# *Relatório de Consultadoria*

*(No âmbito do experiência piloto de Votação Electrónica efectuada a 13 de Junho de 2004)*

André Ventura Zúquete
IEETA / UA

Paulo Jorge Pires Ferreira
INESC ID / IST

26 de Julho de 2004

## Sumário Executivo

Este documento apresenta os aspectos fundamentais resultantes da avaliação científica e tecnológica efectuada às soluções de votação electrónica que foram utilizadas na experiência piloto de 13 de Junho de 2004. A equipa de consultores é formada por: Prof. Paulo Ferreira INESC ID / IST e Prof. André Zúquete do IEETA / UA.

A avaliação científica e tecnológica das soluções em causa foi feita com base nos documentos que nos foram cedidos pelas empresas. Esses documentos descrevem fundamentalmente aspectos macroscópicos de funcionamento dos sistemas e possuem muito pouca informação acerca da sua realização (algoritmos usados, realização dos mesmos, controlo da sua correcção, etc.). Assinalamos que para aceitação de um sistema final toda a documentação em falta, bem como exemplares das máquinas usadas, teriam que ser fornecidos para avaliação pela equipa de auditoria.

As soluções foram avaliadas com base em propriedades básicas (correcção, democracia, etc.), robustez, usabilidade e mais-valias em relação à votação tradicional (i.e. com boletins em papel). Com base no historial das empresas em causa pensamos que, de uma forma genérica, as soluções tecnológicas apresentam um grau de confiança razoável. No entanto, note-se que tal não nos é permitido concluir, antes pelo contrário, com base na documentação apresentada. Assumindo que estes documentos são apenas uma primeira apresentação dos sistemas, será necessário no futuro ter acesso a mais informação e, em particular, ao próprio software e hardware. Neste caso, há aspectos de propriedade intelectual que as empresas, compreensivelmente, quererão concerteza assegurar, impedindo que caiam no domínio público. Coloca-se assim a questão de qual a disponibilidade que as empresas em causa, ou quaisquer outras, poderão de facto demonstrar em termos de disponibilizar a informação necessária.

A mais-valia dos sistemas em consideração, quando comparada com a solução actual (i.e., tradicional, baseada em papel) é muito reduzida, uma vez que se limita, *grosso modo*, a apresentar uma interface (talvez) mas agradável ao votante e a potenciar a diminuição do tempo de apuramento dos resultados. Nenhum destes aspectos nos parece justificar o investimento, por mais reduzido que seja, nas tecnologias em causa. Com efeito, na nossa opinião, uma solução de cariz informático justifica-se se permitir a mobilidade do votante, i.e. se for permitido que este exerça o seu direito de voto num local que não a mesa de voto por onde se encontra registado.

No que diz respeito aos sistemas de votação electrónica no geral, há basicamente duas opções: uma que se baseia na utilização de soluções cujo acesso é restrito, outra (dita "*open-source*") que assume a total abertura no acesso às soluções hardware e software. Pensamos que este aspecto deverá ser alvo de uma ampla discussão, não limitada às entidades com capacidade científica e tecnológica, i.e. deverá deverá abranger a sociedade em geral.

# Índice

# 1 Introdução

Este documento apresenta os aspectos fundamentais resultantes da avaliação científica e tecnológica efectuada às soluções de votação electrónica que foram utilizadas na experiência piloto de 13 de Junho de 2004.

A equipa de consultores é formada por: Prof. Paulo Ferreira INESC ID / IST e Prof. André Zúquete do IEETA / UA.

Antes de mais, é importante notar que a equipa de consultores entende a experiência piloto realizada nas eleições Europeias do 13 de Junho como o início de um processo longo e que requer muito cuidado na sua possível extensão. Em particular, os prazos impostos pela UMIC possibilitam apenas uma primeira análise das soluções em causa. No entanto, julgamos que este processo é sem dúvida um passo na direcção certa.

Os subscritores deste documento vêm-no como o embrião de um trabalho de consultadoria a ser prestado pelas instituições de investigação a que pertencem. Esse trabalho é, por várias razões, extremamente complexo do ponto de vista científico e tecnológico mas também do ponto de vista social, uma vez que está em causa a confiança que a sociedade em geral pode ter (ou não) numa solução deste tipo para efeitos de eleições numa sociedade democrática com é a Portuguesa. Assim, algumas das questões aqui abordadas são de cariz geral não estando directamente e apenas relacionadas com a experiência piloto antes referida.

Há ainda a notar que a avaliação científica e tecnológica das soluções em causa foi feita com base nos documentos que nos foram cedidos pelas empresas. Esses documentos descrevem fundamentalmente aspectos macroscópicos de funcionamento dos sistemas e possuem muito pouca informação acerca da sua realização (algoritmos usados, realização dos mesmos, controlo da sua correcção, etc.). Assinalamos que para aceitação de um sistema final toda a documentação em falta, bem como exemplares das máquinas usadas, teriam que ser fornecidos para avaliação pela equipa de auditoria.

Por fim, é de notar que os documentos acima referidos foram enviados à equipa de consultadoria na sequência de um documento[1] elaborado por esta no qual se referem os elementos fundamentais a ser facultados pelas empresas em causa.

Este documento está organizado do seguinte modo. Na secção 2 apresentamos os aspectos básicos subjacentes às eleições. Na secção 3 apresentamos as soluções que foram utilizadas nas experiências piloto. Na secção 4 é resentada uma avaliação da interface de um sistema de votação (o da Unisys) com os utentes. A secção 5 apresenta as conclusões finais.

[1] "Votação Electrónica - (reflexão inicial no âmbito da experiência piloto de votação electrónica agendada para 13 de Junho e coordenada pela UMIC)".

## 2 Eleições: aspectos a ter em consideração

Todos os sistemas de votação electrónica devem incluir as quatro seguintes propriedades básicas, acordadas ao longo de duas décadas de investigação:

1. **Correcção**: (i) os votos expressos não podem ser alterados, (ii) os votos válidos não podem ser eliminados na contagem final e (iii) a contagem final não pode incluir votos inválidos.

2. **Democracia**: (i) só os votantes autorizados podem participar numa eleição e (ii) cada um desses votantes só pode votar uma vez nessa eleição.

3. **Privacidade**: (i) ninguém deverá ser capaz de associar votos a votantes e (ii) nenhum votante deverá ser capaz de demonstrar como votou perante terceiros.

4. **Verificabilidade**: (i) qualquer votante pode verificar independentemente que todos os votos foram contados correctamente e (ii) que o seu voto não foi ignorado.

Nas eleições tradicionais a correcção, democracia e verificabilidade são asseguradas por mesas e comissões eleitorais compostas por representantes de interesses antagónicos. A privacidade é assegurada por gabinetes de voto isolados e por urnas fechadas.

Algumas destas propriedades são mais “fortes” do que as que são asseguradas nos sistemas eleitorais tradicionais, com urnas e boletins de voto em papel. Um exemplo é a verificabilidade que, nos sistemas tradicionais, é feita por representantes das forças em confronto. No entanto, a verificabilidade é aconselhável para reforçar a segurança no sistema. Com efeito, qualquer pessoa consegue perceber como funciona o sistema tradicional e como se assegura o seu funcionamento rigoroso. Num sistema informático tal não é possível; o sistema só é compreensível para uma pequena minoria, e mesmo parte desse pequeno grupo de pessoas não é normalmente capaz de provar ou assegurar a total correcção do sistema. É por este facto que é tão importante a verificabilidade, porque ela é fundamental para garantir ao votante comum que o resultado do sistema pode, em parte, ser auditado por si mesmo.

Algumas destas propriedades podem ou não ser contraditórias consoante o modo como são facultadas. Por exemplo, a capacidade de um votante verificar se o seu voto não foi ignorado na contagem final (e que foi correctamente interpretado nessa contagem) pode colidir com a (desejável) incapacidade de um votante demonstrar como votou perante terceiros. Ou seja, se o processo de verificação revelar de alguma forma o voto de um votante, o processo de verificação deverá ser protegido da coação por terceiros.

A execução real de um protocolo de votação electrónica requer que o mesmo seja robusto, i.e. que seja capaz de tolerar diversos tipos de falhas

operacionais. A robustez deve assegurar as seguintes propriedades, que não se encontram na maioria dos protocolos publicados e protótipos realizados:

1. **Resistência ao conluio**: nenhuma das entidades controladoras da eleição, isoladas ou até um certo grau de conluio, podem introduzir votos por outrem ou impedir de votar os votantes autorizados. Esta propriedade deve ser avaliada em termos da fracção mínima de entidades honestas necessárias para garantir a impossibilidade de fraude em conluio.

2. **Disponibilidade**: (i) o sistema de votação funciona correctamente durante o período de votação e (ii) todos os votantes têm a oportunidade de votar durante todo esse período.

3. **Capacidade de interrupção e continuação**: o sistema permite que qualquer votante interrompa o processo de votação, por vontade própria ou por imposição de uma falha, e a retome mais tarde durante o período de votação.

4. **Capacidade de protestar anonimamente**: como antes se referiu, se o sistema permitir verificabilidade, cada votante pode detectar erros de contagem relativos ao seu voto. Neste caso o sistema deverá permitir a capacidade dos votantes protestarem anonimamente para que seja feita a correcção adequada.

5. **Capacidade de auditoria durante a eleição**: durante a eleição podem surgir problemas que impeçam votantes de votar. Para resolver tais situações o sistema deverá incluir uma componente de arbítrio que deverá tratar as reclamações dos votantes e ser capaz de detectar falhas operacionais ou fraudes que estejam a afectar os votantes que reclamam.

6. **Capacidade de auditoria após a eleição**: se após a conclusão da eleição se detectarem erros devidos a falhas técnicas ou fraude o sistema deverá ser capaz de permitir uma auditoria tão completa quanto possível que, sem violar a privacidade dos votantes, permita recolher os elementos necessários para explicar o sucedido. A auditoria deverá ainda, tanto quanto possível, ter a possibilidade de corrigir o resultado final como se não tivesse surgido qualquer problema, porque não é normalmente aceitável a repetição de eleições em larga escala.

Para que o sistema de votação electrónica seja aceito pela comunidade de votantes devem ainda ser considerados na sua realização diversos critérios de usabilidade, nomeadamente:

1. **Facilidade de registo dos votantes**: o processo de registo dos votantes deverá ser tão simples quanto possível. Esse registo deverá ainda poder facultar o acesso dos votantes registados a diversas eleições, mas não necessariamente a todas. Ou seja, por cada eleição poderão participar um subconjunto dos votantes registados, mas o

mesmo registo poderá ser usado para diversas eleições em que o votante esteja autorizado a participar.

2. **Facilidade de autenticação dos votantes no acto de votação**: admitindo que os votantes serão em grande maioria pessoas pouco habituadas ao uso de tecnologias informáticas, o processo de autenticação deverá ser o mais simples possível para evitar a info-exclusão. No entanto, a simplicidade não deverá ser entendida como sinónimo de mecanismos simples e fracos em termos de segurança, mas apenas como mecanismos robustos com o mínimo de intervenção dos votantes e com o menor grau possível de personalização.

3. **Robustez do mecanismo de autenticação**: como se pretende idealmente que um votante registado participe em várias eleições usando os mesmos mecanismos de votação, o mecanismo de autenticação não deve ser substancialmente enfraquecido pela sua utilização em diversos actos eleitorais. Também se deve evitar que os votantes menos cuidadosos ou sensibilizados para o problema da segurança possam, deliberada ou involuntariamente, divulgar algo acerca da sua própria autenticação que possa ser usado por terceiros para os personificar.

Finalmente, as mais-valias inerentes à utilização de um protocolo de votação electrónica devem ser manifestamente superiores às dos sistemas clássicos. Com efeito, só desse modo é possível demonstrar à sociedade que o investimento numa infra-estrutura tão complexa e crítica, do ponto de vista social, serve para mais do que para acelerar a contagem de votos. Assim, os seguintes aspectos devem ser tomados em consideração, na utilização de soluções de índole informática no suporte de eleições:

1. **A possibilidade de voto remoto em secções de voto alheias**: o sistema deverá permitir que um votante possa exercer o seu direito em qualquer assembleia de voto, e não só naquela onde se encontra registado. Este aspecto poderá ser decisivo para diminuir a abstenção devida à ausência, forçada ou voluntária, do local normal de voto (tradicional).

2. **A possibilidade de voto remoto em qualquer lugar**: o sistema deverá permitir que um votante possa exercer o seu direito em qualquer lugar, e não só em assembleias de voto. Este mecanismo deverá ser facultado para situações onde não seja viável aceder fisicamente a assembleias de voto, uma vez que estas fornecem uma maior protecção contra a coação.

Existe um conjunto de outros aspectos que, numa perspectiva mais abrangente da votação electrónica, deverão ser equacionados. De uma forma não exaustiva, apresentamos em seguida os que, por agora, nos parecem ser mais relevantes:

- Solução "*open-source*" vs. código total ou parcialmente secreto.
- Custo da solução e impacto no tecido universitário/industrial português.
- Facilidade e flexibilidade no âmbito da elaboração de boletins de voto.

- Possibilidade de implantação de uma rede nacional de apoio à votação electrónica que possa ser usada para todas as eleições e consultas de opinião.

Assim, de uma forma concisa, os requisitos de uma eleição são os seguintes:

| **Propriedades Básicas** | **Robustez** | **Usabilidade** | **Mais Valias** |
|---|---|---|---|
| Correcção | Resistência ao conluio | Facilidade de registo dos votantes | |
| Democracia | Disponibilidade | Facilidade de autenticação dos votantes no acto de votação | Possibilidade de voto remoto em secções de voto alheias |
| Privacidade | Capacidade de interrupção e continuação | Robustez do mecanismo de autenticação | Possibilidade de voto remoto em qualquer lugar |
| Verificabilidade | Capacidade de protestar anonimamente | | |
| | Capacidade de auditoria durante a eleição | | |
| | Capacidade de auditoria após a eleição | | |

# 3 Soluções Avaliadas

Nesta secção apresentamos a avaliação efectuada pela equipa de consultadoria às três soluções em causa que foram disponibilizadas pelas empresas Indra, Multicert e Unysis.

## 3.1 **Indra**

O sistema avaliado foi a plataforma de votação electrónica denominada Point&Vote, desenvolvida pela Indra. A documentação fornecida sobre o mesmo consta do Anexo I. Os comentários que se seguem foram feitos tendo em conta exclusivamente essa documentação e assumindo a correcção implícita das acções efectuadas pelas várias componentes usadas. No entanto, essa correcção terá se ser igualmente auditada se o sistema alguma vez for considerado para uso.

### 3.1.1 Arquitectura

O sistema Point&Vote consiste numa máquina de voto que contempla hardware próprio e de terceiros assim como o respectivo software. A máquina de voto consiste basicamente num computador pessoal destacando-se o ecrã táctil e o leitor de *smart cards* (i.e. cartões inteligentes).

1. **Cabine de Voto**. Esta componente substitui o processo tradicional de preenchimento do boletim em papel. O Eleitor coloca o cartão inteligente (que lhe foi cedido pela mesa) na máquina, de modo a identificar-se como votante válido, podendo em seguida expressar o seu voto. A Cabine de Voto possui um ecrã sensível ao toque que serve para efectuar a votação. No final da votação, a Cabine de Voto guarda o voto de uma forma segura.

2. **Cartão Inteligente do Administrador**. Este cartão, em conjunto com uma palavra-chave, permite ao Administrador do sistema identificar-se perante a máquina de voto e aceder às funções de administração (menu do administrador); estas funções são as seguintes: abrir mesa, impressão de resultados, transmissão de resultados, parâmetros de transmissão, e desligar máquina. Destas funções, há duas que se destacam: a função impressão de resultados permite verificar que, por exemplo, antes da eleição ter início não há votos guardados na máquina; a função abrir mesa, tal como o nome sugere, permite dar início à votação.

Portanto, o processo de votação é em tudo idêntico ao que se usa actualmente apenas com a diferença que o boletim de voto é preenchido na máquina de voto ficando os votos guardados de forma digital nessa mesma máquina.

O sistema operativo que existe na máquina de voto é o Windows 2000. É por cima deste sistema operativo que se executa a aplicação que permite que os votantes votem e que os respectivos boletins sejam armazenados em ficheiros. Portanto, o hardware e o software que constituem a máquina de

voto têm componentes que são desenvolvidos pela Indra mas também por terceiros. O software desenvolvido pela Indra é em Visual Basic.

No documento fornecido pela Indra não são feitas referências à utilização de técnicas para cifrar os votos quando estes se encontram armazenados na máquina de voto. Apenas se menciona a utilização de palavra-chave para identificação do administrador do sistema.

No mesmo documento é feita referência à possibilidade de ser transmitida via rede o ficheiro com os resultados acumulados da votação efectuada e que se encontra na máquina de voto. Não consideramos essa possibilidade na nossa avaliação uma vez que a experiência piloto que foi efectuada não contemplou esta funcionalidade.

### 3.1.2 Avaliação

**Correcção**

É afirmado, no documento da Indra, que a coerência dos resultados (embora não se defina de forma precisa o que isto significa) é conseguida através do registo de toda a actividade do sistema o que assegura a sua fidelidade e a ausência de intromissões nos mesmos. No entanto, não é claro como isto é conseguido pois nada é dito do ponto de vista técnico (e.g. utilização de criptografia).

**Democracia**

Assegurar que só os votantes autorizados possam participar numa eleição é algo que depende apenas do controle efectuado pelos presentes uma vez que a atribuição do cartão inteligente a um votante é efectuado do modo tradicional. O mesmo se pode dizer em relação ao número de vezes que um votante é autorizado a votar; em particular, não é descrito nenhum mecanismo que detecte a utilização repetida do cartão inteligente várias vezes pelo mesmo votante.

**Privacidade**

A privacidade dos dados é conseguida pois a máquina de voto não guarda nenhum registo que permita associar o votante com o voto. No entanto, nada é dito como isto é assegurado; por exemplo, basta que os votos sejam guardados em ficheiro de forma sequencial para que se saiba qual o voto do primeiro eleitor, do segundo, etc.

Nenhum votante consegue demonstrar como votou perante terceiros porque no final do processo não fica com qualquer informação relativa à sua participação no processo eleitoral.

**Verificabilidade**

Nenhum votante pode verificar independentemente que todos os votos foram contados correctamente. Nenhum votante consegue verificar independentemente que o seu voto não foi ignorado.

**Resistência ao conluio**

Nenhuma das entidades controladoras da eleição, isoladas ou até um certo grau de conluio, podem introduzir votos por outrem ou impedir os votantes autorizados de votar. Esta propriedade é assegurada, *grosso modo*, pela semelhança com o processo de controlo eleitoral tradicional em papel, onde os elementos da mesa se controlam mútua e presencialmente.

**Disponibilidade**

Não é possível garantir que o sistema de votação funciona correctamente durante o período de votação. Com efeito, o sistema não possui qualquer redundância, bastando que qualquer uma das suas componentes falhe durante a eleição para comprometer localmente a mesma. Apenas é considerada a capacidade de resistência a falhas de energia eléctrica e problemas no ambiente (e.g. humidade). No entanto, uma vez efectuados os procedimentos de recuperação, é razoável admitir que a máquina de voto em causa possa voltar a ser utilizada. No entanto, nada é dito sobre o que sucede aos boletins de voto entretanto já armazenados.

**Capacidade de interrupção e continuação**

Nada indica que seja impossível um eleitor interromper o processo de voto e continuá-lo mais tarde. Note-se que para tal é preciso que haja a concordância dos elementos da mesa.

**Capacidade de protestar anonimamente**

O sistema, por imposição expressa da UMIC, não permite verificabilidade, logo cada votante não pode detectar erros de contagem relativos ao seu voto. Consequentemente, o sistema também não prevê quaisquer capacidades dos votantes protestarem, anonimamente ou não, para que sejam feitas correcções

**Capacidade de auditoria durante a eleição**

Não foram previstas quaisquer capacidades de auditoria durante a eleição. Uma elementar, por exemplo, consistiria num cruzamento regular entre o número de autorizações dadas e o número de votos guardados.

**Capacidade de auditoria após a eleição**

É possível efectuar uma auditoria final, i.e. depois da eleição ter terminado, uma vez que depois de efectuar o fecho da mesa (função efectuada pelo administrador) é possível imprimir os resultados da votação.

**Facilidade de registo dos votantes**

O sistema não considera este aspecto.

**Facilidade de autenticação dos votantes no acto de votação**

O sistema não trata deste aspecto. Assim, é usado o processo habitual de autenticação de votantes dos sistemas baseados em papel.

**Robustez do mecanismo de autenticação**

O sistema não contribuiu nem positiva nem negativamente neste aspecto.

**Possibilidade de voto remoto em secções de voto alheias**

O sistema actualmente não contempla esta possibilidade.

**Possibilidade de voto remoto em qualquer lugar**

O sistema actualmente não contempla esta possibilidade.

### 3.1.3 Comentário geral

O sistema parece ter sido feito para ser operacionalmente semelhante aos tradicionais baseados em papel. O resultado é um sistema que pode transmitir algum conforto ao votante, que vê no mesmo um funcionamento algo semelhante ao que porventura já se habituou a ver nos sistemas clássicos.

As normas que são respeitadas pelos equipamentos e que foram seguidas no desenvolvimento, assim como as certificações que foram obtidas, tal como é indicado no documento apresentado pela Indra, permitem aumentar a confiança na qualidade da solução apresentada. No entanto, note-se que o controlo destas normas e certificações no que diz respeito a equipamento e software de terceiros, não é responsabilidade da Indra. Assim, uma vez que de facto são utilizados componentes de terceiros, a questão da confiança na correcção do sistema é dependente destes e terá, portanto, de os considerar.

É ainda de referir que grande parte das afirmações feitas em termos de correcção, privacidade, etc. das eleições efectuadas com a tecnologia providenciada pela Indra não está devidamente fundamentada no documento respectivo. Assim, não querendo de forma alguma pôr em causa a qualidade do sistema em consideração, pensamos que, com base na documentação que nos foi fornecida, e uma vez que esta não apresenta a correspondente fundamentação, a máquina de voto não apresenta as devidas garantias de segurança para o efeito. Claro que esta conclusão pode ser alterada caso seja fornecida mais informação; no entanto, devemos referir que a dependência de terceiros e, em particular, a utilização de um sistema operativo de tão grande complexidade como o Windows aumenta em muito a probabilidade dos requisitos de segurança não sejam respeitados.

## 3.2 **Multicert**

O sistema avaliado foi a plataforma de votação electrónica voto@PT, desenvolvida pela MULTICERT S.A./PT Inovação. A documentação fornecida sobre o mesmo consta do Anexo II. Os comentários que se seguem foram feitos tendo em conta exclusivamente essa documentação e assumindo a correcção implícita das acções efectuadas pelas várias componentes usadas. No entanto, essa correcção terá de ser igualmente auditada se o sistema alguma vez for considerado para uso.

### 3.2.1 Arquitectura

A plataforma voto@PT é constituída pelas seguintes componentes:

1. **Mesa de Voto**. Esta componente substitui o caderno eleitoral, que passa a ter um formato puramente electrónico. Cada elemento da Mesa tem um cartão inteligente de identificação que lhe permite pesquisar os votantes no caderno eleitoral electrónico, assim como indicar qual o estado do eleitor (em votação, já votou, ainda não votou) através do registo do eleitor no caderno eleitoral electrónico.

2. **Boletim de Voto**. Esta componente é um cartão inteligente que substitui o tradicional boletim em papel. O eleitor, após a sua identificação pela Mesa de Voto e se autorizado a votar, recebe um cartão inteligente que usa para votar.

3. **Cabine de Voto**. Esta componente substitui o processo tradicional de preenchimento do boletim em papel, que é substituído por um cartão inteligente. O eleitor usa a Cabine de Voto para colocar nesse cartão inteligente o seu voto. A Cabine de Voto possui um ecrã sensível ao toque que serve para efectuar a votação. No final da votação, a Cabine de Voto guarda o voto de uma forma segura no cartão inteligente.

4. **Urna Electrónica**. Esta componente substitui a urna tradicional e permite aos eleitores depositarem o seu Voto Electrónico para posterior contagem. Para tal, os eleitores colocam o cartão inteligente com o Voto no leitor de *chipcard* da Urna Electrónica, sendo o mesmo transferido e arquivado pela Urna Electrónica. Após arquivar o Voto, a Urna Electrónica apagará do cartão inteligente toda e qualquer informação do Voto, ficando pronto a ser reutilizado por outro eleitor.

5. **Cartões inteligentes da mesa (Presidente e Escrutinadores)**. Estes cartões, um por cada elemento da mesa, são iniciados quando o sistema é globalmente iniciado. Servem em conjunto para abrir e fechar a mesa, o que é equivalente a iniciar e terminar o processo eleitoral nesse local de voto.

Os sistemas computacionais das Mesa de Voto, Cabine de Voto e Urna Electrónica são sistemas comerciais, nomeadamente Windows.

A Mesa de Voto possui um par de chaves assimétricas, que são geradas quando o processo eleitoral é iniciado. A componente privada é usada no final da eleição para revelar os votos expressos. A componente pública é usada pela Cabine de Voto para esconder os votos expressos durante o processo eleitoral.

A Cabine de Voto possui uma chave simétrica privada que é gerada quando o processo eleitoral é iniciado. Esta chave é igualmente usada no final da eleição pela Mesa de Voto/Urna Electrónica para revelar os votos expressos. Durante o processo eleitoral é usada pela Cabine de Voto para esconder os votos expressos.

A Cabine de Voto possui igualmente um par de chaves assimétricas, que são geradas quando o processo eleitoral é iniciado. A componente pública é usada pela Mesa de Voto/Urna Electrónica durante a eleição para garantir a validade dos votos expressos nas cabines. A componente privada é usada pela Cabine de Voto para assinar os votos expressos (após serem duplamente cifrados com as chaves antes descritas) durante o processo eleitoral.

### 3.2.2 Avaliação

**Correcção**

Os votos expressos não podem ser alterados porque são cifrados com várias chaves que estão fisicamente protegidas pelas componentes do sistema.

Os votos válidos não podem ser eliminados na contagem final a menos que exista uma alteração concertada dos registos guardados na Mesa de Voto e na Urna Electrónica. No entanto, tal é facilitado pelo simples facto de as bases de dados co-existirem na mesma máquina.

A contagem final não pode incluir votos inválidos desde que se assumam as garantias habituais dadas por elementos da mesa com interesses antagónicos.

**Democracia**

Só os votantes autorizados podem participar numa eleição, o processo de controlo de acesso à eleição é basicamente o existe nos sistemas baseados em papel.

Cada um desses votantes só pode votar uma vez nessa eleição, uma vez mais o processo de controlo de acesso à eleição é basicamente o existe nos sistemas baseados em papel.

No entanto, nos processos baseados em papel existem várias cópias iguais de cadernos eleitorais que são preenchidos independentemente por cada elemento da mesa que os controla. No caso da Mesa de Voto não é claro quantas pessoas controlam a sua manipulação, se é apenas uma e os

demais corroboram a operação, se têm que ser todos a efectuar a mesma operação independentemente. De qualquer modo, a existência à partida de um único caderno eleitoral central por mesa torna o processo mais sensível a falhas humanas e tecnológicas, sendo por isso um retrocesso em relação ao sistema actual baseado em papel.

**Privacidade**

Não é totalmente garantido que ninguém consiga ser capaz de associar votos a votantes. Com efeito, os votos expressos são guardados numa base de dados. Esta base de dados é autónoma em relação à usada na Mesa de Voto, o que aparentemente garante uma não ligação entre autorizações de voto concedidas e votos depositados. Muito embora não seja registada a hora que ocorrem os depósitos de votos, os registos de actualização da base de dados da urna Electrónica guardam as alterações efectuadas de forma sequencial, para conseguirem desfazer ou reproduzir acções de alteração sequenciais. O mesmo se passa com a base de dados da Mesa de Voto. Consequentemente, os registos das bases de dados, que são divulgados após o final da eleição, podem permitir associar registos de autorizações de voto a votos. Ou, por outro lado, um simples processo de anotação manual das autorizações de voto concedidas pode ser usado para associar votantes a votos se se tiver acesso aos votos depositados e à ordem porque os mesmos foram depositados.

Há ainda um aspecto que pode ser complicar a tarefa de assegurar a privacidade, que é o facto de todas as informações usadas e guardadas --- cadernos eleitorais e votos --- serem geridas na mesma máquina, se bem que em bases de dados diferentes. Para garantir que não existe qualquer cruzamento de informação das duas bases de dados, por software estranho ou mal concebido, é preciso auditar de forma muito exaustiva o sistema da Mesa de Voto/Urna Electrónica. Esse processo seria muito facilitado se as bases de dados residissem em máquinas diferentes sem capacidade de interacção directa.

Nenhum votante consegue demonstrar como votou perante terceiros porque no final do processo não fica com qualquer informação relativa à sua participação no processo eleitoral.

**Verificabilidade**

Nenhum votante pode verificar independentemente que todos os votos foram contados correctamente.

Nenhum votante consegue verificar independentemente que o seu voto não foi ignorado.

**Resistência ao conluio**

Nenhuma das entidades controladoras da eleição, isoladas ou até um certo grau de conluio, podem introduzir votos por outrem ou impedir os votantes autorizados de votar. Esta propriedade é assegurada, *grosso modo*, pela

semelhança com o processo de controlo eleitoral tradicional em papel, onde os elementos da mesa se controlam mútua e presencialmente.

**Disponibilidade**

Não é possível garantir que o sistema de votação funciona correctamente durante o período de votação. Com efeito, o sistema não possui qualquer redundância, bastando que qualquer uma das suas componentes falhe durante a eleição para comprometer localmente a mesma. Mais ainda, uma grande parte das garantias de segurança é dada por alguma forma de protecção física, como a geração interna de chaves de cifra pelas diversas componentes. Este facto é suficiente para invalidar a substituição de uma máquina por outra igual em caso de falha da primeira.

Todos os votantes têm a oportunidade de votar durante todo esse período desde que o sistema não falhe e seja operável de forma minimamente eficiente para minimizar o tempo de participação de cada votante.

**Capacidade de interrupção e continuação**

O sistema permite que qualquer votante interrompa o processo de votação, por vontade própria, e a retome mais tarde durante o período de votação. Para esse fim a Mesa de Voto pode anular uma votação em curso.

Não é possível afirmar que o sistema permite que qualquer votante interrompa o processo de votação, por imposição de uma falha, e a retome mais tarde durante o período de votação. Com efeito, tal dependerá muito do tipo de falha. Mas se a mesma implicar a substituição de componentes do sistema então tal não será possível.

**Capacidade de protestar anonimamente**

O sistema, por imposição expressa da UMIC, não permite verificabilidade, logo cada votante não pode detectar erros de contagem relativos ao seu voto. Consequentemente, o sistema também não prevê quaisquer capacidades dos votantes protestarem, anonimamente ou não, para que sejam feitas correcções

**Capacidade de auditoria durante a eleição**

Não foram previstas quaisquer capacidades de auditoria durante a eleição. Uma elementar, por exemplo, consistiria num cruzamento regular entre o número de autorizações dadas e o número de votos guardados. Tal não é feito, muito embora as duas bases de dados co-existam na mesma máquina.

**Capacidade de auditoria após a eleição**

Aparentemente, o sistema exporta informação suficiente após a conclusão da eleição para, por cruzamento de dados, se detectarem erros devidos a falhas técnicas ou fraude. Para não violar a privacidade dos votantes, e por

indicação expressa da CNPD[2], não são exportadas as identificações dos eleitores que participaram ou não da eleição. No entanto, são exportados registos de actualização das bases de dados, os quais podem fornecer dados relativos à identidade dos votantes, o que contraria a intenção anterior. E, como já antes se referiu, tais registos de operação, nomeadamente os relativos à base de dados da Urna Electrónica, podem violar a privacidade dos votantes porque podem permitir associar votos a votantes.

Aparentemente, a auditoria não tem a possibilidade de corrigir resultados finais como se não tivesse surgido qualquer problema; apenas permite detectar problemas e possivelmente a sua origem.

**Facilidade de registo dos votantes**

O sistema não trata deste aspecto, apenas usa uma base de dados com os votantes autorizados a participar. Essa base de dados é fornecida aquando da iniciação do sistema.

**Facilidade de autenticação dos votantes no acto de votação**

O sistema não trata deste aspecto, é usado o processo habitual de autenticação de votantes dos sistemas baseados em papel.

**Robustez do mecanismo de autenticação**

O sistema não contribui nem positiva nem negativamente neste aspecto.

**Possibilidade de voto remoto em secções de voto alheias**

O sistema actualmente não contempla esta possibilidade. São feitas afirmações acerca de um futuro suporte deste tipo de mobilidade mas nada é dito acerca dos problemas que se pensam resolver para fornecer essa facilidade.

No documento de descrição do sistema é dito que “A MULTICERT / PT Inovação desenharam uma solução que possibilita a utilização de modelos de votação electrónica que permitem a mobilidade do eleitor, i.e., modelos em que o eleitor pode exercer o seu direito de Voto a partir de qualquer Assembleia de Voto (o que permitirá diminuir a abstenção).”. No entanto, nada no modelo descrito mostra como tal pode ser feito porque o sistema funciona em modo desligado, logo num universo de votantes puramente local.

Afirma-se, contudo, que “a aplicação de Mesa de Voto actual poderá permitir aceder a cadernos eleitorais centralizados, assim como depositar os Votos numa Urna Electrónica centralizada”. Esta estratégia tem, contudo, problemas de segurança que importa considerar, como ligação a redes externas, e de tolerância a faltas, porque a realização do processo eleitoral ficaria fortemente condicionado por falhas das componentes centrais do sistema.

[2] Comissão Nacional de Protecção de Dados

**Possibilidade de voto remoto em qualquer lugar**

O sistema actualmente não contempla esta possibilidade nem se prevê que o possa fazer alguma vez por replicar de forma muito próxima a votação em papel e presencial em secções de voto concretas.

### 3.2.3 Comentário geral

O sistema foi feito para ser operacionalmente semelhante aos tradicionais baseados em papel. O resultado é um sistema que pode transmitir algum conforto ao votante, que vê no mesmo um funcionamento algo semelhante ao que porventura já se habituou a ver nos sistemas clássicos.

Operacionalmente o sistema não é muito complexo de usar mas a sua única mais valia em relação ao processo actual é reduzida: apenas serve para contar os votos mais rapidamente e evitar os votos nulos.

Em termos de risco de confiança, o sistema tem vários problemas. A auditoria das bases de dados pode revelar associações entre votos e votantes e o processo de controlo dos votantes autorizados não é replicado por múltiplas autoridades (tanto quanto se percebeu).

Em termos de risco operacional, o sistema é muito vulnerável a falhas dos seus componentes, em especial à falha da Mesa de Voto/Urna Electrónica, o único que não pode ser replicado de forma alguma. As Cabines de Voto podem ser replicadas, mas não podem ser substituídas durante o processo eleitoral. Logo, se se usar apenas uma Cabine de Voto, a falha da mesma compromete o processo eleitoral nesse local de voto.

## 3.3 **Unysis**

O sistema avaliado foi a plataforma de votação electrónica iVotronic, desenvolvida pela Election Systems and Software (ES&S). A documentação fornecida sobre o mesmo consta do Anexo III. Os comentários que se seguem foram feitos tendo em conta exclusivamente essa documentação e assumindo a correcção implícita das acções efectuadas pelas várias componentes usadas. No entanto, essa correcção terá se ser igualmente auditada se o sistema alguma vez for considerado para uso.

### 3.3.1 Arquitectura

A plataforma iVotronic é constituída pelas seguintes componentes:

1. **Personal Electronic Ballot (PEB)**. Esta componente é um cartão especial, com características proprietárias (dimensão e uma interface de infra-vermelhos) que substitui o tradicional boletim em papel. O eleitor, após a sua identificação pela mesa de voto e se autorizado a votar, recebe um PEB que usa para votar. Este PEB possui um boletim que só pode ser usado uma vez.

2. **Voter Terminal (*Voting Terminal*)**. Esta componente substitui o processo tradicional de preenchimento do boletim em papel. O eleitor, munido de um PEB correctamente carregado com um boletim de voto, usa o *Voting Terminal* para preencher o boletim e guardá-lo para a contagem final. O *Voting Terminal* possui um ecrã sensível ao toque que serve para efectuar a votação. No final da votação, o *Voting Terminal* guarda o voto de uma forma segura e redundante em vários suportes de memória sem partes mecânicas e sem necessidade de alimentação contínua.

3. **Supervisor Terminal (ST)**. Esta componente serve para carregar um boletim novo num PEB para que um votante possa usar este último. Esta componente, em conjunto com a seguinte (Supervisor PEB), usa diversas cópias em memória do boletim para garantir que o mesmo não está de alguma forma adulterado.

4. **Supervisor PEB**. Este componente serve para abrir e fechar os *Voting Terminal*, o que é equivalente a iniciar e terminar o processo eleitoral nesse local de voto, em particular para transferir os votos depositados num *Voting Terminal* para um local central de contagem. Serve também para accionar os ST.

O iVotronic permite uma votação paralela em papel através da emissão de boletins de voto em papel preenchidos pelo *Voting Terminal*.

O iVotronic, tanto quanto se percebeu, não serve para gerir cadernos eleitorais. Serve apenas para suportar o processo de votação em concreto, não a autorização de participação no mesmo. No entanto, está preparado

para impedir a votação múltipla por um votante autorizado quando este está na posse de um PEB.

O sistema usa em grande extensão sistemas proprietários, tanto de hardware como de software. O próprio sistema operativo dos *Voting Terminal* é proprietário. Não é claro, no entanto, se o hardware dos *Voting Terminal* é maioritariamente convencional ou se ele é também totalmente proprietário.

### 3.3.2 Avaliação

**Correcção**

Os votos expressos não podem ser alterados porque estão guardados em múltiplas zonas de memória diferentes, com CRC (*Cyclic Redundancy Checks*) de controlo, nas *Voting Terminal*, que não permitem acessos do exterior para alteração dos votos guardados. Esta garantia é assegurada fundamentalmente através de segurança física.

Os votos válidos não podem ser eliminados na contagem final a menos que exista uma alteração concertada dos registos guardados na mesa de voto e na contagem agregada de todos os votos recolhidos por um *Supervisor* PEB junto dos vários *Voting Terminal*.

A contagem final não é pormenorizada na documentação, apenas é descrita a passagem de votos de um *Voting Terminal* para um PEB. Consequentemente, não pode ser aqui avaliada.

**Democracia**

Só os votantes autorizados podem participar numa eleição, o processo de controlo de acesso à eleição é exactamente o existe nos sistemas baseados em papel.

Cada um desses votantes só pode votar uma vez nessa eleição, uma vez mais o processo de controlo de acesso à eleição é basicamente o existente nos sistemas baseados em papel acrescido do uso singular do boletim de voto disponibilizado ao votante no PEB.

**Privacidade**

Os boletins de voto transmitidos via PEB não possuem informação personalizada e votos guardados nos *Voting Terminal* não são armazenados sequencialmente mas aleatoriamente. Consequentemente, não é possível relacionar votos e votantes, nem mesmo através de registos temporais de operações efectuadas pelos *Voting Terminal*.

Nenhum votante consegue demonstrar como votou perante terceiros porque no final do processo não fica com qualquer informação relativa à sua participação no processo eleitoral.

**Verificabilidade**

Nenhum votante pode verificar independentemente que todos os votos foram contados correctamente. Nenhum votante consegue verificar independentemente que o seu voto não foi ignorado. No entanto, o sistema permite efectuar paralelamente uma votação em papel que permite detectar anomalias locais.

**Resistência ao conluio**

Nenhuma das entidades controladoras da eleição, isoladas ou até um certo grau de conluio, podem introduzir votos por outrem ou impedir os votantes autorizados de votar. Esta propriedade é assegurada, *grosso modo*, pela semelhança com o processo de controlo eleitoral tradicional em papel, onde os elementos da mesa se controlam mútua e presencialmente.

**Disponibilidade**

O sistema foi desenhado para poder funcionar correctamente durante o período de votação. Com efeito, o sistema possui diversas formas de redundância, independência de factores normais de falha (alimentação eléctrica exterior) ou mesmo capacidade de operar com múltiplas instâncias das suas componentes (PEB e *Voting Terminal*).

Todos os votantes têm a oportunidade de votar durante todo esse período desde que o sistema não falhe (no seu todo, ou seja, desde que subsista um *Supervisor terminal*, um PEB e um *Voting Terminal* a funcionar correctamente) e seja operável de forma minimamente eficiente para minimizar o tempo de participação de cada votante.

**Capacidade de interrupção e continuação**

Tecnicamente, o sistema permite que qualquer votante interrompa o processo de votação, por vontade própria, e a retome mais tarde durante o período de votação. Politicamente, tal depende da autorização dada pela mesa de voto para que tal seja autorizado, porque essa anulação interfere com o processo de controlo de acesso ao sistema, que não faz parte do iVotronic.

Não é possível afirmar que o sistema permite que qualquer votante interrompa o processo de votação, por imposição de uma falha, e a retome mais tarde durante o período de votação. Com efeito, tal dependerá muito do tipo de falha.

**Capacidade de protestar anonimamente**

O sistema não permite verificabilidade, logo cada votante não pode detectar erros de contagem relativos ao seu voto. Consequentemente, o sistema também não prevê quaisquer capacidades dos votantes protestarem, anonimamente ou não, para que sejam feitas correcções

**Capacidade de auditoria durante a eleição**

A única capacidade de auditoria durante uma eleição consiste em comparar o número de votos armazenados nos vários *Voting Terminal* com o total de votantes que já foram autorizados a votar.

**Capacidade de auditoria após a eleição**

Muito embora seja dito que o sistema guarda exaustivamente todas as suas operações, não é dito como é que as mesmas são exportadas ou auditadas. Presume-se que a auditoria seja feita internamente, ou seja, usando o sistema operativo proprietário.

Aparentemente, a auditoria não tem a possibilidade de corrigir resultados finais como se não tivesse surgido qualquer problema; apenas permite detectar problemas e possivelmente a sua origem. No entanto, a auditoria em princípio não consegue relacionar votos com votantes a menos que fique registado, com as demais operações, a operação de selecção aleatória do local de salvaguarda de cada voto.

**Facilidade de registo dos votantes**

O sistema não trata deste aspecto.

**Facilidade de autenticação dos votantes no acto de votação**

O sistema não trata deste aspecto.

**Robustez do mecanismo de autenticação**

O sistema não contribui nem positiva nem negativamente neste aspecto.

**Possibilidade de voto remoto em secções de voto alheias**

O sistema não trata deste aspecto.

**Possibilidade de voto remoto em qualquer lugar**

O sistema não trata deste aspecto.

### 3.3.3 Comentário geral

O sistema trata apenas as etapas do processo eleitoral relativas ao preenchimento de um boletim de voto, seu depósito numa urna e contagem final. Nada é feito em termos de autenticação de votantes e autorização de participação na votação.

Operacionalmente o sistema não é muito complexo de usar mas a sua única mais valia em relação ao processo actual é reduzida: apenas serve para contar os votos mais rapidamente e evitar os votos nulos.

Em termos de risco de confiança, o sistema não apresenta quaisquer problemas evidentes.

Em termos de risco operacional, o sistema é pouco vulnerável a falhas dos seus componentes, que podem em grande medida ser replicados num grau à escolha. Mas não é claro o que se pode fazer com os votos guardados num *Voting Terminal* que falha completamente, nem é claro o que acontece quando falham *Supervisor* PEB críticos.

# 4 Interface com o utente

Não era intenção desta equipa de auditoria debruçar-se sobre os aspectos de interface de voto com o votante. No entanto, uma vez que houve pessoas da UA que mostraram interesse em fazer tal avaliação, e uma das experiências piloto decorreu num local geograficamente próximo da UA (na freguesia de S. Bernardo), foi feita uma avaliação *in loco* sob o ponto de vista de usabilidade por uma equipa de especialistas na matéria.

Essa equipa era constituída pela Profª Beatriz Sousa Santos (do Dep. de Electrónica e Telecomunicações da UA), pelo Prof. Óscar Mealha (do Dep. de Comunicação e Arte da UA) e o Eng. Florin Zanfir, bolseiro do IEETA, ambos com interesses científicos na área da usabilidade. Esta equipa deslocou-se ao local da experiência durante a sua realização e a Profª Beatriz Santos produziu um relatório que seguidamente se reproduz com uma edição mínima.

## 4.1 Relato das visitas à experiência piloto do sistema de voto electrónico da Unisys realizado na junta de freguesia de S. Bernardo, em Aveiro

No dia 13 de Junho de 2004 a equipa fez duas visitas à junta de Freguesia de S. Bernardo, em Aveiro. Uma das visitas foi ao início da manhã, a outra foi na altura do encerramento das urnas, tendo permanecido no local cerca de 2h.

Até ao encerramento das urnas puderam contactar com o responsável pelo teste do sistema e com um técnico da PT-Inovação, que fizeram uma descrição dos principais aspectos do sistema bem como do procedimento adoptado no teste. No entanto, não foi possível fazer qualquer observação directa das interfaces de utilizador da aplicação de voto a ser utilizada pelos eleitores, ou da aplicação a ser utilizada pelos membros da Mesa, devido ao elevado número de eleitores que se encontravam à espera de poder participar no teste.

Depois do encerramento das urnas, e decorridas as formalidades de encerramento do escrutínio, pôde-se observar uma demonstração do funcionamento da aplicação a ser utilizada pelos eleitores e houve oportunidade de recolher algumas opiniões de pessoas que tinham acompanhado o teste. De acordo com as mesmas, a adesão dos eleitores tinha sido elevada, não tendo sido superior por se verificarem, em certos períodos do dia, tempos de atendimento relativamente longos e que se tornaram desmotivadores.

Na posse de tão pouca informação, a equipa apenas pode referir alguns aspectos que pareceram poder necessitar de um estudo adicional e projecto mais cuidado, no sentido de melhorar a usabilidade da aplicação a ser utilizada pelos eleitores:

1. tempos de leitura dos cartões (os leitores usados pareceram demasiado lentos).
2. representação no ecrã do leitor de cartões (que deve ser consistente com o modelo usado, i.e., ambos na vertical ou na horizontal e não um na vertical e outro na horizontal, tal como foi utilizado).
3. características da letra a usar (talvez maior, para que o texto seja mais legível).
4. metáfora de preenchimento do boletim de voto (que exigia a confirmação da escolha feita através de um botão, ao contrário do que acontece na votação em papel, devendo o botão ser mais visível).

Quanto à aplicação a ser utilizada pelos membros da Mesa, não tendo havido oportunidade de assistir a qualquer demonstração, nem de fazer qualquer outra observação, apenas se pode referir, com base em conversa informal tida com alguns dos presentes, que esta aplicação parece ter um procedimento de abertura da Mesa demasiado complexo (sendo demasiado sensível à temporização de vários passos), o que terá provocado um atraso considerável na abertura da Mesa de voto electrónica.

Finalmente, é importante realçar o facto destes sistemas se destinarem a ser utilizados por utilizadores sem qualquer treino específico e, na maioria dos casos, com uma literacia computacional muito baixa ou inexistente, o que torna os aspectos de usabilidade absolutamente fundamentais para a sua utilização com sucesso. Sendo assim, recomenda-se vivamente que seja levado a cabo um estudo de usabilidade do sistema, nas suas diversas componentes, quer de S/W quer de H/W.

# 5 Conclusões

A conclusão básica relativa às três soluções consideradas é a seguinte: a sua mais-valia, quando comparada com a solução actual (i.e., tradicional, baseada em papel) é muito reduzida, uma vez que se limita, *grosso modo*, a apresentar uma interface (talvez) mas agradável ao votante e a potenciar o aumento da velocidade de apuramento dos resultados. Nenhum destes aspectos nos parece justificar o investimento, por mais reduzido que seja, nas tecnologias em causa. Com efeito, na nossa opinião, uma solução de cariz informático justifica-se se permitir a mobilidade do votante, i.e. se for permitido que este exerça o seu direito de voto num local que não a mesa de voto por onde se encontra registado.

Uma outra conclusão fundamental está relacionada com a confiança que se pode ter nas soluções testadas. Com base no historial das empresas em causa pensamos que, de uma forma genérica, as soluções tecnológicas apresentam um grau de confiança razoável. No entanto, note-se que tal não nos é permitido concluir, antes pelo contrário, com base na documentação apresentada. Assumindo que estes documentos são apenas uma primeira apresentação dos sistemas, será necessário no futuro ter acesso a mais informação e, em particular, ao próprio software e hardware. Neste caso, há aspectos de propriedade intelectual que as empresas, compreensivelmente, quererão com certeza assegurar, impedindo que caiam no domínio público. Coloca-se, assim, a questão de qual a disponibilidade que as empresas em causa, ou quaisquer outras, poderão de facto demonstrar em termos de disponibilizar a informação necessária.

Este último aspecto levanta uma questão de base no que diz respeito aos sistemas de votação electrónica no geral. Há basicamente duas opções: uma que se baseia na utilização de soluções cujo acesso é restrito, outra (dita "*open-source*") que assume a total abertura no acesso às soluções hardware e software. Pensamos que este aspecto deverá ser alvo de uma ampla discussão, não limitada às entidades com capacidade científica e tecnológica, i.e. deverá abranger a sociedade em geral.

André Ventura da Cruz Marnôto Zúquete licenciou-se em Engenharia Electrotécnica pelo IST em 1988. Nessa mesma escola concluiu o Mestrado, em 1992, e o Doutoramento em Eng. Informática e de Computadores, em 2001.
É actualmente Prof. Auxiliar da Universidade de Aveiro, investigador do IEETA e colaborador do IT. Antes foi docente do IST (Assistente Estagiário de 1990 a 1992, Assistente de 1992 a 2001 e Prof. Auxiliar de 2001 a 2003) e investigador do INESC de 1986 a 2003 no Grupo de Sistemas Distribuídos. Ainda no IST foi em 2003 vice-presidente do Centro de Informática.
Leccionou diversas cadeiras de licenciatura e mestrado na área das arquitecturas de computadores, sistemas operativos, sistemas distribuídos e segurança. A sua área principal de investigação é a da segurança em sistemas computacionais distribuídos, na qual tem desenvolvido trabalho em diversas vertentes, dos algoritmos aos sistemas, e nomeadamente na área dos sistemas distribuídos de votação electrónica. Tem igualmente tentado fazer a ponte entre a investigação e a exploração dos meios informáticos, levando o conhecimento dos problemas e soluções de segurança a diversos fóruns. É ainda colaborador regular da revista "Segurança". Desde 1994 participou em diversos projectos nacionais e internacionais relacionados com a segurança em sistemas computacionais. Publicou, como autor e co-autor, cerca de duas dezenas de artigos em conferências, workshops e revistas nacionais e internacionais na área de segurança em sistemas informáticos.

Paulo Jorge Pires Ferreira licenciou-se em Engenharia Electrotécnica pelo IST em 1988, tendo nessa mesma escola obtido o grau de Mestre, em 1992. Obteve o Doutoramento em Informática, na Université Pierre et Marie Curie (Paris VI), em 1996.
No IST foi Assistente Estagiário de 1989 a 1992, Assistente no ano de 1996, e é Professor Auxiliar desde 1997. Tem a seu cargo diversas disciplinas na Licenciatura e no Mestrado em Engenharia Informática e de Computadores na área de plataformas e aplicações distribuídas na Internet.
É investigador no INESC desde 1986 onde é responsável pelo Grupo de Sistemas Distribuídos (http://www.gsd.inesc-id.pt/). Foi investigador no INRIA em França (Rocquencourt) de 1992 a 1996 no grupo de Sistemas de Objectos Distribuídos.
Desde 1986 participou em diversos projectos Europeus de investigação na área de Sistemas Distribuídos. A sua área de investigação centra-se nas áreas de Sistemas Operativos e Sistemas Distribuídos, com ênfase nos mecanismos e algoritmos de suporte a aplicações distribuídas em redes de grande escala, i.e, aplicações na Internet (como por exemplo, WEB, comércio electrónico, segurança, etc.).
Publicou, como autor e co-autor, mais de cinco dezenas de artigos em conferências, workshops e revistas internacionais da área de sistemas distribuídos e é revisor de várias conferências e workshops internacionais na área de sistemas distribuídos.