, durante a votação. As credenciais são entregues à empresa de mailing, através da UMIC, com o nome do eleitor, para o respectivo envio no passo 3, em conjunto com informação sobre o processo de votação, em particular o URL do sítio do SVE. Note-se que da informação entregue à empresa de mailing não faz parte o número de eleitor, impedindo que quem tenha acesso a esta informação possa realizar votos indevidamente. Esta protecção não é muito robusta.

A BD no Backend é também preparada com uma tabela contendo todas as credenciais emitidas, no 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.

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. Existe uma operação de geração das chaves, 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 CDs e entregues uma a cada partido representado na CNE e uma à CNPD. Desta forma, garante-se que os votos só podem ser desencriptados com a anuência das sete partes envolvidas.

A partir do momento em que o SVE é activado, consideram-se abertos os postos de votação e a mesa de voto do SVE.

2.2.2 Votação

No passo 4, 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.

No correspondente ao passo 5, o voto confirmado e enviado ao servidor Web do SVE é codificado e registado numa das tabelas de votos da BD. 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, passando ao já referido inquérito sobre o projecto.

2.2.3 Fecho da mesa e dos postos de votação

No momento do encerramento do período de votação, o sítio de votação do SVE é desligado 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. Isto encerra o correspondente ao passo 5.

2.2.4 Apuramento de resultados

O passo 6 de apuramento dos resultados é, no sistema de voto por correspondência, atrasado alguns dias, relativamente à data da votação presencial. Para manter o paralelismo, o apuramento dos resultados do SVE não presencial é atrasado até essa data, embora tecnicamente pudesse ocorrer imediatamente após o fecho da votação.

A contagem é efectuada no terceiro nó, nas instalações da CNE, o qual contém uma BD vazia e 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 gerado no passo 5, com a cópia da informação da votação, é carregado na BD. Na fase seguinte, o programa de contagem desencripta os votos, usando a chave reconstruída, e produz a contagem.

3 Apreciação do SVE

Para uma correcta compreensão e avaliação do SVE não presencial é necessário explicitar desde já o objectivo e as circunstâncias em que decorreu o projecto piloto. O objectivo foi estudar a viabilidade e a aceitação de um método de voto à distância, recorrendo à Internet, no sentido de facilitar e incentivar o exercício do direito ao voto. Para isso procedeu-se a uma votação não vinculativa, usando um SVE não presencial, que acompanhou o processo de voto por correspondência dos círculos internacionais.

Ao contrário do que sucedeu no SVE presencial, em que alguns parceiros apresentaram sistemas já utilizados em votações vinculativas, neste caso o parceiro seleccionado (Novabase) desenvolveu de raiz um SVE e testou-o pela primeira vez neste projecto. Dadas as restrições temporais impostas a todo o projecto, a solução utilizada não pode ser considerada como completamente desenvolvida. No entanto, considera-se que existem condições para auditar um conjunto de aspectos dessa solução. A análise foi efectuada sobre o sistema efectivamente utilizado, tendo embora a perspectiva do que haveria a mudar no caso de uma votação vinculativa.

3.1 Apreciação da arquitectura e desempenho do sistema

3.1.1 Indicadores de desempenho e calendário

Número de eleitores nos círculos internacionais	147 000
Geração de credenciais	1 hora
Criação do Active Directory	7 horas
Activação do nó Voto Electrónico/Votação	2005-02-07
Desactivação do nó Voto Electrónico/Votação	2005-02-20 (19H)
Apuramento dos resultados	2005-03-04 (11H)
Carregamento da BD dos votos via SVE	10 minutos
Programa de contagem	16 minutos
Número de votantes pelo SVE	4 367 (3%)
Votantes por correspondência	36 938 (25%)

3.1.2 Comentários sobre o processo

Forma de distribuir as credenciais. Reconhece-se que não houve tempo nesta simulação sequer para pensar em métodos alternativos de distribuição de credenciais. No entanto esse é um dos pontos mais críticos do ponto de vista das propriedades de um SVE. A autenticação por reunião de uma credencial enviada por correio com o número de eleitor, uma informação que não é propriamente secreta, não garante suficientemente a autenticidade, pelo menos por comparação com o método usado na votação presencial. Reconhece-se no entanto que não é muito diferente do nível de autenticidade que se obtém na votação por correspondência, em que vários boletins de voto são enviados na mesma carta. A situação é contudo problemática, pois o facto de a lista de credenciais ser gerada num só momento e depois ser enviada até à empresa de mailing em conjunto, constitui um ponto frágil que pode permitir uma fraude em escala significativa. Se um atacante obtivesse as credenciais e os respectivos números dos eleitores, que não são informação secreta, e se lhes antecipasse, mesmo que detectado por queixas de eleitores impedidos de votar, colocaria a CNE perante a decisão drástica de deixar correr ou anular a votação. Seriam de estudar hipóteses alternativas como o envio de credenciais por CD através dos postos consulares, o que significaria uma melhoria significativa face ao método actual.

Autenticação. A solicitação do número de eleitor no processo de autenticação configura uma situação de pouca garantia de anonimato, pelo menos aparente para o eleitor. Mesmo que uma entidade de certificação garantisse que o voto não é associado ao eleitor na BD, a desconfiança pode provocar o efeito de afastamento contrário ao pretendido.

Partição da chave privada. A gravação de um único CD com cada fracção da chave privada é provavelmente o ponto de maior risco para o sucesso do projecto, pois basta um dos CDs falhar para todos os votos se tornarem ilegíveis, uma vez que estão encriptados. Sugere-se um esquema em que cada membro da CNE fique com pelo menos dois bocados da chave para criar um nível de redundância. Note-se que a única função desta chave é permitir a desencriptação e correspondente contagem dos votos, não permitindo alterá-los.

Condições da votação. A votação não presencial comporta riscos para vários aspectos valorizados num processo de votação que importa referir, como é o caso da não coercibilidade, da privacidade e da própria autenticidade.

3.1.3 Comentários sobre a arquitectura de rede e servidores

Operação do SVE. O SVE não presencial foi operado pelo parceiro encarregado do seu desenvolvimento, o que é compreensível face ao calendário definido. Numa situação de

votação vinculativa tal não parece adequado, uma vez que boa parte da confiança no anonimato e invulnerabilidade da votação assenta na confiança dos operadores intervenientes. Da mesma forma que na votação por correspondência se confia no sistema de transporte de cartas, no SVE tem que se confiar nos ISPs que suportam a Internet e nos operadores do próprio SVE. Considera-se por isso que o SVE deveria ser operado pelo STAPE, o que, em conjunto com uma certificação por uma entidade idónea do software e do hardware efectivamente utilizados, forneceria a garantia de que o voto não é armazenado de alguma forma relacionável com o eleitor e que não é adulterado.

Ataques do exterior. Apesar de a comunicação entre o navegador Web do eleitor e o SVE ser sobre uma ligação segura, existem mecanismos que podem por em causa o anonimato e até a invulnerabilidade do voto. Um deles é a possibilidade de código malicioso (vírus, trojans) se alojar de forma generalizada em máquinas pessoais, das quais algumas possam ser usadas pelos eleitores, e actuar, no momento da votação, entre o navegador e a ligação segura, no sentido de alterar o voto ou quebrar o anonimato. Outra hipótese é da utilização da técnica *man in the middle*, em que um programa intercepta uma determinada comunicação, fazendo-se passar pelo interlocutor oposto relativamente a cada um deles e dessa forma enganando a ligação segura.

Servidor informativo. Identificaram-se várias falhas de segurança no nó Voto Electrónico/Info, através da execução de software de análise apropriado (tipo *nessus*). Se isto aparentemente não compromete o nó da votação, pode acontecer que um ataque àquele nó desvie os votantes para outros servidores sem que eles se apercebam disso, simplesmente provoque uma situação de negação de serviço que os leve a desistir, ou consiga obter informação indevida.

Aspectos de risco. A arquitectura seleccionada para esta experiência assentou em máquinas virtuais montadas em duas máquinas reais. Para o Frontend a arquitectura de acesso através de dois ISPs parece adequada, sendo o maior risco o de ter alguma indisponibilidade no SVE em caso de avaria. Para o Backend existe um risco semelhante em caso de falha, por exemplo, na BD. Foi afirmado que existia uma segunda máquina preparada para substituir o Backend em tal eventualidade, embora não esteja a funcionar em paralelo. O aspecto que se afigura mais crítico é o recurso a um único sistema de discos para armazenar os dados. Pese embora o facto de se tratar de um sistema em RAID5, poderia haver perda de informação no caso de corrupção da BD ou em caso de catástrofe. É de equacionar a possibilidade de um sistema de réplica em instalações fisicamente separadas. Note-se que as próprias cópias de salvaguarda só podem ser feitas na própria máquina, o que é imposto por configuração local, até ao momento do fecho.

Adulteração dos votos já registados. Se a confidencialidade do voto parece suficientemente garantida, o mesmo não se pode dizer da impossibilidade de adulterar votos já registados. A única coisa que impede a substituição de um voto por outro, também codificado, é a garantia de que o código do SVE não é malicioso, o que pode ser feito por certificação, e que ninguém tem acesso à BD do SVE. Isto requer procedimentos de segurança física dos servidores e de isolamento da rede em que operam, que parece terem sido seguidos na Novabase. Apenas quatro pessoas têm acesso às máquinas virtuais e os servidores encontram-se numa VLAN própria com firewall para o exterior e entre o Frontend e o Backend. Detectou-se aqui um ponto fraco que é o facto de estas redes não estarem fisicamente separadas. Como as máquinas estão fisicamente ligadas a um switch, a segurança do esquema lógico montado na realidade não é superior à segurança do próprio switch. A sala das máquinas é também sujeita a restrições de acesso, embora os servidores do SVE se encontrem no mesmo espaço de outros servidores. Os transaction logs da BD, que podem constituir um enfraquecimento do anonimato, permitem ajudar a detectar eventuais alterações directas da BD.

3.1.4 Comentários sobre o software

Registo na BD. A informação correspondente ao envio do voto pela Internet é constituída pelo nome de utilizador (parte da credencial que identifica o eleitor), opção escolhida (um carácter) e círculo eleitoral. Esta informação segue por uma ligação segura (https) estabelecida entre o cliente do eleitor e o servidor Web do SVE. Ao chegar aqui, vai, por uma ligação directa ao Backend, marcar o registo do eleitor no Active Directory como tendo votado, marcar o registo do eleitor na tabela de credenciais no mesmo sentido e registar o voto encriptado numa outra tabela independente.

Esta encriptação é feita com uma chave gerada para cada registo, a qual é ela própria guardada no registo encriptada com a chave pública. Esta técnica é considerada suficientemente segura para garantir a confidencialidade do voto até à fase da contagem.

É ao registar na BD que se efectua a dissociação entre utilizador e opção de voto, juntos em todo o percurso anterior. A informação nas tabelas de facto não permite qualquer ligação entre o registo do eleitor e o voto, mesmo encriptado, até porque a tabela de credenciais é armazenada através de uma função de dispersão (*hash*) que a desordena. No entanto, o funcionamento do servidor de BD faz registos de monitorização (*transaction logs*) que permitem reproduzir a actividade da BD e que são essenciais para garantir a recuperação do máximo de informação em caso de falha. O problema é que através da análise destes registos se pode refazer a ligação entre o utilizador e o voto,

que aparentemente se encontravam definitivamente desassociados. A situação agrava-se por ser possível ligar o nome de utilizador ao número do eleitor, no Active Directory. Esta é uma das razões pelas quais se apaga o Active Directory mal o Caderno Eleitoral deixa de ser necessário, isto é, no fecho da votação.

A razão pela qual existe a tabela de credenciais não é muito clara, para além de ser um registo redundante do estado do eleitor face ao Active Directory e poder facilitar o controlo de concorrência usando os mecanismos do SGBD que evitem o registo simultâneo de dois votos para o mesmo eleitor.

Processo de fecho. O processo de fecho inclui a cópia para CD do conteúdo da BD. Feita desta forma, a informação fica armazenada num formato específico do sistema de BD utilizado, o MS SQLServer, o que obriga a, no momento da contagem, voltar a carregar a informação para um sistema semelhante e só depois executar o programa de desencriptação e contagem. No entanto, o fecho deveria ser o último momento em que o carácter não malicioso do código fosse crítico. De facto, a partir do momento em que os votos encriptados são copiados para CD, o formato dos dados deveria ser aberto, no sentido em que não deveria depender de um formato privado de um fabricante de BD. Sugere-se que fique armazenado em XML, o que aliás já é parcialmente feito, pois esse é o formato dos registos dos votos encriptados. O programa de contagem ficaria assim independente do sistema de BD e dependeria apenas do conhecimento da chave privada particionada. Nesta perspectiva, a cópia do conteúdo da BD poderia ser entregue a várias entidades, por exemplo, aos partidos membros da CNE e vários programas de contagem poderiam confirmar os dados, sem qualquer prejuízo para o processo do SVE.

3.1.5 Comentários sobre a empresa de desenvolvimento

Idoneidade da empresa. A Novabase tem no seu currículo alguns projectos em que os aspectos de segurança são críticos, como sejam o desenvolvimento de software para bancos, sítios de comércio electrónico e aplicações do sector militar. É de esperar um nível técnico apropriado para a tarefa em causa. Os seus funcionários assinam uma declaração de confidencialidade. É de considerar a possibilidade de elevar as exigências de certificação do pessoal envolvido no eventual desenvolvimento do projecto para níveis semelhantes aos exigidos para colaborar em projectos militares da NATO.

Metodologia de desenvolvimento. A certificabilidade do software do SVE é facilitada pela existência de uma metodologia de desenvolvimento de software estabelecida e ela própria certificável. Embora o desenvolvimento de software na Novabase, em particular na sua divisão de Engineering, siga tais procedimentos, as condições em que foi lançado este projecto impediram a respectiva aplicação neste caso. A unidade que esteve envolvida foi a divisão de Consulting. Isso é patente, por exemplo, na exiguidade da

documentação técnica, o que só foi compensado pela boa vontade no fornecimento de acesso ao software desenvolvido. Antes de qualquer processo de certificação, aquele aspecto teria de ser corrigido.

3.2 Ocorrências imprevistas observadas durante o processo de votação

Dada a distribuição temporal e espacial do processo, há poucas ocorrências imprevistas observadas.

A activação do nó Voto Electrónico/Votação ocorreu no dia 2005-02-07. Registou-se um problema inicial com a publicação do endereço voto.votoelectronico.pt no servidor de DNS da FCCN o que provocava o aparecimento de uma caixa de diálogo relativa ao certificado digital. Esta questão foi ultrapassada no dia 2005-02-09.

Detectou-se, ao experimentar o processo de votação, que, se o navegador estivesse configurado para não aceitar *cookies*, uma situação normal para utilizadores com preocupações de segurança, a resposta obtida era a de indisponibilidade do servidor, o que induzia o eleitor em erro. Esta situação foi posteriormente corrigida, passando a ser apresentada uma mensagem indicando a razão do problema, mas sugerindo como solução a redução do nível de segurança do navegador, prática considerada criticável, uma vez que bastaria autorizar as cookies para o sistema se comportar da forma prevista.

A UMIC manteve um serviço de helpdesk com um número de telefone e atendimento em horário alargado, secundado pela equipa da Novabase, quando necessário. Registaram-se duas queixas, uma reportando o problema anterior e a outra referente a um problema de autenticação que não foi possível esclarecer por ausência de meio de contacto com o eleitor.

Embora a arquitectura do sistema previsse o acesso em linha dedicada em fibra óptica através de dois ISPs, um deles acabou por não activar o serviço a tempo.

3.3 Aspectos não auditados

Ficou por esclarecer se a função de hash utilizada na tabela das credenciais era unívoca ou podia provocar colisões.

Ficou por esclarecer se a função pseudo aleatória de geração das chaves não é facilmente reproduzível, o que retiraria eficácia a essa encriptação.

4 Análise das características do SVE

As características dos Sistemas de Voto Electrónico, ao nível da Segurança, Transparência, Usabilidade e Acessibilidade (referidos nos pontos seguintes), serão objecto de apreciação detalhada de seguida. A atribuição de pesos relativos aos vários atributos de Segurança, Transparência, Usabilidade e Acessibilidade, permitirá ainda definir o «Índice de viabilidade tecnológica», a incluir no relatório final.

4.1 Segurança (S)

Verificou-se a adopção de um conjunto de medidas, apreciável para o horizonte temporal do projecto, no sentido de garantir a segurança das comunicações e do armazenamento da informação no sistema central.

Esta experiência mostra que o paradigma da votação via Internet tem como pontos potencialmente mais fracos as componentes distribuídas para uso directo dos eleitores, os computadores pessoais, browsers, etc.

Os aspectos que mais preocupações levantam são a detectabilidade de eventuais tentativas de intrusão, a imunidade a ataques e o isolamento.

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

SEGURANÇA (S)							**Comentários**
S	**Auditabilidade**				x		
	O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.						É de salientar a boa vontade da empresa no fornecimento das fontes do projecto. No entanto, detectaram-se dois aspectos negativos: a utilização de bibliotecas de software de outros fabricantes, cuja fonte não foi fornecida ou não é conhecida; e o facto de não se ter seguido, dada a calendarização do projecto, uma metodologia de desenvolvimento de software formalizada, repetível e com controlo de qualidade, a qual constitui uma condição para a certificabilidade do produto. A componente distribuída não é facilmente auditável, devido à distribuição geográfica, que ultrapassa a jurisdição nacional, dos operadores envolvidos no processo, desde o browser cliente até aos operadores de telecomunicações.
S	**Autenticação do Operador**					x	
	Os utilizadores autorizados a operar o sistema devem ter mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjunção de alguns dos tipos de autenticação existentes. Por exemplo: cartão inteligente («Smartcard»), PIN ou senha, ou ainda autenticação bio-métrica – impressões digitais, retina ocular e voz.						Dado existir apenas um sistema central, existe apenas uma Mesa Eleitoral e os procedimentos de autenticação descritos, em conjunto com as outras circunstâncias do sistema, não merecem reparos.
S	**Certificabilidade**			x			
	O sistema deve poder ser testado e certificado por agentes oficiais.						O principal problema é a dificuldade em certificar o browser do Eleitor. Também não foram descritos mecanismos de auto-verificação do sistema que garantam que toda a configuração é a correcta. Como ponto positivo, refira-se a utilização no sistema central de uma arquitectura baseada em máquinas virtuais, que permite um maior controlo do ambiente em que cada componente opera.
S	**Fiabilidade**			x			
	O SVE deve funcionar de forma fiável, sem perda de votos.						Dois problemas graves na fiabilidade da solução apresentada: - só existia uma chave privada, repartida em sete pedaços,

							cada um gravado num CD e sob a responsabilidade dos membros da CNE e da CNPD; a contagem dos votos só é possível com a chave privada, pelo que uma falha num dos CDs faria perder toda a votação; - não se detectou um planeamento para recuperação de desastres, que exigiria um funcionamento em paralelo ou pelo menos um backup num segundo sistema fisicamente separado do primeiro, inclusive noutro edifício.
S	**Detectabilidade**		x				
	O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.						Não houve informação sobre nenhum alarme ou software de detecção de intrusão, para além dos logs das máquinas, no sistema central. Em particular não existia nenhuma máquina com ligação unidireccional à VLAN do backend que monitorizasse todo o tráfego no sentido de detectar padrões de uso suspeitos. Na componente distribuída, não se encontrou software para detecção, que avisasse algum administrador de sistema ou o próprio utilizador no caso de ocorrer um ataque ao sistema, no lado cliente.
S	**Disponibilidade do Sistema**				x		
	Durante o período eleitoral, o SVE deve estar sempre disponível para todos os actores legítimos, em particular para os eleitores votantes, para que o processo decorra normalmente.						Tanto quanto foi possível observar a disponibilidade do sistema foi alta, ao que ajuda o período alargado em que decorreu. Notou-se apenas uma indisponibilidade aparente que resultava de uma configuração inadequada no browser mas cuja mensagem de erro induzia o utilizador a pensar que se tratava de indisponibilidade e portanto tinha o mesmo efeito.
S	**Imunidade a Ataques**			x			

	Medidas de defesa contra fraudes, inclusive vindas dos próprios agentes que projectaram e desenvolveram o sistema, devem ser rigorosas e redundantes. Um SVE, tal como outros sistemas de alto risco, pode ser alvo privilegiado de ataques mal intencionados.	O facto de haver apenas um sistema de registo dos votos permite estabelecer mecanismos de segurança sofisticados. As medidas tomadas nesse sentido foram em geral satisfatórias. Ao nível da rede local, foram criadas VLANs próprias para as máquinas envolvidas, com parte dos equipamentos activos e passivos também dedicados e uma firewall para o exterior e outra entre o front-end e o back-end. A comunicação entre o servidor Web e o servidor de BD é feita com uma "connection string" própria e não é possível estabelecer ligações a partir de outras máquinas. Notou-se no entanto que o facto de não se terem usado redes fisicamente separadas e de as máquinas estarem ligadas a um switch, faz com que o nível de segurança do sistema não seja superior ao nível de segurança do switch, que não é um equipamento especialmente seguro e cujo comprometimento arrastaria o de todo o sistema. Idealmente, deveria ter havido uma ligação aos ISPs completamente autónoma da rede da empresa. No sentido de reduzir o impacto de ataques do tipo "denyal of service" e aumentar a disponibilidade, foi solicitada uma segunda ligação a um ISP, o qual não respondeu em tempo útil. Do ponto de vista de sistema operativo, houve o cuidado de inibir todos os serviços não essenciais ao funcionamento do SVE e, em particular, de inibir a possibilidade de fazer backups da BD para fora da máquina respectiva. O acesso ao sistema ficou restrito a quatro pessoas e só a partir de máquinas localizadas no edifício da empresa. No entanto, não foram relatadas medidas que impedissem uma alteração do conteúdo da BD por parte de um agente interno à equipa de operação. Mesmo que por análise de logs se descobrisse um ataque desse tipo seria difícil garantir que se conseguiam repor os votos originais. Assim, a concentração do registo dos votos num único sistema, que pode parecer uma vantagem do ponto de vista da facilidade de estabelecer políticas de imunidade a ataques, revela-se também um ponto especialmente vulnerável do sistema, em especial pelo carácter global que possui. Saliente-se a especial sensibilidade desta configuração do ponto de vista de decisão política pois, em

							caso de detecção de fraude, a única medida possível seria provavelmente a anulação completa da votação e não apenas numa mesa de voto numa freguesia. Do ponto de vista do componente distribuído colocam-se problemas complexos. O SVE funciona através de uma ligação https, que se considera segura. No entanto, identificaram-se dois tipos de ataques possíveis. O primeiro poderia resultar de uma colocação de código malicioso nas máquinas dos eleitores. O acto poderia ser especialmente dirigido a alguns eleitores, como forma de quebrar o anonimato, ou resultar de uma distribuição generalizada, estilo vírus, com o intuito de influenciar os resultados ou simplesmente atrapalhar a votação. Note-se que o carácter distribuído do método, que numa votação presencial torna complexa uma tentativa de fraude generalizada, no caso da Internet traz poucas garantias, dada a facilidade de nesta rede se afectar porções significativas dos nós a partir de um único centro. O código malicioso poderia assim actuar na máquina do eleitor, antes de a informação entrar no canal seguro. O segundo tipo de ataque poderia ocorrer a jusante, através da técnica "man-in-the-middle", em que um terceiro sistema se introduz no meio de uma comunicação entre dois sistemas, simulando para cada um deles ser o outro parceiro e podendo dessa forma consultar ou alterar o voto, ou simplesmente simular o voto convencendo o eleitor de que o efectivou, sem que isso efectivamente tenha acontecido. Este tipo inclui a variante de ataque ao DNS, mais ou menos sofisticado. Admitindo que muitos Eleitores recorram a motores de busca para encontrar o SVE, é de admitir que páginas que simulem o SVE possam fazer perder muitos votos, sem que o Eleitor se aperceba.
S	**Integridade dos Votos**				x		

	Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.						Descontados os problemas de imunidade a ataques já referidos, considera-se a integridade dos votos após a chegada da informação ao servidor Web do SVE. Cada voto é armazenado encriptado duplamente. Uma vez através de uma chave simétrica pseudoaleatória gerada no SVE, que garante que votos iguais ficam registados com aspecto diferente, e uma segunda vez através de uma chave pública que garante que os votos só podem ser contados na presença de uma chave privada. A integridade dos votos está assim, num primeiro momento, dependente da invulnerabilidade do software do SVE, o qual se admite virá a estar certificado. No entanto este método garante essencialmente o anonimato. De facto, alguém com acesso à BD poderia, chamando a API correspondente, forjar, modificar ou eliminar votos. Portanto, a integridade dos votos depende também do controlo de acessos à máquina do SVE. A partir do momento do fecho da votação, em que se faz uma cópia do conteúdo da BD para um ficheiro, que é selado com MD5, o problema da integridade dos votos muda completamente. Se existir apenas uma cópia desse ficheiro, qualquer substituição do mesmo é dramática. No entanto, nada obsta a que existam várias cópias, eventualmente distribuídas por várias entidades, o que garantiria não só redundância como dificultaria atentados à sua integridade. Esta distribuição não põe problemas de divulgação extemporânea dos resultados pois só com a chave privada a sua informação é legível. O passo da contagem dos votos ficaria assim muito menos crítico, pois, não havendo questões de confidencialidade, é admissível a existência de vários programas de contagem, sobre os mesmos dados. Nesta linha, sugere-se que o formato do ficheiro dos dados seja público (em XML, por exemplo), em vez de ser um formato de exportação da BD, específico de um determinado fabricante. Um tal ficheiro teria a vantagem de ser arquivável sem problemas de leitura futura.
S	**Invulnerabilidade**				x		
	A invulnerabilidade do SVE é a garantia de que não se pode aceder e alterar o sistema indevidamente.						Este aspecto já foi comentado implicitamente a propósito da integridade dos votos. A invulnerabilidade do sistema central é essencialmente garantida pelas restrições de acesso

							às máquinas, físicas e de software. A invulnerabilidade da componente distribuída é muito problemática.
S	**Rastreabilidade**				x		
	O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir registos ("logs") de entrada e saída de utilizadores não eleitores ou de quaisquer outros acessos, bem como registos do envio e recepção de dados, que obviamente não comprometam as restantes propriedades (anonimato e privacidade do eleitor).						Considera-se a rastreabilidade do sistema, na sua componente central, boa, em especial devido à existência de logs da BD e do sistema operativo. Não é praticável garantir o mesmo nível de rastreabilidade de eventos nos ISPs ou nas máquinas dos Eleitores.
S	**Recuperabilidade**				x		
	O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.						A recuperabilidade do SVE é no essencial a do SGBD utilizado (MS SQL Server). Estes sistemas estão projectados para possuírem boas características de recuperação, garantindo a atomicidade das transacções, o que evita incoerências entre o registo de votantes e o número de votos registado. Parte do mecanismo de recuperação assenta nos logs da BD, os quais não podem assim ser dispensados, apesar dos problemas de eventual quebra de anonimato que acarretam. A outra parte assenta num sistema de discos RAID para a BD, o que garante alguma redundância e capacidade de recuperação de falhas no disco. Seria desejável que, tal como referido na fiabilidade, existisse um backup numa instalação fisicamente distinta.
S	**Tolerância a Falhas**				x		
	Caso ocorra uma falha no sistema é possível recuperar o estado anterior e o funcionamento regular, assegurando um serviço aceitável.						Sobrepõe-se com o anterior. Para garantir que não há interrupção no serviço, seria necessário possuir um equipamento em hot standby. Existia de facto um equipamento suplementar para uma situação de emergência mas não em estado de agarrar o serviço automaticamente ao detectar uma falha no principal. A arquitectura adoptada de colocar várias máquinas virtuais numa mesma plataforma física (todo o backend) torna todo o SVE dependente de uma única máquina.
S	**Isolamento**			x			

	Só devem existir no SVE os dispositivos de interface externos absolutamente essenciais para o acto eleitoral, sendo todos os componentes certificados e iguais a um padrão, incluindo o software.						No sistema central, houve o cuidado de desactivar os serviços não essenciais e de isolar ao menos logicamente as máquinas envolvidas. Já o isolamento no componente distribuído é muito problemático (é possível até votar num cybercafé.)
S	**Segurança das comunicações**				x		
	As comunicações entre as assembleias de voto e o sistema central utilizam mecanismos de validação de identidade de ambos (assembleia e sistema central), de não adulteração da informação e de cifragem da mesma para garantir a confidencialidade, integridade e autenticidade.						Ver o ponto Imunidade a Ataques.

4.2 Transparência (T)

Na transparência as avaliações dos vários parâmetros são mais extremadas, mercê de algumas características inerentes ao paradigma de votação pela Internet com um nó central e de outras resultantes da falta de tempo para explorar alternativas.

Aspectos negativos: autenticação, documentação técnica, não coercibilidade, verificabilidade e transparência do processo.

Pontos positivos: a atomicidade, a precisão e a singularidade.

TRANSPARÊNCIA (T)							**Comentários**
T	**Anonimato**			x			
	A associação entre o voto e a identidade do eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam manutenção do sistema) quer após a votação (mesmo que por ordem judicial).						Ao nível de modelo de dados, a informação de que um Eleitor votou e qual o sentido do seu voto ficam em tabelas independentes e ainda no Caderno Eleitoral, em Active Directory. No entanto, os logs da BD podem permitir associar um voto a um Eleitor, uma vez que o seu objectivo é precisamente reconstruir a BD em caso de falha. A medida de não registar no Active Directory o nome do Eleitor, mas apenas o número, melhora ligeiramente este aspecto.
T	**Atomicidade**					x	
	Garantia de que, em caso de falha a meio do processo, não permanecem registos ou percepções inconsistentes relativos ao mesmo. Por exemplo: registos no caderno eleitoral de votantes, mas sem registos de voto no computador; o eleitor e a mesa ficaram com a percepção de que o voto se concretizou, quando na realidade não ficou nenhum registo no computador; falha de alimentação quando o votante confirma a opção de voto no computador, como se sabe se o voto foi concretizado (por forma a tornar os registos consistentes entre si e consistentes com a percepção das pessoas envolvidas)?						A atomicidade é garantida pela BD. O Eleitor, se tiver dúvidas sobre se chegou a votar ou não, por exemplo porque uma quebra de conectividade impediu a recepção da página de confirmação do voto, pode sempre tentar votar uma segunda vez. Se o registo tiver sido realmente efectuado, obtém-se uma mensagem de que o Eleitor já foi descarregado no Caderno Eleitoral.
T	**Autenticidade (método de autenticação do utilizador)**	x					
	Autenticar o indivíduo é o meio pelo qual a identificação de um votante é validada e confirmada. Apenas os eleitores autorizados devem poder votar. Exemplos de tipos de autenticação são: presencial, PIN, senha, certificado digital, cartão inteligente ou bio-métrica.						Após a geração de credenciais pelo SVE, códigos de 12 caracteres utilizados para identificar o Eleitor perante o SVE, estas são enviadas para uma empresa de mailing juntamente com os nomes e moradas dos Eleitores, para se proceder ao envio de cartas. As pessoas envolvidas neste processo, desde a geração ao envio, necessitam apenas de saber o número de eleitor, o segundo elemento de confirmação do pedido, o qual é semi-público, para poderem votar em vez do Eleitor. A decisão de utilizar, para o envio de credenciais, o método

								de distribuição de boletins de voto por correspondência aos emigrantes, é muito condicionadora deste tópico. Qualquer pessoa que receba a carta (seja ou não o Eleitor), se conseguir saber o número de eleitor correspondente, pode votar em vez dele. Ao Eleitor não adianta sequer protestar pois não há forma de saber se é o Eleitor que pretende fazer uma segunda votação.
T	**Confiabilidade**					x		
	O SVE deve funcionar de forma fiável e robusta, tornando-se confiável aos olhos dos diversos actores envolvidos, em particular o eleitor.							O sistema é considerado fiável e robusto, tendo-se apenas detectado um problema de má informação quando não conseguia colocar cookies, o que aparentava para os eleitores indisponibilidade de serviço.
T	**Documentação técnica**	x						
	Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema, devem estar documentados, devendo não conter ambiguidades e ser coerente.							A documentação técnica, mercê do prazo de desenvolvimento, é praticamente inexistente. A própria metodologia de desenvolvimento de software seguida foi muito simplificada, por essa razão.
T	**Integridade do Pessoal**				x			
	O pessoal envolvido no projecto, implementação, administração e operação do SVE deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.							Embora a empresa tenha alguma experiência de participação em projectos do sector militar, onde este tipo de questões se põe, nomeadamente ao nível da NATO, não foi identificado nenhum procedimento especial de verificação das características de integridade do pessoal envolvido com o desenvolvimento do SVE, a geração de credenciais, o envio do mailing, a operação do SVE, e a contagem dos votos, para além da exigência de confidencialidade relativa ao trabalho efectuado.
T	**Integridade do Sistema**				x			
	Deve ser possível garantir em qualquer momento que o SVE que está a ser usado é o mesmo que foi validado e certificado por auditores externos, pela Comissão Nacional de Eleições e pelos membros da mesa de voto, eventualmente por um processo de amostragem.							Não foi mencionada a existência de nenhuma ferramenta de verificação automática da configuração dos vários componentes de software de aplicação e de sistema em uso a cada momento. Mas como o sistema central é único, instalado em ambiente controlado e se utiliza uma arquitectura baseada em máquinas virtuais, esse aspecto é pouco relevante. O mesmo não acontece com o software a correr do lado do Eleitor em que a dificuldade de garantir a integridade do componente cliente do SVE, do browser em uso e do sistema operativo (em particular a inexistência de

							software malicioso) se considera um problema grave.
T	**Não-Coercibilidade**	x					
	O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.						Esta característica não é garantida.
T	**Precisão do SVE**					x	
	O sistema deve garantir que todos votos são adequadamente registados e contabilizados.						O registo dos votos é feito de forma atómica e individualizada e, a menos de ataques, o único problema detectado reside na eventual indisponibilidade momentânea do sistema, que pode ser ultrapassada em momento posterior. A contabilização também não oferece problemas.
T	**Privacidade**			x			
	O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.						Uma vez que o acto de votar não é em ambiente controlado, o Eleitor é livre de tornar público o seu voto. Mesmo pretendendo manter a sua privacidade, os métodos de ataque ao SVE referidos acima (código malicioso na máquina do Eleitor, "man-in-the-middle") e a análise dos logs da BD podem comprometê-la.
T	**Singularidade (Não Reutilização)**					x	
	O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.						A singularidade é garantida por uma dupla descarga no Caderno Eleitoral implementado no Active Directory e numa tabela da BD organizada por chave de dispersão com controlo de concorrência, o que impede duas votações simultâneas do mesmo utilizador
T	**Transparência do Processo**			x			
	Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.						A transparência do processo sofre de dois problemas principais. Por um lado, o eleitor tem que acreditar que o SVE regista correctamente o voto o que, sendo impossível de verificar pelo próprio, passa por um processo de certificação credível. Por outro lado, a obrigatoriedade de indicação do número de eleitor no próprio formulário de voto poderá levantar dúvidas justificadas sobre o anonimato e a privacidade, porventura inibidoras da participação no processo, as quais mais uma vez só poderão ser dissipadas por confiança num processo de certificação e na inexistência

								de software malicioso no caminho do browser para o sistema central. Sugere-se que a informação complementar fornecida pelo eleitor para autenticação dê garantias de não permitir, por si só, a sua identificação unívoca.
T	**Transparência do Sistema**				x			
	Todo o software, documentação, equipamento, micro-código e circuitos especiais devem poder ser abertos para inspecção e auditoria a qualquer instante. Deve ser conhecido o formato dos dados registados e transmitidos.							A transparência do SVE requer a existência de documentação adequada, incluindo a relativa à metodologia de desenvolvimento e aos testes efectuados. A transparência é limitada pela falta de controlo do ambiente de execução da componente distribuída. Reconhecem-se as vantagens de utilização de um SGBD para garantir as propriedades de singularidade e atomicidade do processo, durante a votação, o que significa que os dados estão num formato dependente do SGBD. Não se compreende a necessidade de manter os dados num formato de exportação específico desse SGBD após o fecho, em vez de num formato neutro, arquivável sem dependência do SGBD mas apenas dos algoritmos de encriptação.
T	**Verificabilidade**			x				
	O sistema deve permitir verificar que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a autenticidade dos registos dos votos, sem no entanto quebrar outras propriedades como o anonimato ou a privacidade do votante.							Na ausência de outro registo alternativo dos votos (em papel, por exemplo) a verificabilidade é uma propriedade muito interna ao SVE. Como no fim da votação se exporta o conteúdo da BD para um ficheiro, o qual é selado com MD5, se se admitir que a certificação garante a integridade dos votos até esse momento, a verificabilidade limita-se a garantir que o ficheiro pode ser lido por diferentes programas de contagem, uma vez conhecido o formato dos dados e a chave privada necessária para a desencriptação. A encriptação destina-se a garantir uma propriedade que não foi explicitamente considerada nesta grelha e que é a da confidencialidade dos resultados intermédios. Cada voto é encriptado com uma chave aleatória simétrica para esconder o valor e depois a chave é encriptada com uma chave pública assimétrica que só pode ser desencriptada com uma chave privada correspondente. Portanto, até esta chave ser conhecida, não é possível obter a distribuição dos votos. Uma vez conhecida, qualquer programa que implemente os algoritmos de desencriptação e conheça o formato dos dados está apto a verificar a contagem dos votos.

T	**Separação de papéis**			x			
	O fabricante do SVE, o instalador e o operador não devem ser da mesma instituição ou empresa. Os únicos operadores do SVE durante o acto eleitoral devem ser elementos da mesa de voto ou elementos previamente acreditados pela Comissão Nacional de Eleições.						Não houve separação de papéis, uma vez que o fabricante do SVE, o instalador e o operador de todas as fases do processo foi a mesma empresa, sendo apenas de salientar a presença de elementos da CNE, da UMIC e da CNPD em certos momentos chave.

4.3 Usabilidade (U)

Relativamente à usabilidade, ela foi considerada em geral elevada, não tendo sido detectados problemas de maior.

USABILIDADE (U)							**Comentários**
U	**Facilidade de uso**				x		
	O sistema deve ser de uso fácil, quer para eleitores quer para operadores (membros da mesa de voto).						Em geral o sistema é fácil de usar, para os Eleitores e para os operadores, sendo que estes devem incluir alguém com competência técnica para algumas operações, nomeadamente na obtenção do Caderno Eleitoral, na configuração dos Círculos Eleitorais e nos backups da BD.
U	**Rapidez de uso**					x	
	O sistema deve ser de uso rápido, quer para eleitores quer para operadores (membros da mesa de voto).						Para o Eleitor já conhecedor do SVE, a votação pode demorar menos de um minuto. Do ponto de vista dos operadores, a operação mais demorada é a geração de credenciais e a criação do Active Directory. A operação de contagem demorou cerca de 20 minutos.
U	**Clareza da Linguagem na Interface**			x			
	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.						A definição dos círculos eleitorais é por configuração de ficheiros e não por uma interface apropriada, o que poderá exigir algum treino. Apesar da simplicidade da interface do Eleitor, admite-se que as pessoas que nunca tenham usado a Web experimentem alguma dificuldade no uso do SVE.
U	**Localização da Interface**			x			
	A localização, orientação e altura do monitor, bem como dos restantes dispositivos de interacção, devem ser apropriadas ao eleitor.						Dependente do próprio Eleitor.
U	**Satisfação emocional**				x		
	O sistema deve ser atraente e agradável de usar.						O contexto da utilização e o resultado do inquérito aos 12% (4.367) dos votantes por correspondência que também votaram pela Internet apontam para satisfações acima dos 90%. Este valor deve no entanto ser temperado com a polarização do universo de respostas e com as dúvidas sobre a segurança do mesmo (só 57,80% consideram seguro).

4.4 Acessibilidade (A)

É nos aspectos relativos à acessibilidade que se pode jogar uma boa parte das decisões para o futuro devido ao carácter mais subjectivo dos diversos factores.

Pontos negativos: desigualdade dos eleitores na literacia informática e na facilidade de acesso à Internet.

Pontos positivos: conveniência e mobilidade.

ACESSIBILIDADE (A)							**Comentários**
A	**Conveniência**					x	
	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.						Este é um dos pontos mais fortes do método.
A	**Direito de Voto**			x			
	O direito de voto deverá poder ser efectivamente exercido se um eleitor verificar simultaneamente as propriedades de Autenticidade e Singularidade.						Admite-se que haja problemas no método de distribuição das senhas de acesso, por correio, sem tempo para reclamações, o que limita o direito de voto.
A	**Documentação para eleitor**				x		
	O eleitor deve ter acesso com a antecedência adequada a informação de compreensão simples sobre o SVE e as suas características.						Embora sem grande antecedência, a informação sobre o SVE é em geral clara e fácil de entender, embora talvez pudesse alertar os Eleitores para a necessidade de instalar antivírus.
A	**Flexibilidade**		x				
	Os equipamentos de votação que fazem parte do SVE devem suportar uma variedade de questões relacionadas com o processo de votação, com por exemplo a utilização por pessoas com necessidades especiais, analfabetas, etc.						A dificuldade de utilização do SVE por parte de Eleitores com níveis elevados de iliteracia informática é um dos aspectos a ultrapassar, sob pena de se promoverem desigualdades de base económica ou cultural.
A	**Mobilidade**					x	
	O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.						Não há restrições.

4.5 Características transversais e outros aspectos (O)

Embora sem entrar em detalhes, é de salientar a escalabilidade deste SVE e o relativamente baixo custo de uma sua implementação.

Características transversais e outros aspectos (O)							**Comentários**
				-		+	
O	**Viabilidade (Custo/Beneficio)**						
	O SVE deve ser eficiente e viável economicamente.						Não existem dados suficientes para avaliar este aspecto. No entanto no relatório final global de auditoria da FEUP serão apresentadas algumas considerações sobre o assunto.
				-		+	
O	**Escalabilidade do Sistema**					x	
	A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.						Admitindo que a votação pela Internet se fará sempre em períodos relativamente alargados, não são previsíveis problemas significativos em termos de escalabilidade, com a tecnologia actual.

4.6 Quadro Resumo da Apreciação

			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

5 Conclusões e Recomendações

5.1 Conclusões

A experiência analisada permite concluir que, do ponto de vista técnico, a votação pela Internet compara favoravelmente com a votação por correspondência e permite contribuir para o objectivo que norteia o projecto do Voto Electrónico de facilitar e promover a participação dos cidadãos nos processos de votação. Esta conclusão é sujeita a duas principais ressalvas:

- A verificação de uma adesão de apenas 3% à votação no SVE, por comparação com 25% no voto por correspondência, não é considerada significativa, dado o carácter não vinculativo daquele. Não é possível determinar a eventual influência de factores sociológicos no nível de adesão em situação vinculativa.
- O projecto necessita de revisão significativa, nomeadamente na melhoria das facilidades de configuração de uma votação específica; no processo de distribuição de credenciais; no aumento de segurança relativamente aos aspectos de operação do sistema e de ataques nos computadores dos eleitores; e de redução dos factores de risco de perda de informação na repartição da chave privada e no armazenamento dos dados. O surgimento de dúvidas relativamente à autenticidade, ao anonimato ou à integridade dos votos poderia ser contraproducente para o fim pretendido.

Relativamente a uma comparação com a votação presencial, o SVE não presencial, no seu estádio actual de desenvolvimento, apresenta muitas debilidades que desaconselham a sua adopção.

5.2 Recomendações

As recomendações relativas ao SVE da Novabase são as seguintes:

- A redefinição do modelo de gestão do SVE, de forma a garantir uma efectiva separação de papéis, com a atribuição da operação a uma equipa dependente da CNE e não da empresa fabricante;
- Revisão da arquitectura técnica de forma a garantir redes fisicamente separadas, dedicadas ao projecto, com interligação apenas por firewalls. O

sistema deverá funcionar de forma a armazenar os dados em duas instalações em edifícios distintos, em hot standby ou com balanceamento de carga;

- A fiabilidade do sistema deve ser aumentada, em particular na forma de armazenamento da chave privada de encriptação dos dados;
- O ficheiro resultante da exportação dos dados no fecho da votação deve ter um formato aberto e neutro.
- 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.

.