Resumo

Os sistemas de votação tradicionais não têm acompanhado a evolução das Tecnologias de Informação e Comunicações (TIC), apesar de se lhes reconhecer diversas vantagens, como dar resposta à forte abstenção que, em eleições gerais, se têm vindo a acentuar, à existência da negação de privacidade a pessoas com necessidades especiais e à morosidade dos processos de contagem. Naturalmente verifica-se uma forte vontade política, de todos os quadrantes, para a implementação de sistemas de votação electrónica. No entanto, as recentes implementações destes sistemas têm vindo a apresentar falhas de segurança graves, que põem em causa os requisitos básicos dos processos eleitorais. Qualquer sistema de votação electrónica, têm várias pessoas a desempenhar diferentes papéis e várias tecnologias a suportar os variados processos necessários, aumentando a complexidade e as ameaças de quebra de segurança. Dada a elevada exigência de garantia da segurança e, de acordo com a actividade da gestão de risco, é fundamental a criação de uma política de segurança para lidar com esta complexidade. Nesta tese é proposto um método de construção de políticas de segurança, baseado nos guiões e normas existentes de segurança, assente nas propriedades da segurança: confidencialidade, Integridade, disponibilidade, autorização e privacidade (estas últimas particularmente adaptadas a um sistema de votação electrónico). Com este método, a partir de uma visão global do sistema, onde são conhecidas as ameaças, vulnerabilidades, papéis desempenhados e os acessos à informação, será possível identificar as tecnologias e as regras de utilização que, de um modo equilibrado, optimizando a alocação de recursos, confiram ao sistema um nível de segurança desejado.

Palavras-chave: Voto electrónico, Gestão de risco, Políticas de segurança e Tecnologias de segurança

Abstract

The traditional voting systems have not evolved with the Communication and Information Technologies, despite their recognized advantages in issues like the increasing abstention (specially in nation-wide elections); the non-privacy of people with special needs and, the slowness of counting votes process. Naturally, there is a great political motivation to implement e-voting systems. However, the most recent implementations bring up security faults that can compromise the basics requirements of a voting process. Any kind of e-voting system involves many people, many roles, many technologies to support the required functions and many processes, increasing the complexity and the number and type of security breaches. In order to control the security level and optimize resource allocation, it is essential to create an adequate security policy. In this thesis a security policy creation method is proposed, which is based on standards and regulations for security and risk management. It starts with the fundamental security properties, i.e., confidentiality, integrity, availability, authorization and privacy (these last two particularly critical in a e-vote system). Using this method, along with a detailed global system vision, where vulnerabilities, secure threats, different user roles and information accesses are well detailed, it will be possible to identify the technologies and its utilization rules, which together and in a balanced way, promotes resource allocation for a given security level.

Keywords: Electronic Vote, Risk Management, Security Policies and Security Technologies

Índice

Índice de figuras

Índice de tabelas

Agradecimentos

Não poderia deixar de agradecer:

À minha esposa e ao meu filho,
Ao Orientador Professor Henrique Santos,
Ao Professor Leonel Santos,
Ao amigo Fernando Correia,
Ao amigo José Caetano,

e a todos os que acreditaram, apoiaram e acompanharam o desenvolvimento deste trabalho, sabendo o que ele representa para mim.

Introdução

A crescente abstenção sentida nos processos eleitorais, a possibilidade de permitir, com privacidade, o direito a voto a pessoas com necessidades especiais, a possibilidade de se poder votar confortavelmente a partir de um acesso à Internet e a vontade política de todas as áreas e de vários governos europeus e dos Estados Unidos da América, são motivos fortes para que o voto electrónico remoto seja ambicionado. Porém, na opinião de vários autores, ainda está longe de ser alcançado (Rubin 2001; Malkhi 2002). A opinião destes autores baseia-se nas falhas de segurança sentidas nas recentes implementações de sistemas de voto electrónico, provocando desconfiança. Qualquer sistema de votação electrónica, tal como o voto tradicional, têm várias pessoas a desempenhar diferentes papéis, e várias tecnologias a suportar os variados processos e a fornecer / processar a informação necessária, aumentando a complexidade das questões de segurança.

Como é facilmente compreendido, neste contexto a segurança é um dos aspectos fundamentais a considerar,(Shamos 1993) sendo por isso exigido um cuidado muito especial na escolha e implementação das tecnologias de suporte para a votação electrónica, mesmo face às implementações de segurança noutras áreas exigentes, como o comércio electrónico e a banca electrónica.

A actividade de gestão de risco é fundamental no que toca a questões de segurança de sistemas de informação. Existem várias normas e critérios (ISO/IEC 1996; ISO/IEC 2000; Dorofee 2001) que procuram orientar esta actividade. As políticas de segurança assumem um papel fulcral e, no caso do voto electrónico, este papel é reforçado devido ao nível de exigência de segurança.

Cada sistema de voto electrónico tem o seu contexto (local, regional, nacional e internacional) e especificidades próprias (presencial, não presencial, totalmente informatizado ou não), implicando políticas de segurança, em grande parte também específicas. A política de segurança de um sistema de votação electrónica, tal como os sistemas de informação das organizações, exige um levantamento de requisitos, a identificação de todos os intervenientes, uma descrição de todos os processo e a escolha de um leque de tecnologias adequadas, cada uma exigindo medidas de segurança ou administrativas devidamente ajustadas. As políticas de segurança envolvem também outras componentes, tais como: acesso físico, catástrofes naturais, entre outros aspectos não tecnológicos e que estão fora do âmbito deste trabalho, mas que são referidos em diversas normas, como a ISO 17799.

Como se pode depreender, a criação de uma política de segurança é uma tarefa complexa, cuja realização carece de uma abordagem metodológica. Esta é a motivação para a elaboração desta tese.

Utilizando como ponto de partida as propriedades fundamentais da segurança (confidencialidade, integridade e disponibilidade), acrescentando-se a autenticação (englobando aqui a identificação e autorização) e a privacidade que é um direito, o método de construção de políticas de segurança aqui proposto permite envolver todas estas componentes de uma forma clara, fornecendo uma visão global de responsabilidade no, manuseamento da informação, bem como a identificação das vulnerabilidades e ameaças conhecidas com vista à adequada definição de medidas de segurança e a adopção de tecnologias de segurança.

No primeiro capítulo, é feita uma revisão de literatura nas várias áreas em questão: voto electrónico, segurança, gestão de risco, políticas de segurança e tecnologias de segurança. No segundo capítulo é descrito o método aqui proposto, o seu enquadramento com outros métodos de gestão de risco, as suas várias fases e os seus resultados. No capítulo 3, é apresentado um estudo de caso onde é aplicado o método proposto a um sistema de voto electrónico em desenvolvimento no departamento de Sistemas de Informação da Universidade do Minho, através de uma versão inicial da sua arquitectura (Santos 2004). Finalmente, no capítulo 4 são apresentadas as conclusões bem como algum trabalho futuro.

1. Revisão de Literatura

Para o devido enquadramento do método de construção de políticas de segurança a desenvolver, foi necessária uma revisão de literatura extensiva, sobre as áreas em causa: voto tradicional e voto electrónico (vantagens, desvantagens e requisitos de um sistema de voto electrónico); fundamentos de segurança; gestão do risco de segurança; políticas de segurança, e tecnologias de segurança.

1.1. Processo eleitoral tradicional

Os sistemas de votação tradicionais não têm conseguido dar resposta à forte abstenção que têm vindo a sofrer, em parte, devido à obrigatoriedade da votação ser feita no local de recenseamento do eleitor. Por outro lado existe a negação de privacidade a pessoas com necessidades especiais, uma vez que têm de se acompanhadas até à cabina de voto, e ainda a morosidade dos processos de contagem. O processo de voto eleitoral tradicional é sempre uma constante na referência de um sistema de votação electrónica. Seguidamente, será descrito o processo do voto tradicional.

1.1.1. Recenseamento

O recenseamento consiste do registo, no caderno eleitoral, da pessoa que tenha as condições exigidas por lei para o processo de eleição em questão. A cada indivíduo é dado um cartão de eleitor com um número único, no respectivo caderno, que serve de identificação, na altura da eleição. Este cartão contém a denominação da freguesia onde o eleitor pode votar.

Esta fase fica a cargo das juntas de freguesia que procedem ao carregamento e validação dos cadernos eleitorais.

1.1.2. Validação da identificação do eleitor

A validação da identificação do eleitor é feita na altura em que o eleitor se dirige à mesa de voto e requisita o seu boletim de voto. O presidente da mesa pronuncia o nome e número do eleitor e os restantes elementos da mesa

registam, na sua lista de eleitores, o votante. Esta fase acontece no decorrer da eleição, ao contrário da fase anterior.
O mesmo registo serve para não-repúdio, evitando que o eleitor o faça uma segunda vez.

1.1.3. Recolha de Votos

Após o levantamento do boletim de voto, o eleitor dirige-se à cabine de voto onde regista no boletim a sua votação. Normalmente, dobra o boletim em quatro partes, dirige-se, novamente à mesa de voto onde introduz o seu boletim na urna. Termina nesta fase a participação do eleitor. Os elementos da mesa acompanham esta fase.

1.1.4. Contagem dos votos

Após o encerramento da votação, as urnas são abertas e os votos são validados, classificados e contados, sendo depois publicado o resultado da contagem. Esta tarefa fica a cargo dos elementos da mesa.

1.2. Voto electrónico (e-Vote)

O voto electrónico consiste na utilização de sistemas informáticos que automatizem qualquer etapa ou processo de uma eleição (Gritzalis 2002; Xenakis 2004). Já existem várias implementações de sistemas de contagem de votos, sistemas de urnas automáticas, entre outros. O ideal seria conseguir-se um sistema de votação completamente informatizado, com a possibilidade de se votar remotamente de qualquer parte em que o eleitor se encontre, obviamente sem comprometer o conjunto de pressupostos que estão subjacentes a um processo eleitoral livre, não coercivo e livre de fraudes.

As vantagens de um sistema deste tipo, identificadas por diversos autores (Rivest 2001; Malkhi 2002; Rosner 2002; Kitcat 2004), prendem-se com os seguintes factores:
- combate à forte abstenção, com tendência a aumentar;

- possibilitar a invisuais e pessoas com necessidades especiais poderem votar confortavelmente, sem necessidade de se deslocar, ou sem nenhum acompanhante até à cabina de voto; e
- uma forte redução de custos a médio prazo, através da redução do destacamento de pessoas para o processo eleitoral (para além eliminação dos boletins de voto em papel).

Para além destes factores positivos, é notória uma forte vontade política em introduzir as Tecnologias de Informação e Comunicações (TIC) (Pitt 2003; Kitcat 2004), tanto a nível da União Económica Europeia como nos Estados Unidos, que obviamente se reflecte nos países ou estados a estes pertencentes.

As diversas tentativas de implementação destes sistemas têm gerado alguma controvérsia, como é notório pelas várias opiniões de autores que se posicionam contra, pelas falhas identificadas em experiências efectuadas nos Estados Unidos (Neumann 2000; Peter Neumann 2000; Rubin 2001; Bannet 2003; Kitcat 2004; KOHNO 2004), bem como noutros países (McGaley 2004). As falhas de implementação que provocam renitência a estes sistemas, passam por:
- falta de fidedignidade das aplicações instaladas no computador do eleitor;
- uso da Internet como meio de comunicação entre os servidores de voto e o computador do qual os eleitores estão a votar;
- a possibilidade da coercibilidade;
- a colisão entre a confirmação do voto e em quem foi votado, e a possibilidade de venda de votos; e
- tolerância à falha do próprio sistema;.

1.2.1. Tipos de voto electrónico

O sistema de voto tradicional, descrito anteriormente, implica a presença do eleitor junto do local definido na sua freguesia de recenseamento. Na votação electrónica pode não acontecer, daí ser necessário distinguir dois tipos de voto electrónico: presencial e não presencial.

Presencial

Neste caso, embora o processo eleitoral possa ser informatizado, ele não dispensa a presença do eleitor. A fase de identificação e validação é feita na presença do mesmo e junto dos elementos da mesa, embora possam ser utilizados meios electrónicos de identificação (Gritzalis 2002).

Não presencial

Neste caso, a fase de identificação e validação é também informatizada, sendo possível o eleitor votar remotamente, sem estar confinado ao seu local de recenseamento.(Rubin 2001)

1.3. Requisitos do processo eleitoral

Nas leis eleitorais (Mendes and Miguéis 2005; Pereira 2005) estão patentes os requisitos necessários para que o processo eleitoral tradicional decorra com normalidade. De seguida irão ser enunciados os mais relevantes:

Elegibilidade/Autenticação

Numa eleição democrática apenas os eleitores constantes dos cadernos eleitorais e em condições de o fazer devem poder votar. Para tal, é necessário que o sistema de voto electrónico permita a identificação e autenticação dos mesmos, assim como a verificação da sua admissibilidade ao processo em questão.

Singularidade (reutilização)

A cada eleitor tem de ser permitido um voto. A regra democrática de “um eleitor, um voto”.

Apuramento

Todos os votos válidos têm de ser contabilizados no processo da eleição.

Integridade

Os votos têm de permanecer inalterados, mesmo após o término do processo eleitoral.

Verificabilidade / Auditabilidade

Em todos os tipos de eleições deverá ser possível verificar se todos os votos válidos foram contabilizados, especialmente perante o votante. Este requisito é particularmente importante no caso de um sistema de e-Vote.

Apesar do e-Vote trazer mais valias para diversas fases do processo de eleição, ao mesmo tempo acarreta novas vulnerabilidades e ameaças, exigindo um estudo complementar associado à interferência das tecnologias com os requisitos acima indicados. Existe imensa literatura que toca no tema dos requisitos do voto electrónico. Uns Baseados na lei eleitoral (Xenakis 2004), outros com base nas questões democráticas e ainda outros, em complemento, baseados nos requisitos de segurança. Com base numa revisão de literatura (Parth P. Vasa 2005) feita por estudantes do Instituto John Hopkins, que faz parte do desenvolvimento de um projecto de voto electrónico remoto sob a orientação de um dos autores mais relevantes na área Aviel Rubin, foram identificados os mais importantes requisitos de um sistema de voto electrónico, a acrescentar aos identificados para o processo de votação tradicional.

Transparente

O sistema de e-Vote não pode ser uma caixa negra. O seu funcionamento deverá ser do conhecimento público e monitorizado por todas as partes envolvidas no processo eleitoral.

Robustez / Tolerância a faltas

Consiste na continuidade de disponibilidade, independentemente, de uma falha ou erro nos componentes do sistema. Existem vários métodos que permitem a tolerância a falhas, tais como: redundância – quando um disco duro falha ao ser acedido, sem o utilizador notar um disco redundante continua a fornecer o serviço; - o simples uso de um dispositivo acumulador de corrente, permite tolerar a falha de energia.

No caso do voto electrónico, o sistema deve ter um mecanismo de recuperação/tolerância a faltas, de forma a evitar a perda de votos e permitir o eleitor dar continuidade a partir da altura em que ocorreu a falha ou erro. No sistema de votação tradicional esse mecanismo pode passar pela realização de novas eleições numa data própria.

Flexibilidade / conveniente

Uma das vantagens que os autores defendem que o e-Vote vem trazer é a possibilidade de este ser flexível o suficiente para se adaptar à especificidade do leitor. Por exemplo, no caso de este ser invisual, o sistema deve adaptar a sua interface para uma forma sonora.

Usabilidade

O sistema e-Vote deve ser de formato amigável e de fácil utilização por parte de todos os eleitores.

Rastreabiliade

Durante a votação o eleitor deverá ter a possibilidade de retomar o processo em caso de mau funcionamento, sem lhe ser negado o direito ao voto. Por outro lado, existe a necessidade da criação de registos de acções feitas perante o sistema, sem comprometer o direito à privacidade do eleitor. Este é, porventura, o requisito mais difícil de garantir, exigindo simultaneamente o registo de acções do eleitor para futura utilização e a privacidade desses mesmos registos, sob controlo exclusivo do eleitor.

Disponibilidade

O sistema deverá estar disponível a todos os eleitores, durante todo processo eleitoral. Evitando a negação do direito ao voto.

1.4. Propriedades de Segurança no e-Vote

No âmbito dos inúmeros trabalhos e normas publicados sobre Segurança dos Sistemas de Informação, são identificadas, normalmente, um conjunto de três propriedades que constituem os pilares dessa segurança: Confidencialidade, Integridade e Disponibilidade (ISO/IEC 1996; ISO/IEC 1999; ISO/IEC 2000; ISO/IEC 2005). No domínio do e-*Vote* é fácil reconhecer a importância destas propriedades, sendo, no entanto, necessário reforçar outras duas: a Autenticidade (no sentido de garantir sempre a correcta associação entre a identidade de um indivíduo e a transação que ele realiza) e a Autorização (capacidade de conferir o direito a executar uma dada transação). Por outro lado, surge, igualmente importante o direito da privacidade, o qual não pode ser ferido por qualquer medida que procure promover aquelas propriedades de segurança. De uma forma mais detalhada, as propriedades em foco no sistema e-Vote são (Neumann 1993; Bannet 2003; Whitson 2003; Ed Tittel 2004):

Confidencialidade

Confidencialidade significa que qualquer informação trocada é secreta e apenas as partes autorizadas conseguem aceder a estas.

No caso do e-Vote, esta propriedade é basilar, dado que em todas as fases do processo eleitoral existe troca de informação crítica e que apenas deve ser perceptível para as entidades/actores devidamente autorizados pelo sistema. Não é possível manter a confidencialidade se a informação não for íntegra.

Integridade

Manter a integridade da informação significa manter a sua veracidade, ou seja, garantir que a informação apenas é alterada intencionalmente por actores devidamente autorizados. Neste grande objectivo não é difícil encontrar três medidas complementares: não permitir a alteração por entidades não autorizadas; garantir que as entidades autorizadas têm sempre conhecimento de alterações; e garantir que a informação permanece consistente.

Disponibilidade

Disponibilidade de informação significa que os actores do sistema devem aceder à informação, íntegra e confidencial, de uma forma permanente e em qualquer altura que necessitem. No caso do e-Vote o eleitor terá de ter acesso ao sistema permanentemente, enquanto durar o processo eleitoral e/ou até que o tenha utilizado.

Autenticação/Identificação/autorização

Autenticação está directamente relacionada com outra propriedade de segurança a identificação. Identificação significa que o actor se identifica de uma forma reconhecida pelo sistema. Autenticação é o acto de verificar a identificação. Com base nestas duas propriedades e ao longo do processo eleitoral os actores podem ou não ser autorizados a aceder a informação do sistema.

Privacidade

A privacidade, mais do que uma propriedade de segurança, é um direito que assiste aos actores de um sistema e-Vote (Keller 2004; Neumann 2005). Por esta razão nenhum mecanismo a ser implementado para suportar um requisito do e-Vote, poderá por em causa este direito. Consiste em manter o secretismo pessoal de informação, manter livre de monitorização e livre do acesso a actores não autorizados, tendo em linha de conta a confidencialidade e integridade da informação em causa.

1.5. Ameaças de segurança

Os computadores foram construídos para executar processos repetitivos com grande rapidez. Naturalmente, o seu mau uso pode provocar uma falha de segurança em larga escala e com repercussões insustentáveis (Whitson 2003).

Qualquer ataque a uma votação electrónica bem sucedido teria uma mediatização e um impacto enorme. Por esta razão, a segurança no voto

electrónico tem a maior relevância. Cada sub-processo eleitoral, ao ser informatizado, atrai uma série de ameaças de segurança sobre a informação que trata:

Recenseamento

Nesta fase as ameaças estão relacionadas com o registo de pessoas inexistentes, ou com o registo de pessoas em vários círculos eleitorais, ou ainda com a possibilidade de anulação do registo de eleitores, entre outras.

Validação da identificação

A informatização desta fase é um dos maiores entraves à implementação do voto electrónico. O facto desta fase poder ser feita não presencialmente, levanta uma série de questões identificadas por vários autores, tais como (Rubin 2001): venda de voto, coercibilidade, solicitação de voto, privação do voto, entre outras.

Recolha de votos (Rubin 2001; Gritzalis 2002)

Nesta fase, os grandes problemas identificados passam por:
- permitir ao eleitor ter a certeza de que o seu voto foi válido;
- que não existe mais do que um voto por eleitor;
- a integridade da informação;
- a não violação da privacidade do eleitor.

Contagem dos votos

Nesta fase os maiores receios demonstrados pelos autores passam pela contabilização de todos os votos válidos, do número de votos corresponder com o número de votantes, integridade da informação dos boletins de voto, entre outros.

1.5.1. Ataques/Ameaças de segurança

Os ataques na Internet são uma constante e requerem a frequente actualização dos sistemas operativos, de forma a tentar evitar mal

funcionamento e acções indesejadas. No decorrer duma votação electrónica. Estes ataques podem comprometer todo o processo eleitoral.

De seguida são identificados alguns destes ataques recolhidos na literatura (Rubin 2001):

Negação do serviço (Dos[1]) - A1

Consiste no congestionamento do servidor de tal forma que compromete o atendimento. Este tipo de ataque não requer grandes conhecimentos por parte do atacante, a resposta do mecanismo de defesa é moroso, podendo por em causa o direito de voto dos eleitores, inclusivamente, pode ser feito de uma forma selectiva.

Cavalo de Tróia – A2

Este ataque é muito comum nos dias de hoje e quase todos os utilizadores da Internet o conhecem ou foram vítimas do mesmo. Não requer grandes conhecimentos e a sua origem é muito difícil de saber. Pode comprometer o acesso por parte dos eleitores ao sistema de voto electrónico, negando a possibilidade de voto ou ainda alterar o sentido de voto.

"Spoofing" – A3

O "spoofing" consiste num atacante fazer-se reconhecer pelo sistema como um utilizador credenciado. Desta forma, é possível, votar-se por alguém que se abstivesse ou mesmo, negar o voto a alguém.

Ataques internos ao sistema – A4

Este tipo de ataque pode acontecer quando alguém, do próprio sistema, credenciado provoca vulnerabilidades ou falhas de segurança. São extremamente perigosos e difíceis de detectar, com consequências desastrosas, podendo por em causa todo o processo eleitoral.

Vírus – A5

[1] DoS – provém do Inglês "Denial of Service" – Negação do serviço

A existência de um vírus, tanto no cliente como no servidor, pode provocar a alteração do boletim de voto, comprometer a privacidade, entre outros.

Alterações de configuração – A6

O computador do votante pode ser manipulado através de código malicioso e provocar o desvio da página oficial do sistema de votação. Pode provocar falta de privacidade ou negação do direito ao voto.

Comércio de votos automatizado – A7

Pode ser desenvolvida uma ferramenta que pernita de uma forma remota a comercialização dos votos, o que pode comprometer a democracia implícita de uma eleição.

Coercibilidade – A8

O eleitor pode ser sujeito, de uma forma coerciva, a votar em determinado sentido, comprometendo a democracia.

No caso de qualquer um, destes ataques descritos ser bem sucedido, podem ser activadas determinadas acções comprometedoras para o processo eleitoral, por exemplo, sistema de janelas rápidas (“PopUp’s”) que podem permitir a publicitação ou influenciar a vontade do voto, o que comprometeria a liberdade de voto.

Na tabela 1, é apresentada a classificação das ameaças e a sua influência nas propriedades de segurança:

Propriedades/Ameaças	A1	A2	A3	A4	A5	A6	A7	A8
Confidencialidade		**X**		**X**		**X**		
Integridade		**X**		**X**	**X**	**X**		
Disponibilidade	**X**	**X**	**X**	**X**		**X**		
Autenticidade		**X**	**X**	**X**	**X**	**X**	**X**	**X**
Privacidade		**X**		**X**	**X**	**X**	**X**	**X**

Tabela 1 - Classificação das ameaças de acordo com as propriedades de segurança

1.6. Tecnologias de Segurança

A tecnologia está em constante evolução e, com os recentes acontecimentos relacionados com actos de terrorismo, associados a um maior recurso às tecnologias de informação e comunicações em diversos domínios da actividade económica e social, as tecnologias de segurança têm assumido, cada vez mais, um papel de destaque. Existem já diversas tecnologias desenvolvidas para funções que procuram garantir, com maior ou menor grau de flexibilidade e segurança, as propriedades de segurança e direitos a salvaguardar num sistema E-Vote (Malkhi 2002). A exaustiva descrição de todas as tecnologias e suas variantes seria proibitiva no contexto deste trabalho pelo que foram seleccionadas as tecnologias de segurança que estão de acordo com um estudo recente "2005 CSI/FBI Computer Crime and Security Survey" (CSI/FBI 2005) consideradas as mais utilizadas no contexto das organizações, com esta ordem (Kaeo 1999; Grance 2003):

Firewall (TS1)

Firewall significa em língua Portuguesa "Parede de Tiro". De facto o termo ajuda a compreender a utilidade de um *Firewall*. Este pode ser implementado num aparelho (Hardware) ou num programa (Software). Consiste em estabelecer num único ponto de passagem numa comunicação entre computadores. É utilizado nas empresas como interligação entre o acesso à Internet e a rede interna. Desta forma, as comunicações dos computadores da rede interna passam pelo *Firewall* e só depois seguem para o destino exterior, e as comunicações vindas do exterior passam pelo mesmo antes de alcançarem o computador de destino na rede interna.

No Firewall é possível definir regras que permitem funcionar como filtros de comunicação, podendo-se proibir destinos, tanto internos como externos, de modo a salvaguardar informação crítica. Este tipo de tecnologia de segurança pode suster ataques do tipo DoS[2].

[2] DoS – do Inglês Denial of Service – Negação do Serviço

No caso do e-Vote esta tecnologia poderá ser útil na filtração de computadores que acedem a servidores do sistema de voto electrónico. Por exemplo, depois do eleitor ser identificado e autenticado, pode a sua ligação ser feita a um outro servidor que sirva de urna electrónica e este estar com uma *firewall* activada de modo a só permitir comunicações a computadores já identificados e reconhecidos pelo sistema.

Software Antivírus (TS2)

São aplicações residentes que permitem identificar vírus, "*worms*" e código maléfico. Estes, normalmente, são pequenos programas escondidos, residentes e de fácil propagação. A protecção contra este tipo de ataque tem de ser feita de várias formas: prevenção, detecção, isolamento e recuperação. Estas aplicações, usualmente, utilizam variadas técnicas para resolução de ataques deste tipo.

No caso concreto do e-Vote, esta tecnologia de segurança é tão relevante no lado do servidor, como no computador que o eleitor está a utilizar. Qualquer alteração de configuração conseguida por este tipo de ataque pode inviabilizar todo o processo eleitoral.

Sistemas de Detecção de intrusão (TS3)

Este tipo de tecnologia de segurança consiste numa aplicação que analisa as acções tomadas perante o sistema e de acordo com os privilégios dos actores determina se é uma ameaça ou não. Isto pode ser feito de duas formas: tendo como adquirido determinado perfil de acções e se estatisticamente for muito diferente, automaticamente considera como uma ameaça ou confrontando a série de acções com um perfil conhecido como ataque.

No caso do e-Vote esta ferramenta de segurança é necessária para prevenir eventuais ataques de actores internos do sistema.

Lista de controlo de acesso (TS4)

Lista de controlo de acesso consiste no registo de perfis de acções dos actores autorizados e por cada acção requerida o sistema confronta-a com as acções autorizadas para aquele actor. Deste modo, é possível controlar o acesso de cada um dos actores perante o sistema.

No caso do e-Vote esta ferramenta permite definir quem tem acesso e ao que tem acesso ao nível de informação e processos de suporte ao sistema.

Cifra de dados em transporte (TS5)

Por defeito as comunicações entre dois computadores é feita de modo aberta, ou seja, a informação contida nas mensagens é completamente aberta a qualquer ataque de intersecção da mensagem. Por esta razão é necessário o uso de sistemas de encriptação de forma a não revelar o conteúdo das mensagens, evitando o comprometimento do direito à privacidade, e as propriedades de integridade e confidencialidade.

Contas de utilizadores/login (TS6)

As contas de utilizadores são usadas para definir quem são os actores do sistema autorizados, para se proceder a acções de identificação e autenticação perante o sistema ao longo de todo o processo eleitoral.

Cifra de ficheiros (TS7)

Da mesma forma que existe a necessidade de cifrar a informação durante o seu transporte, também é necessário que esta seja cifrada durante o armazenamento. Esta tecnologia permite evitar que seja possível aceder a informação que não lhe é destinada.

Smartcards (TS8)

Os smartcards são cartões do tamanho de cartões de crédito, com um chip embebido, que podem ser programáveis ou não. São utilizados essencialmente na fase de identificação e autenticação perante o sistema.

Infra-estrutura de chaves públicas (TS9)

Este tipo de tecnologia de segurança funciona da seguinte forma: cada actor (humano ou não) é possuidor de um par de chaves electrónicas. Uma delas é pública e a outra privada. Quando o sujeito A envia informação ao B cifra-a com a chave pública do sujeito B. Este ao recebê-la poderá decifrá-la através da sua chave privada e vice-versa. No caso do e-Vote esta ferramenta pode ser utilizada para o eleitor cifrar o seu boletim de voto, submetê-lo ao servidor (urna electrónica) e apenas este, poderá com a sua chave privada, decifrar o boletim e proceder ao seu armazenamento, sem ter conhecimento do eleitor que o enviou, quando muito pode ter conhecimento do computador que foi utilizado (Mary R. Thompson 2003).

Biometria (TS10)

Biometria consiste na utilização de uma característica física ou comportamental humana como forma de identificação e autenticação perante o sistema. Poderá ser uma alternativa ao SmartCard ou complemento. Pode ser usado para controlo de acesso físico, electrónico e monitorização.

Seguidamente, irá ser apresentada uma tabela que classifica as tecnologias de segurança quanto ao suporte das propriedades de segurança. Esta classificação é baseada no guia de selecção de tecnologias de segurança, do NIST[3] (Grance 2003; Pereira 2005).

Propriedades/TS	TS1	TS2	TS3	TS4	TS5	TS6	TS7	TS8	TS9	TS10
Confidencialidade	**2**		**2**	**3**			**3**	**2**	**2**	**2**
Integridade	**2**	**2**	**2**	**3**		**1**	**3**	**2**	**2**	
Disponibilidade	**2**	**2**	**3**							
Autenticidade	**2**	**1**	**2**	**3**	**3**	**3**	**3**	**3**	**3**	**3**
Privacidade	**2**		**3**	**2**	**2**	**2**	**3**	**2**	**2**	**3**

Tabela 2 - Classificação de Tecnologias de Segurança

Esta classificação deverá ser avaliada através de um questionário de medição de eficiência, de forma a tornar mais clara a sua adopção no plano de protecção de ameaças, no âmbito da gestão do risco. No contexto deste trabalho, é considerada a seguinte escala de classificação: - nível 3: na

[3] NIST – National Institute of Security Technologies

literatura é mencionado que a tecnologia suporta a propriedade; nível 2: embora a literatura não o mencione de forma clara, esta está implícita; - nível 1: não existe qualquer menção explícita ou implícita do suporte da tecnologia na literatura, mas admite-se que possa suportar.

1.7. Gestão do risco

A gestão do risco é uma das actividades mais frequentes quando as organizações têm em linha de conta a segurança de sistemas da informação (Krause 1998; Whitson 2003). Consiste num conjunto de práticas, procedimentos com carácter cíclico, definidas pelas seguintes etapas:

- Identificação de informação crítica;
- Análise e cálculo do risco, com base: no valor, na probabilidade e impacto que a concretização de uma ameaça sobre a informação crítica;
- Planificação de medidas de segurança a adoptar; implementação das medidas; monitorização e controlo das mesmas.

1.8. Política de Segurança

Um dos produtos fundamentais da fase de planeamento da gestão de risco é a política de segurança (ISO/IEC 1996; Krause 1998; ISO/IEC 2000). Uma Política de Segurança consiste num conjunto de regras, directrizes e procedimentos que regulamentam a forma como uma organização protege, distribui ou controla a informação que considera sensível, nos vários níveis de acesso ou de procedimentos de uma forma granular (Peltier 1998; Walker 1998; Jackie Rees 2000).

Na construção de uma política de segurança é necessário:

- A reflexão e implementação dos objectivos da organização, de acordo com o fim a que se destina. No caso do e-Vote, estes objectivos são materializados em requisitos;
- A análise da informação, dos actores e dos sistemas tecnológicos ou não, que são utilizados no seu manuseamento;
- A análise das tecnologias de segurança que irão suportar a implementação das medidas de segurança.

Os aspectos não tecnológicos que devem, igualmente, fazer parte da política de segurança tais como: acessos físicos, catástrofes naturais, entre outros, são considerados fora do âmbito deste trabalho, podendo ser disseminados através da norma ISO/IEC 17799.

2. Método de criação de Políticas de Segurança no E-Vote

Como já foi referido, os sistemas e-Vote podem ser de vários tipos presencial ou não presencial, completamente suportados por tecnologias ou parte deles. Necessariamente, diferentes sistemas e-Vote implicam diferentes políticas de segurança. Este facto faz, com que haja a necessidade da criação de um método de construção de políticas de segurança.

Existem vários guiões, normas e princípios de segurança, tais como: Common Criteria (ISO/IEC 1999), critério OCATVE (Dorofee 2001), ISO 17799, ISO 13335 que definem linhas orientadoras na construção de métodos de segurança. O OCTAVE incentiva mesmo a que se criem métodos baseados na sua linha orientadora.

O critério OCTAVE aborda as três primeiras fases da gestão de risco (ver figura 1): identificação; análise e planeamento. O método de construção de políticas de segurança no e-Vote aqui proposto baseia-se neste critério. A razão da escolha prende-se pelo facto de este ser suficientemente genérico, não ter nenhum método específico implícito e com a área de acção limitada.

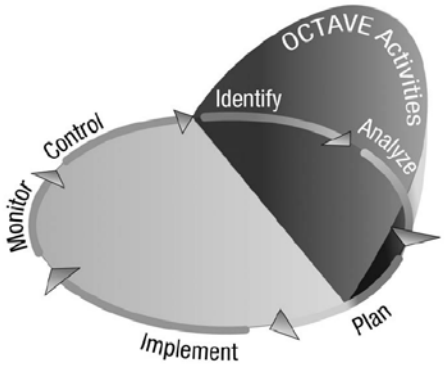


Figura 1 - Critério OCTAVE[SM]

2.1. Descrição do método

Na figura 2, está de uma forma sucinta, a descrição das fases do método enquadradas com as fases abordadas pelo critério OCTAVE[SM.4], Na figura 3, é explicado o processo de uma forma mais operacional.

Na primeira fase, segundo OCTAVE, é necessário:

[4] OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation

- Identificar os objectos de informação críticos: No caso do e-Vote, toda a informação é considerada crítica.

- Definir os requisitos de segurança da informação crítica:

Para definirmos os requisitos de segurança, e de acordo com os princípios mencionados na norma ISO 17799 e ISSO 13335, iremos analisar, para cada informação, as propriedades de segurança adaptadas ao e-Vote, anteriormente mencionadas: confidencialidade, integridade, disponibilidade, autorização e privacidade. Para tal, serão analisados quais os actores do e-Vote que lidam com a informação e a forma como o fazem.

- Identificação de ameaças

As ameaças serão identificadas com base nas ameaças definidas, anteriormente, e de acordo com as propriedades de segurança. A avaliação destas ameaças carece de medição de Impacto, probabilidade de acontecer, que será alvo de análise na terceira fase.

- Identificação de vulnerabilidade

Após a análise da avaliação das ameaças, serão identificadas, prioritariamente, as vulnerabilidades a que o sistema de e-Vote em estudo tem.

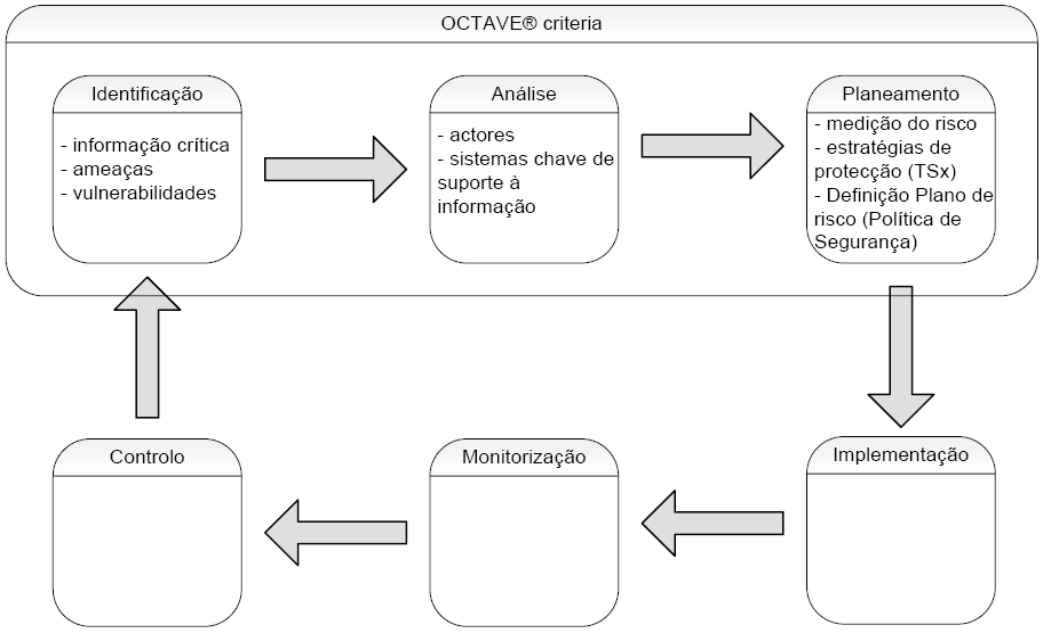


Figura 2 - Método enquadrado no critério OCTAVE[sm]

Na segunda fase:

- Identificação de sistemas chave e vulnerabilidades da tecnologia de suporte usada.

Nesta fase é necessário identificar quais os sistemas chave que lidam com a informação crítica e com os actores que a manuseiam.

Seguidamente, devem ser analisadas as vulnerabilidades que a tecnologia de suporte ao sistema apresenta. No caso do e-Vote é necessário analisar vulnerabilidades impostas pelos requisitos.

Na terceira fase:

- Medição do risco

Será feita uma medição das ameaças de forma a identificar o Impacto e probabilidade para cada uma das propriedades de segurança. Quantificando-se, desta forma, o risco de segurança.

- Estratégia de protecção

A estratégia de protecção passa pela definição de responsabilidades, de novos procedimentos e da adopção das tecnologias de segurança.

Atendendo às diferentes características destas tecnologias, ao seu âmbito de utilização e ainda porque nenhuma delas confere, isoladamente, uma solução cabal, a sua selecção e implementação num sistema e-Vote é uma tarefa complexa e, habitualmente, com pouca clareza quanto ao papel concreto que dada tecnologia de segurança está a desempenhar em determinado requisito.

As tecnologias, identificadas no capítulo 1, na secção 6, tecnologias de segurança, estão classificadas com as propriedades de segurança, ver Tabela 1. As ameaças estão classificadas da mesma forma, sendo possível seleccionar as tecnologias de uma forma adequada às necessidades de segurança em causa.

- Definição do plano de risco

Após a definição da estratégia de protecção, o plano de risco é materializado na definição da política de segurança, como guia de suporte dos requisitos do sistema e-Vote, seguindo-se as seguintes fases da gestão de risco: implementação, monitorização e controlo.

Esta política de segurança deverá ser alvo de constante actualização, através de: monitorização da sua implementação, o aparecimento de novas vulnerabilidades e de novas tecnologias de segurança, ou ainda o melhoramento das existentes.

3. Estudo de Caso

3.1. Descrição do sistema

O sistema e-Vote em estudo trata-se de um sistema desenvolvido pelo Departamento de Sistemas de Informação da Universidade do Minho. Este sistema visa suportar as eleições para o cargo de director do departamento, servindo de piloto para suportar as eleições internas da universidade, entre elas a do reitor da Universidade.

Pelo facto de ser um sistema já implementado, o documento que descreve a arquitectura do sistema na sua versão 1 (Santos 2004), já contempla as tecnologias de segurança usadas, Este facto, criou a necessidade de construir numa linguagem visual, o UML[5], a definição de requisitos que servirá de base de trabalho, o qual está descrito nos anexos 1,2 3, 4 e 5.

O sistema está dividido em cinco fases: criação da comissão eleitoral; criação da eleição (listas); criação do caderno eleitoral (recenseamento); votação; contagem dos votos.

Criação da comissão eleitoral

Esta comissão, constituída por três elementos, solicita ao administrador do sistema que lhe seja facultada uma identificação, mediante a respectiva informação sobre os elementos que a compõem. Esta fase deu origem ao seguinte processo “P1 – Pedir Credencial”.

Criação de uma eleição

A criação da eleição, das listas e restante o processo é da responsabilidade da comissão eleitoral, ficando o administrador do sistema com a responsabilidade de manter o sistema disponível, para o efeito. A comissão eleitoral acede ao sistema para criar a eleição, fornecendo todas as

[5] UML – Unified Modeling Language

informações relativas à mesma. Esta fase dá origem ao processo “P2 – Criar Eleição”.

Criação do caderno eleitoral

É da responsabilidade da comissão eleitoral criar o caderno eleitoral e recensear os eleitores e criar as listas concorrentes.

O eleitor poderá consultar as listas, através de uma publicação do sistema, efémero que o administrador do sistema disponibiliza. Esta fase da origem aos seguintes processos: “P3.1 – Criar Caderno Eleitoral”; “P3.2 – Recensear Eleitor”.

Votação

Para o eleitor poder votar, terá de identificar-se perante o sistema, e essa identificação será confrontada com o caderno eleitoral, sendo descarregado. Seguidamente, o eleitor acede ao sistema onde poderá ver o boletim de voto e submeter o seu voto ao sistema. O sistema está preparado para manter o anonimato do eleitor, e guarda o voto sem qualquer identificação do eleitor. Esta fase dá origem aos processos: “P4.1 – Verificar Caderno Eleitoral”; “P4.2 - Votar”.

Contagem dos votos

No final da votação, a comissão eleitoral poderá aceder ao sistema e proceder à contagem dos votos, e verificação da mesma. É elaborada uma acta da eleição onde constam todas as informações inerentes à eleição. A comissão poderá dar como encerrado o processo eleitoral. Esta fase dá origem aos seguintes processos: “P5.1 – Contar os votos”; “P5.2 – Verificar contagem”.

3.2. Aplicação do método

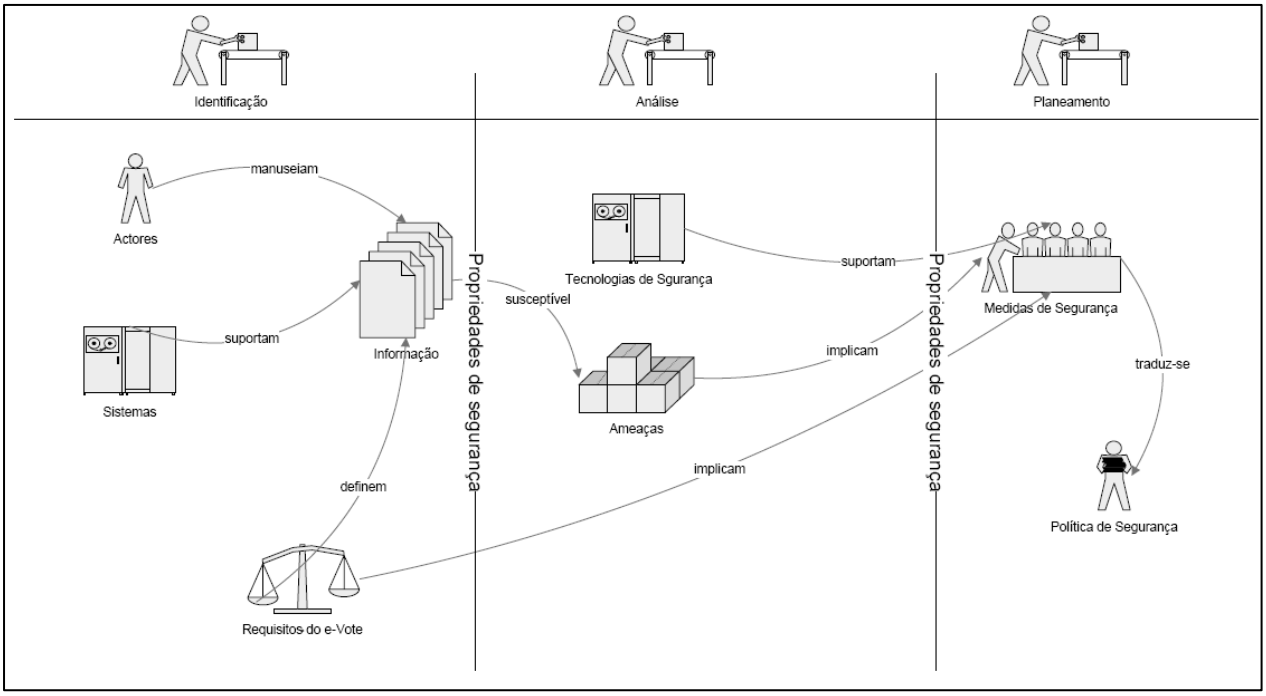


Figura 3 - Método proposto de construção de políticas de segurança

Com base nos diagramas de caso de uso, diagramas de sequência e diagrama de classes, anexos 1,2,3, 4 e 5 procedeu-se à aplicação do método proposto, de acordo com a figura 3.

3.2.1. Fase 1

Identificação de Informação Crítica

Como foi referido, dada a particularidade dos sistemas de voto electrónico, toda a informação é considerada crítica.

Identificação de Ameaças

As ameaças tidas em conta para o método são as enunciadas no capítulo 1, na secção 5.

3.2.2. Fase 2

Identificação de actores e processos chave

Para cada informação descrita no diagrama de classes, anexo 3, foram identificados os processos que a suportam e os actores que a manuseiam. Esta identificação deu origem à seguinte tabela:

		Actores			Processos							
		Ac1	Ac2	Ac3	P1	P2	P3.1	P3.2	P4.1	P4.2	P5.1	P5.2
Info1	Comissão Eleitoral	**X**			**X**	**X**	**X**				**X**	**X**
Info2	Eleição		**X**	**X**		**X**		**X**	**X**	**X**	**X**	**X**
Info3	Eleitor		**X**	**X**			**X**	**X**	**X**	**X**		
Info4	Lista		**X**	**X**		**X**				**X**	**X**	**X**
Info5	Caderno Eleitoral		**X**	**X**			**X**	**X**	**X**	**X**	**X**	**X**
Info6	Urna		**X**	**X**						**X**	**X**	**X**
Info7	Administrador	**X**			**X**							

Tabela 3 - Identificação de Processos e Actores

Em que, “Ac1” – corresponde ao Administrador, “Ac2” – Comissão Eleitoral e “Ac3” – Eleitor.

De seguida, obteve-se quais os processos que determinado actor utiliza, dando origem à tabela seguinte:

	Processos							
Actores	P1	P2	P3.1	P3.2	P4.1	P4.2	P5.1	P5.2
Ac1	**X**				**X**			
Ac2	**X**	**X**	**X**	**X**	**X**		**X**	**X**
Ac3					**X**	**X**		

Tabela 4 - Processos que os actores utilizam

Seguidamente, procedeu-se ao mapeamento dos processos e actores com as propriedades de segurança, que no caso de concretização de uma ameaça, podem ser afectadas, como descrito na seguinte tabela:

	Actores			Processos							
	Ac1	Ac2	Ac3	P1	P2	P3.1	P3.2	P4.1	P4.2	P5.1	P5.2
Confidencialidade	X	X	X	X		X		X	X		
Integridade	X	X	X	X	X	X		X	X		
Disponibilidade	X	X		X	X				X		
Autenticidade	X	X	X	X		X	X	X	X	X	X
Privacidade	X	X	X	X		X	X	X	X		

Tabela 5 - Relação de processos e actores com as propriedades de segurança

De seguida, a tabela anterior foi confrontada com a tabela de ameaças (ver tabela 1), através das propriedades de segurança que são o ponto comum entre as duas. Obtendo-se a seguinte tabela:

	Actores			Processos							
Ameaças	Ac1	Ac2	Ac3	P1	P2	P3.1	P3.2	P4.1	P4.2	P5.1	P5.2
A1	D	D		D	D				D		
A2	CDIAP	CDIAP	CIAP	CDIAP	DI	CIAP	AP	CIAP	CDIAP	A	A
A3	DA	DA	A	DA	D	A	AP	A	DA	A	A
A4	CDIAP	CDIAP	CIAP	CDIAP	DI	CIAP	AP	CIAP	CDIAP	A	A
A5	IAP	IAP	IAP	IAP		IAP	AP	IAP	IAP	A	A
A6	CDIA	CDIA	CIA	CDIAP	DI	CIAP	AP	CIAP	CDIAP	A	A
A7	AP	AP	AP	AP		AP	AP	AP	AP	A	A
A8	AP	AP	AP	AP		AP	AP	AP	AP	A	A
R1	0.95	0.95	0.80	0.95	0.95	0.95	0.90	0.85	0.99	0.80	0.80
R2	0.90	0.95	0.70	0.95	0.50	0.50	0.50	0.80	0.99	0.50	0.30

Tabela 6 - Identificação de ameaças sobre os processos e actores

Em que, C – Confidencialidade, I – Integridade, D - Disponibilidade, A – Autenticidade, P – Privacidade. O actor “Ac1- Administrador” está sujeito à ameaça “A2 – Cavalo de Tróia” em todas as propriedades de segurança.

3.2.3. Fase 3

Depois de obtermos as ameaças sobre processos e actores as fases 1 e 2 do método estão concluídas. Passaremos a terceira que consiste em:

- medição do risco através do R1 e R2 que são, respectivamente, Impacto e Probabilidade. Estes itens foram atribuídos, para o efeito, de uma forma consciente, carecendo de validade através de um inquérito, ver ponto 5 da secção 2, capítulo 3;
- Definição de estratégias e medidas de protecção a adoptar;
- A elaboração de uma política de segurança do sistema e-Vote.

Para tal, foram analisadas as tabelas: de tecnologias de segurança (ver tabela 2), a tabela 4 e tabela 5, tendo como parte comum as propriedades de segurança, dando origem à tabela seguinte:

	Actores			Processos							
Tec. Segurança	Ac1	Ac2	Ac3	P1	P2	P3.1	P3.2	P4.1	P4.2	P5.1	P5.2
R1	0.95	0.95	0.80	0.95	0.95	0.95	0.90	0.85	0.99	0.80	0.80

R2	0.90	0.95	0.70	0.95	0.50	0.50	0.50	0.80	0.99	0.50	0.30
TS1	CDIAP	CDIAP	CIAP	CDIAP	DI	CIAP	AP	CIAP	CDIAP	A	A
TS2	DIA	DIA	DIA	DIA	DI	IA	A	IA	DIA	A	A
TS3	CDIAP	CDIAP	CIAP	CDIAP	DI	CIAP	AP	CIAP	CDIAP	A	A
TS4	CIAP	CIAP	CIAP	CIAP	I	CIAP	AP	CIAP	CIAP	A	A
TS5	AP	AP	AP	AP		AP	AP	AP	AP	A	A
TS6	IAP	IAP	IAP	IAP	I	IAP	AP	IAP	IAP	A	A
TS7	CIAP	CIAP	CIAP	CIAP	I	CIAP	AP	CIAP	CIAP	A	A
TS8	CIAP	CIAP	CIAP	CIAP	I	CIAP	AP	CIAP	CIAP	A	A
TS9	CIAP	CIAP	CIAP	CIAP	I	CIAP	AP	CIAP	CIAP	A	A
TS10	CAP	CAP	CAP	CAP		CAP	AP	CAP	CAP	A	A

Tabela 7 - Cobertura das tecnologias de segurança

Os valores R1 e R2 foram transportados da tabela 6.
Podemos constatar que, apenas, as tecnologias TS1, TS2 e TS3, suportam a disponibilidade.

Com base nos valores de impacto e probabilidade de ameaça sobre os processos e actores do sistema, e com a cobertura que cada tecnologia dá aos mesmos, podemos definir o nível de segurança que pretendemos. No caso de ser necessário maior nível de segurança, opta-
-se por combinar o uso de várias tecnologias, ou na mesma tecnologia, como é o caso da encriptação, podemos optar por maior ou menor grau de complexidade (ex.: a 64 ou 128 bits).

3.2.4. Política de Segurança

De acordo com os requisitos do sistema de voto electrónico descritos no capítulo 1, na secção 3 foi elaborada a política de segurança geral e com base nas tabelas 3,4, 6 e 7 do método de construção foi construída a parte funcional da política de segurança, que ficou com a seguinte redacção:

Segurança Geral
O sistema de voto electrónico (SVE) tem de permitir a verificação de todos os processos, através de um sistema tipo histórico. Deve suportar as auditorias ao sistema. Deve ser robusto e suportar mecanismos de tolerância a falha, permitindo ao eleitor retomar o processo de votação, no caso de alguma

anomalia ou falha o ter interrompido. O sistema deve estar durante todo o processo eleitoral disponível para todos os eleitores.
O eleitor devidamente inscrito no caderno eleitoral, só poderá votar uma só vez no mesmo processo eleitoral.

Segurança Funcional

Administrador
O administrador do sistema é responsável pela disponibilidade do sistema de voto electrónico, pela atribuição da credencial à comissão eleitoral. As informações que este manuseia são: “Info1 – Comissão Eleitoral”, “Info4 – Caderno Eleitoral” e “Info6 – Administrador”. O administrador está sujeito a todas as ameaças em todas as propriedades de segurança, em especial, as ameaças: “A2 - Cavalo de Tróia”, “A4 – Ataques internos” e “A6 – Alterações de configuração”. Todas as tecnologias de segurança devem ser tidas em consideração, ver tabela 7, sendo as mais abrangentes: “TS1 – Firewall”, “TS3 - Detecção de Intrusão” e “TS4 – Controlo de acesso”. Os níveis de risco deste papel são elevados, sendo considerado o impacto de 0.95 e a probabilidade de 0.90.

Comissão Eleitoral
A comissão eleitoral é responsável por todo o processo eleitoral deste a sua criação até à contagem dos votos. A comissão eleitoral manuseia as seguintes informações: “Info2 – Eleição”, “Info3 – Eleitor”, Info4 – Lista”, “Info5 – Caderno Eleitoral”, “Info6 – Urna”. Está sujeita a todas as ameaças, sendo as mais abrangentes em relação às propriedades de segurança, as seguintes: “A2 – Cavalo de Tróia”, “A4 – Ataques internos” e “A6 – Alterações de configuração”. As ameaças afectam de uma forma, igualmente, abrangente os processos: “P1 – Pedir Credencial”, “P4.1 – Verificar Caderno Eleitoral” e “P4.2 – Votação”. Todas as tecnologias de segurança devem ser consideradas, ver tabela 7, sendo as mais abrangentes, face às propriedades de segurança, as seguintes: “TS1 – Firewall”, “TS3 - Detecção de Intrusão”,

“TS4 – Controlo de acesso”, “TS7 – Cifra de ficheiros”, “TS8 - Smartcards”, “TS9 – Chaves públicas” e “TS10 - Biometria”. Os níveis de risco são elevados, sendo considerado que o impacto e a probabilidade é de 0.95.

Eleitor

Os eleitores apenas tem contacto com o SVE nos processos “P4.1 – Verificar Caderno eleitoral” e “P4.2 – Votação”, as informações que manuseiam são: “Info2 – Eleição”, “Info3 – Eleitor”, “Info4 – Lista”, “Info5 – Caderno eleitoral”, e “Info6 – Urna”. As ameaças que os eleitores estão sujeitos são todas à excepção da “A1 – Negação do Serviço”, embora possam ser vítimas da mesma. As tecnologias de segurança devem ser todas consideradas, em especial as que protegem a privacidade e autenticidade, ver tabela 7. Pela sua abrangência, em relação às propriedades de segurança, são destacadas as seguintes tecnologias de segurança: “TS1 – Firewall”, “TS3 - Detecção de Intrusão”, “TS4 – Controlo de acesso”, “TS7 – Cifra de ficheiros”, “TS8 - Smartcards”, “TS9 – Chaves públicas” e “TS10 - Biometria”. Os níveis de risco são elevados, sendo considerados para o impacto 0.80 e para a probabilidade 0.70.

Esta política de segurança poderá estar sujeita a alteração, de acordo com: a evolução da tecnologia, o aparecimento de novas vulnerabilidades e auditorias à sua implementação.

3.2.5. Validação do método proposto

Como foi referido anteriormente o método propõe classificações de tecnologias e do impacto e probabilidade das ameaças com as propriedades de segurança. Estas classificações carecem de validação que deverá ser feita através de questionários a promover.

No caso da classificação das tecnologias o público-alvo terá de ser, o tanto quanto o possível, por entendidos na área de segurança, este inquérito ao validar a tabela de relacionamento de tecnologias de segurança com as

propriedades de segurança poderá ser utilizado noutros sistemas de voto electrónico sem haver a necessidade de validação.

No caso da classificação do impacto e probabilidade de ameaças, o público-alvo deve ser alargado a pessoas envolvidas na implementação do sistema de votação electrónica, entendidos na área e futuros eleitores que utilizem a ferramenta. Este questionário deverá ser específico para cada um dos sistemas de votação electrónica onde se aplique o método proposto, devido à especificidade dos sistemas.

O método seleccionado para promover os questionários é o “Delphi”. Este método (Liou 1990) consiste num questionário organizado por rondas que podem ser qualitativas ou quantitativas, em que as opiniões sobre os itens em estudo são partilhadas e as rondas seguintes são construídas a partir das respostas das anteriores.

As razões que levaram à adopção deste método prendem-se pelo facto deste tipo de método permitir obter juízos, conhecimento, opiniões ou ainda estabelecer objectivos e prioridades. Existe, também a possibilidade da implementação deste método em ambiente de Internet, sendo a disponibilidade de auscultação maior, pretendendo-se desta forma, o maior número de participantes.

Devido à escassez de tempo, não foi possível promover os questionários, de forma a validar o que se propõe. Terá de ficar, como trabalho futuro, esta validação.

3.2.6. Análise dos resultados

As tabelas 3,4,6 e 7 produtos do método proposto são uma mais valia, no que toca à definição de uma política de segurança, com indicação das tecnologias de segurança a utilizar, de uma forma adequada, tendo em conta os factores de risco (impacto e probabilidade).

Com este método é possível, de uma forma simples, ter uma visão global do sistema: o papel das tecnologias; as informações e processos, quem os manuseia e quem os utiliza; fundamentais na definição e implementação de uma política de segurança.

Conclusão

Um dos maiores entraves à implementação do voto electrónico é a confiança (Bannet 2003). Os eleitores têm de confiar no sistema que utilizam, os partidos têm de confiar nos resultados e legitimar os mesmos. Para tal, é necessário construindo a confiança com base na segurança de modo a suportar os requisitos de um sistema de voto electrónico (Rivest 2001).

Quando se trata de segurança em sistemas de informação é necessário ter em linha de conta a gestão do risco. Esta actividade, cíclica, permite que se actue de uma forma pró-activa perante ameaças a que o sistema está sujeito, salvaguardando as propriedades fundamentais da segurança.

Na gestão de risco, a informação é tratada como um bem das organizações, o que num sistema de votação electrónica e na perspectiva de construção de confiança, é fundamental (Shamos 1993). Um dos produtos pilares da gestão de risco é a política de segurança que rege os procedimentos pró-activos que uma organização deve ter.

Na política de segurança devem estar consagrados os papéis a desempenhar no sistema, quais os processos que são acedidos e quem os deve aceder, medidas de segurança, entre outros (Peltier 1998; Barman 2002).

Num sistema de voto electrónico onde toda a informação é crítica, os requisitos são exigentes, a construção da política de segurança deve ser feita de uma forma criteriosa e suportar tudo o que envolve o sistema, sem excepção. A definição de um método de construção de políticas de segurança torna-se fundamental.

O método para além de permitir a construção da política de segurança, permite-nos obter uma visão global do sistema, onde são conhecidas as ameaças, vulnerabilidades, papéis desempenhados, acessos à informação e, adequadamente, o suporte que determinada tecnologia de segurança está a

fornecer ao sistema. Para tal, foi usada como base comum as propriedades de segurança.

Trabalhos futuros

O próximo passo será validar os pressupostos deste método, a tabela de tecnologias de segurança e o impacto e probabilidade das ameaças em função dos processos e actores do sistema.

O método de construção de políticas de segurança, no âmbito deste trabalho, só suporta a parte de segurança tecnológica da informação. Seria interessante, desenvolver trabalhos que suportassem a parte de catástrofes naturais, segurança física, entre outros.

Outra possibilidade será o alargamento do método às restantes fases da gestão de risco: implementação, monitorização e controlo.

Com este método poderá ser possível desenvolver uma ferramenta que suporte todas as fases deste método e que permita gerar de uma forma automática a política de segurança.

Bibliografia

Bannet, J. e. a. (2003). "Hack-a-Vote: Demonstrating Security Issues with Electronic Voting Systems." Department of Computer Science, Rice University.

Barman, S. (2002). "Writing information security policies."

CSI/FBI (2005). Computer Crime and Security Survey, Computer Security Institute.

Dorofee, C. J. A. a. A. J. (2001). OCTAVE Criteria.

Ed Tittel, J. M. S. a. M. C. (2004). Certified Information Systems Security Professional. San Francisco, Sybex.

Grance, T. (2003). Guide to Selecting Information Technology Security Products, NIST - National Institute of Standards and Technology.

Gritzalis, D. (2002). "Principles and requirements for a secure e-voting system." Computers & Security **21**(6): 539-556.

ISO/IEC (1996). "Information technology - Guidelines for the management of IT Security - ISO/IEC 13335."

ISO/IEC (1999). Common Criteria for Information Technology Security Evaluation - ISO/IEC 15408.

ISO/IEC (2000). "Information Technology - Code of Practice for Information Security Management, ISO/IEC 17799."

ISO/IEC (2005). Information technology — Security techniques — Code of practice for information security management, ISO/IEC.

Jackie Rees, S. B. a. E. H. S. (2000). PFIRES: A Policy Framework for Information Securit. Americas Conference on Information Systems (AMCIS 2000), Long Beach, California, Association for Information Systems.

Kaeo, M. (1999). "Security Tecnhonologies." IinformIT.

Keller, A. M., David Mertz, Joseph Lorenzo Hall and Arnold Urken (2004). "Privacy Issues in an Electronic Voting Machine."

Kitcat, J. (2004). "Electronic Voting: I want to understand the issues." Retrieved 10-11-2004, 2004.

KOHNO, T. (2004). Analysis of an Electronic Voting System. Symposium on Security and Privacy, IEEE.

Krause, H. T. a. M. (1998). Handbook of Information Security Management, CRC Press LLC.

Liou, Y. I. (1990). Knowledge Acquisition: Issues, Techniques, and Methodology. ACM SIGBDP Conference on Trends and Directions in Expert Systems.

Malkhi, D. (2002). Electronic Voting Protocols and Schemes, The Hebrew University of Jerusalem, Israel.

Mary R. Thompson, A. E. a. A. S. M. (2003). "Certificate-based Authorization Policy in a PKI Environment." ACM Transactions on Information and System Security (TISSEC).

McGaley, M. a. J. M. (2004). Transparency and e-Voting:Democratic vs. commercial interests. Gesellschaft für Informatik, GI-Edition.

Mendes, M. d. F. and J. Miguéis (2005). LEI ELEITORAL DA ASSEMBLEIA DA REPÚBLICA - Anotada, Comissão Nacional de Eleições. **Lei 14/79**.

Neumann, P., Rebecca Mercuri, Lauren Weinstein (2000). "Internet and Electronic Voting." ACM Committee on Computers and Public Policy **21**(14).

Neumann, P. G. (1993). Security Criteria for Electronic Voting. 16th National Computer Security Conference, Baltimore, Maryland.

Neumann, P. G. (2005). Risks to the public: Risks to the public in computers and related systems. ACM SIGSOFT Software Engineering Notes, ACM Press.

Parth P. Vasa, e. a. (2005). Remote Poll-Site Voting, Johns Hopkins University.

Peltier, T. R. (1998). Information Security - Policies and Procedures.

Pereira, T. a. H. S. (2005). Tecnologias de segurança no e-Vote. 6ª Conferência da Associação Portuguesa de Sistemas de Informação, Bragança, Actas da 6ª CAPSI.

Peter Neumann, R. M., Lauren Weinstein (2000). "Internet and Electronic Voting." ACM Committee on Computers and Public Policy **21**(14).

Pitt, W. R. (2003). "Electronic Voting: What You Need To Know." Liberal Slant.

Rivest, R. L. (2001). Electronic Voting. Financial Cryptography '01, Grand Cayman, BWI, International Financial Cryptography Association.

Rosner, G. (2002). "Electronic Voting Protocols and Schemes Não usar."

Rubin, A. (2001). "Security Considerations for Remote Electronic Voting over the Internet." AT&T Labs – Research, Florham Park, NJ.

Santos, L. (2004). Arquitectura do sistema de voto electrónico do DSI - Versão 1.0, Universidade do Minho.

Shamos, M. I. (1993). Electronic Voting - Evaluating the Threat. CFP'93.

Walker, K. M. (1998). Computer security policies and sunscreen firewalls.

Whitson, G. (2003). Computer Security: Theory, Process and Managenment. Computer Science Department. Texas, The University of Texas as Tyler.

Xenakis, A. a. A. M. (2004). Procedural Security in Electronic Voting. 37th Annual Hawaii International Conference on System Sciences (HICSS'04), Oakland, CA.

Anexo 1 – Diagrama de caso de uso - geral

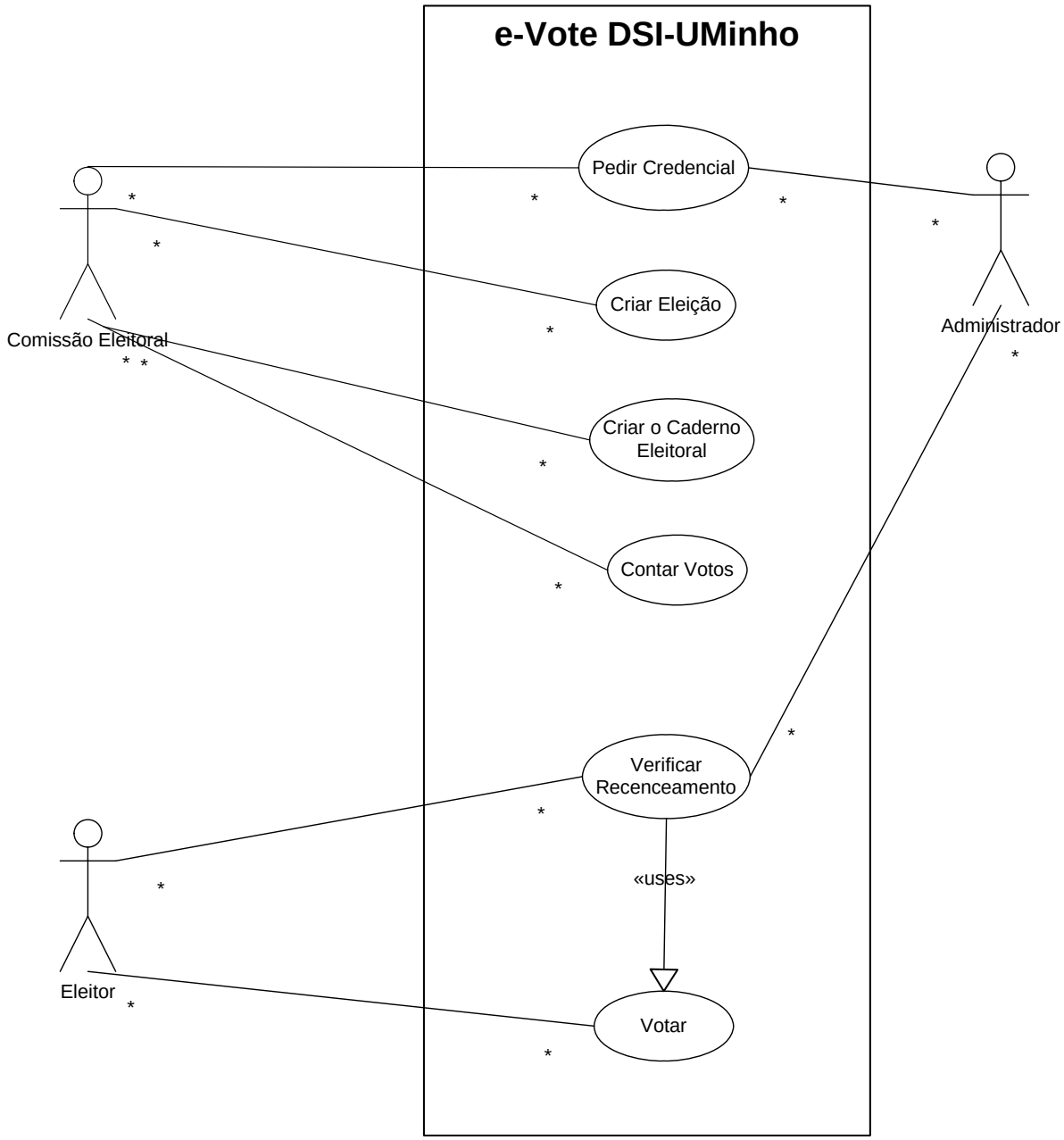
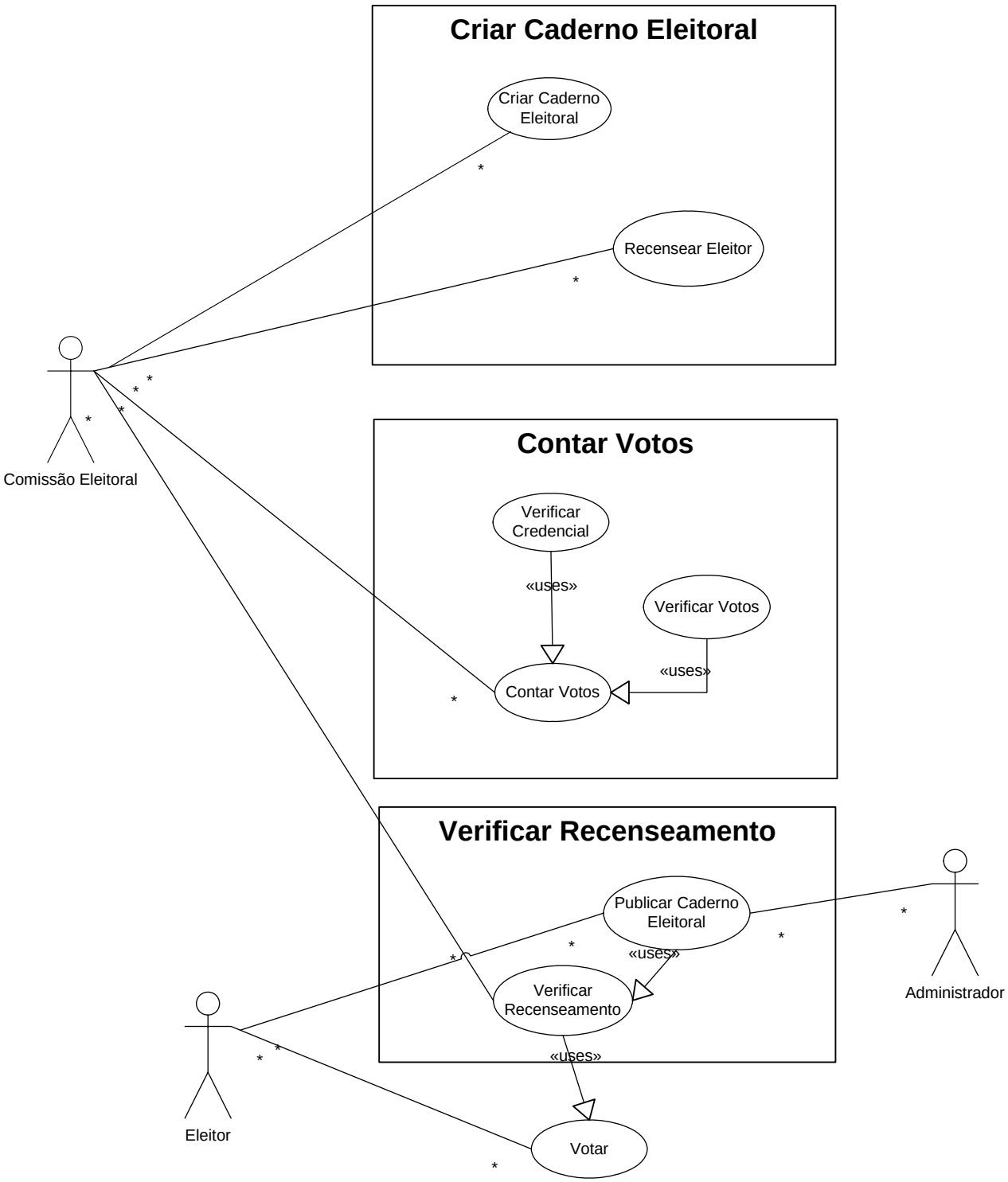
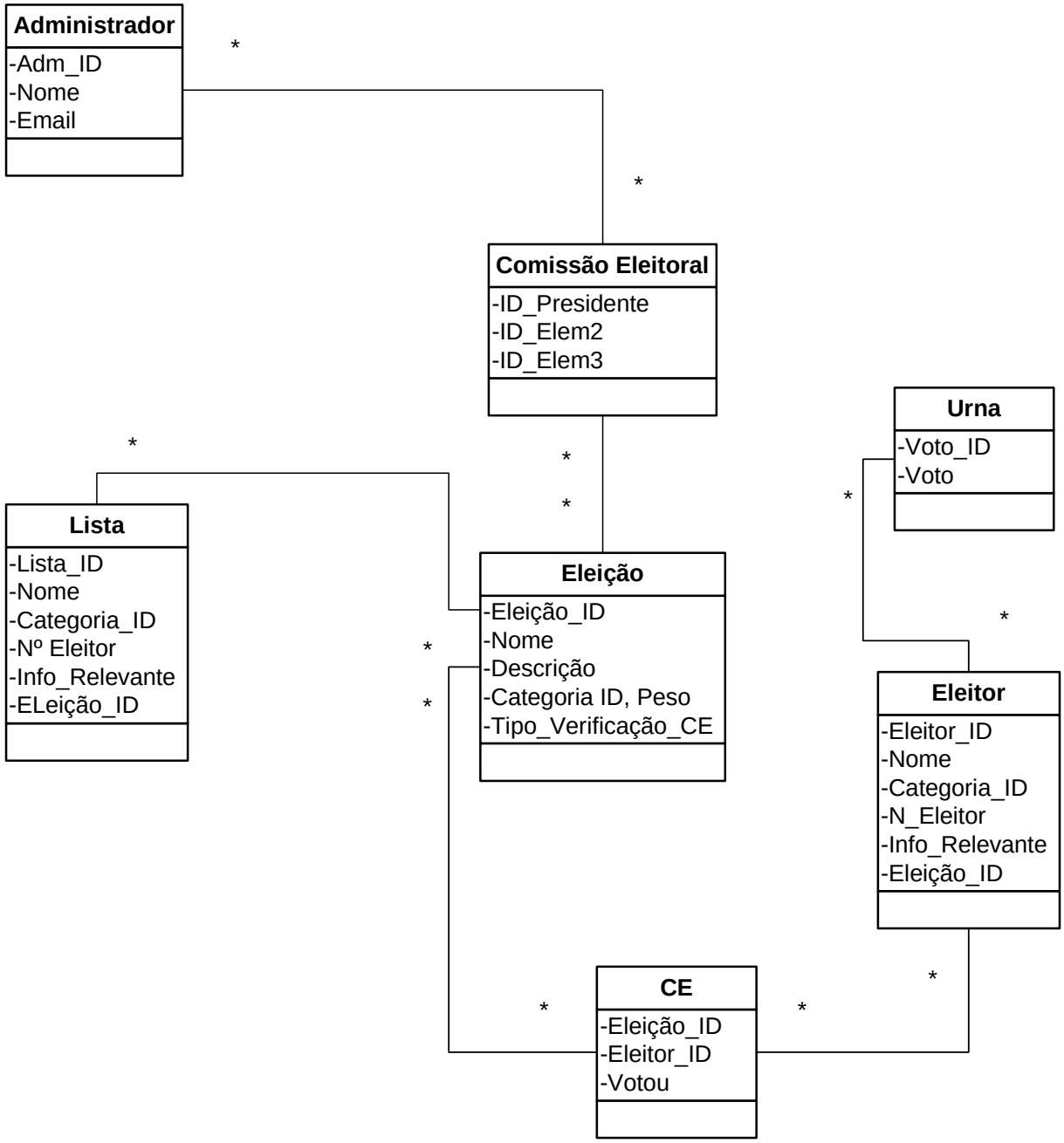


Diagrama de Caso de Uso - Geral

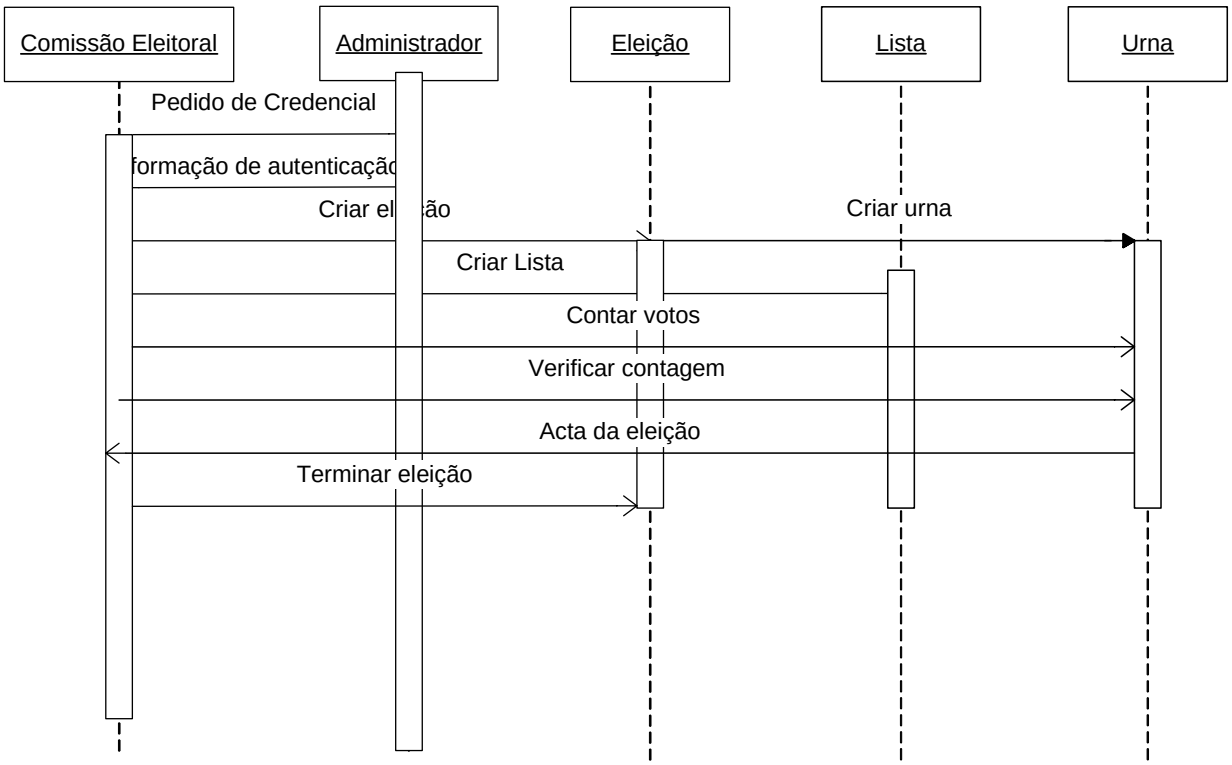
Anexo 2 – Diagrama de caso de uso – nível 2



Anexo 3 – Diagrama de Classes



Anexo 4 – Diagrama de Sequência – comissão eleitoral



Anexo 5 – Diagrama de Sequência - Eleitor