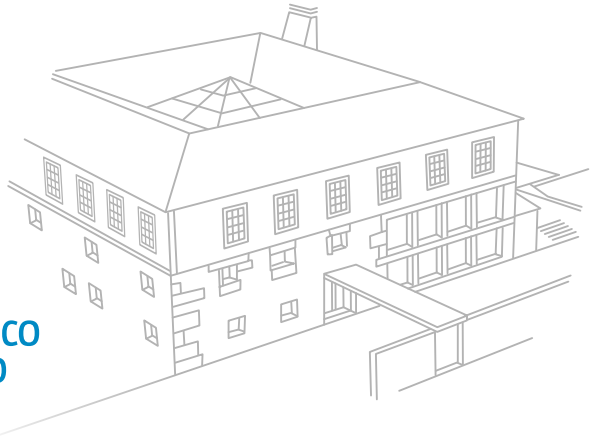


ESTGF | POLITÉCNICO DO PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Electronic Vote as a Service (E-VaaS)

DESIGNAÇÃO DO MESTRADO Mestrado em Engenharia Informática

AUTOR Abraham Da Silva Mesa

ORIENTADOR(ES) Ricardo André Fernandes Costa

Orientador 2

ANO 2014

Agradecimentos

Esta dissertação contou com importantes apoios e incentivos que foram cruciais para levar a bom porto o presente trabalho. A todos os que tornaram isto possível deixo algumas palavras de agradecimento e reconhecimento.

Ao meu orientador o Doutor Ricardo Costa pela orientação científica, compreensão, apoio e sobretudo paciência durante esta árdua etapa.

Às empresas Basepoint, nomeadamente ao Eng.º Pedro Almeida, e VentureOak, em especial ao Eng.º Pedro Almeida e ao Eng.º Miguel Garcia pelo incentivo e pela criação de condições necessárias para a conclusão deste trabalho.

À Escola Superior de Tecnologia e Gestão de Felgueiras / Instituto Politécnico do Porto e à Professora Doutora Dorabela Gamboa pela motivação e disponibilidade que sempre demonstrou para comigo.

Por último, mas não menos importante, quero agradecer à minha família, ao meu pai, avós, aos meus amigos e à minha namorada por todo o apoio e compreensão no decorrer desta fase.

Abstract

It is generally considered that a key component of electronic government in the future will be electronic voting, as a means of facilitating the participation of citizens in elections and public debates. However, a long path has to be pursued before electronic voting, particularly if based on Internet, is accepted as a reliable system alternative to conventional methods. In this dissertation, it is proposed a new and simple platform, based on open software, which can be used primarily in small to medium or even big sized communities. The core of this work was to implement cryptographic methods to ensure security and confidentiality in our elections using a Software as a Service approach to empower the election manager with all his needs, dynamically and elastically, without any additional concern.

Resumo

Considera-se que um componente-chave das instituições governamentais será o voto eletronico, na medida em que este irá tornar mais ativa a participação de todos os cidadãos nas eleições, referendos e debates públicos. No entanto, existe ainda um longo caminho a percorrer antes do voto eletrónico ser considerado, sobretudo via Internet, uma alternativa fiável e confiável face aos métodos mais tradicionais e convencionais.

Nesta dissertação é proposta uma plataforma simples, baseada em *software* livre, com diversos níveis de segurança, que pode ser usada principalmente em pequenas e médias votações, sobretudo em âmbitos mais fechados, nomeadamente pequenas e médias empresas, clubes de futebol, associações, instituições públicas, entre outros. Apesar disso, são considerados níveis de segurança e confidencialidade máximos, através da implementação de métodos criptográficos *state-of-the-art*, permitindo deste modo a aplicação da solução desenvolvida em votações mais complexas.

Adicionalmente, é proposta uma aproximação *Software as a Service*, que melhora a gestão de eleições, adaptando-se de forma dinâmica às necessidades reais, sem qualquer tipo de preocupação adicional para a comissão eleitoral. O objetivo é dinamizar todo o processo eleitoral, tornando-o em algo simples e seguro para todos os envolvidos.

Índice

Índice de Figuras

Indice de Tabelas

Siglas e acrónimos

AS – Authentication System.

BS – Ballot System.

DoS – Denial of Service.

EC – Election Commission (Comissão Eleitoral).

ECI – Electoral Circumscription Identifier (Circulo Eleitoral).

GNU – GNU's Not UNIX.

HTML – HyperText Markup Language.

JDBC – Java Database Connectivity.

LAN – Local Area Network (Rede Local).

MAN – Metropolitan Area Network (Rede Metropolitana).

PVE – Plataforma de Votação Electrónica.

SVE – Sistema de Votação Electrónica.

WAN – Wide Area Network (Rede Alargada).

VC – Vote Collector.

CRUD - acrónimo de Create, Read, Update e Delete na língua Inglesa.

1 Introdução

1.1 Contextualização

Votar é um ato que permite a um grupo de pessoas chegar a um consenso sobre uma determinada ideia, escolher um candidato para uma determinada tarefa ou apoiar uma determinada proposta [1]. Este tipo de ato evita problemas entre os eleitores dado que é escolhida a opção mais votada, obtida por um consenso [2].

Uma eleição pode ser feita para que não seja possível saber as escolhas dos eleitores, com o objetivo de manter o anonimato, evitando votos forçados por parte dos mesmos [3].
O voto pode ser feito de forma tradicional ou de forma eletrónica, sendo a última modalidade abordada no presente estudo.

Apesar de o voto eletrónico ser um meio de votação cada vez mais utilizado, a sua utilização é considerada ainda, nos dias de hoje, um tema tabu na sociedade atual, devido à desconfiança que ainda existe em relação a este tipo de votação, causada pela falta de garantias satisfatórias de que os votos estão a ser contados de forma correta e que a votação é realmente justa [4]. Contudo, o voto eletrónico tem sido pouco a pouco introduzido na nossa sociedade, começando a ser cada vez mais aceite graças à evolução dos métodos e tecnologias utilizados na sua implementação, que gradualmente preenchem as lacunas que contribuem para a existência da insegurança existente em relação a esta modalidade de votação.

O objetivo principal do voto eletrónico consiste em elevar o nível de segurança e aumentar o grau de confiabilidade das eleições garantindo a redução, ou mesmo mitigação, de erros humanos e a impossibilidade de adulterar os votos por formas normais [5]. Nesta dissertação é proposta uma plataforma *on-line,* disponibilizada como um serviço, na qual é possível uma pessoa ou conjunto de pessoas devidamente identificadas, escolher, iniciar e finalizar uma eleição.

Um dos problemas das votações eletrónicas incide sobre a segurança, pois um indivíduo que faz a votação tem de confiar na aplicação para efetuar o seu voto e esperar que este não seja adulterado ou que o seu anonimato seja violado [5].

Para resolver estes problemas é proposta uma abordagem usando técnicas criptográficas, de modo a evitar a existência deste tipo de problemas. São utilizadas técnicas de criptografia assimétrica e simétrica, assinaturas e funções de hash para obter um sistema robusto e confiável para o utilizador [6].

1.2 Objetivos

O presente estudo teve como finalidade a definição de uma plataforma de votação eletrónica [7] com capacidade para abranger uma grande área de aplicação/utilização. Um dos objetivos consistiu em desenvolver uma plataforma rápida e funcional, que fosse facilmente utlizada por todos aqueles que interagem com ela: administradores de sistemas, comissão eleitoral e eleitores. Esse sistema será disponibilizado sob a forma de serviço, seguindo os princípios do modelo *Software as a Service* (SaaS). Adicionalmente, tendo em vista a obtenção de um nível elevado de *performance,* o desejado nível de *performance*, é proposto um sistema seguro baseado em código *open source*.

Esta estratégia de introduzir os Sistemas de Votação Eletrónica (SVE's) gradualmente na vida social dos cidadãos é um ponto muito forte e de extrema relevância na nossa proposta. Deste modo, espera-se conseguir obter um nível de aceitação adequado, baseado na confiança e na usabilidade da plataforma. Além disso, será demonstrado que através do uso de tecnologias, a solução proposta incorpora papéis bem claros e percetíveis, nos mais variados níveis, demonstrando assim a transparência existente na globalidade dos sistemas e das suas componentes, sendo este um ponto-chave para obter a confiança dos seus utilizadores.

1.3 Estrutura do documento

O presente documento encontra-se organizado da seguinte forma:

- No capítulo 1 é apresentada uma introdução sobre o tema abordado na presente dissertação, bem como os objetivos da mesma e a estrutura do documento.
- No capítulo 2 é feita uma introdução ao voto eletrónico, são apresentados os tipos de voto eletrónico, propriedades, ameaças, tecnologias de segurança e o voto eletrónico como um *software as a service*.

- No capítulo 3 é apresentado o estado da *arte* dos sistemas de voto eletrónico, apresentando sistemas semelhantes ao desenvolvido e casos de sucesso de utilização de votações eletrónicas em diversos países.
- No capítulo 4 são apresentadas e descritas as propriedades necessárias para que seja possível existir o voto eletrónico.
- No capítulo 5 são apresentadas e descritas as técnicas criptográficas utilizadas no contexto do presente estudo, para cobrir as necessidades de segurança do voto eletrónico na aplicação desenvolvida.
- Por fim, no capítulo 6 é apresentada a aplicação *Electronic Vote as a Service* (e-VaaS), criada no âmbito do presente estudo.

2 Fundamentos Teóricos

2.1 Votação Tradicional

Votar é o ato através do qual um individuo escolhe uma ideia, proposta ou candidato para cumprir uma função [1], como apresentado na Figura 1. Este ato pode ser privado ou público, dependendo do âmbito e pode ser levado a cabo em vários contextos, desde pequenas empresas até nações inteiras. De uma forma simplista, pode afirmar-se que a votação é um método de tomada de decisão, na qual um grupo de pessoas, como por exemplo o eleitorado, chega a um consenso. Numa votação existe um comité cuja função é organizar, conduzir e controlar todo o processo eleitoral. Após o ato de votação, esse comité conta os resultados obtidos, que ficarão mais tarde ficam disponíveis publicamente para a sua leitura.

Este tipo de eleição nunca é vista como um problema que precisa de resolução, no entanto, existem inúmeras dificuldades, tais como:

- O processo de voto manual obriga o eleitor a deslocar-se até um ponto selecionado para efetuar a eleição, para identificar-se perante a votação como um eleitor autorizado e preencher um boletim com a sua escolha [8].

- É necessário ter em conta toda a logística e custos associados ao transporte dos boletins, que têm de chegar até o local das eleições [9].

- É necessária uma preparação prévia, que inclui a impressão dos boletins de voto, a garantia de que os boletins são entregues nos locais corretos e o transporte da urna para a localização respetiva. Todo este processo tem de ser executado com a maior segurança possível, sendo muitas vezes necessário recorrer a forças de segurança (polícia) [8].

- Neste tipo de eleição o ato de votar é um processo simples em que o eleitor tem de se deslocar fisicamente ao local assignado para a eleição, tal como fora referido anteriormente e exercer o seu direito de voto. Aparentemente é um processo seguro, todavia não está isento de falhas, dado que este processo é gerido por pessoas, estando deste modo mais exposto a falhas humanas.

- Os boletins de voto, após o fecho da eleição, são contados manualmente. Este processo pode tornar-se numa tarefa demorada, especialmente em contextos em que o número de eleitores dependendo da localização, especialmente em países elevado número de eleitores [10].

Figura 1: Exemplo de votação tradicional

2.2 Voto Eletrónico

O voto eletrónico é um sistema de voto no qual os dados da eleição são guardados, armazenados e processados como informação digital [7].

Figura 2: Exemplo de voto eletrónico[1].

2.2.1 Vantagens

O processo de voto eletrónico possui várias vantagens em relação ao voto tradicional, tais como:

- A votação tradicional não permite aos eleitores votar com comodidade, obrigando-os a deslocarem-se até aos locais designados para o processo de votação. Com o voto eletrónico esta situação não se verifica, pois este permite ao eleitor participar na eleição a partir de qualquer lugar, evitando deslocações e eliminando as questões de logística associadas ao processo de votação tradicional (ex.: arranjar locais apropriados para o efeito, contratar pessoas para a monitorização do processo, …). Assim, este fator contribui para o aumento do número de eleitores [3]. Esta abordagem é especialmente vantajosa para eleitores com mobilidade limitada. [8], [11].

[1] http://pulsosocial.com/2013/03/14/en-2013-america-latina-vota-en-que-situacion-se-encuentra-el-voto-electronico-en-la-region/

- O voto eletrónico, tal como apresentado na Figura 2, dotarão as eleições de um novo potencial, pois será possível integrar a funcionalidade de línguas, sendo possível a escolha da linguagem utilizada no sistema de votação de entre vários idiomas disponibilizados pela plataforma. Nos sistemas de votação tradicional apenas está disponível o idioma da nação na qual ela decorre, podendo ser um fator limitador em algumas circunstâncias. [3].

- No voto tradicional, os eleitores não têm qualquer garantia de que o seu voto tenha sido de facto contabilizado e de que este não tenha sofrido nenhum tipo de violação. Os eleitores não têm meios para averiguar a fiabilidade da autoridade elegida para a contagem de votos, não tendo por isso qualquer garantia de que o seu voto não será de alguma forma adulterado. Com o voto eletrónico pretende-se criar um sistema seguro que não permita qualquer tipo de adulteração dos votos, a aceitação de votos inadequados ou até mesmo duplicados, que podem levar a resultados errados e insatisfatórios [12].

.

Os sistemas de voto eletrónico atuais têm falhas de segurança graves, contrariando os requisitos básicos dos processos eleitorais. Qualquer sistema tecnológico tem vários recursos humanos responsáveis por funções distintas, o que leva a possíveis situações de erro humano ou de corrupção, aumentando deste modo as ameaças à segurança do processo [11].

Muitos sistemas de voto eletrónico foram propostos ao longo dos últimos anos, tendo cada deles trazido melhorias a questões relacionadas com a segurança e efetividade, contudo nenhum deles é ainda capaz de dar resposta ao problema de segurança de forma efetiva, para tornar este método completamente seguro e infalível [12].

A segurança é um dos fatores mais importantes a ter em conta, pelo que se deve ter muito cuidado na altura de escolher o material tecnológico necessário para implementar o processo de voto eletrónico. Uma escolha cuidada e acertada pode garantir o cumprimento de todas as necessidades de segurança deste método. [12].

2.2.2 Possibilidades do Voto Eletrónico.

Existem várias previsões e resultados de aplicação do processo de voto eletrónico. Abaixo serão enunciados e explicados sucintamente alguns deles:

- Muitos países preveem que o voto eletrónico será disponibilizado para levar a cabo as suas eleições já na próxima década [3].

- O voto eletrónico ajudará as pessoas fisicamente limitadas, conferindo-lhes uma oportunidade para participar em processos de votação de uma forma mais facilitada [3].

- Uma grande quantidade de países pretende que a adaptação ao voto eletrónico comece rapidamente com uma pequena aplicação, de forma a comprovar se o sistema cobrirá as suas necessidades de votação e se irá melhorar o sistema de votação do país [3].

- Uma grande quantidade de países sente alguma frustração com a limitação das opções disponíveis do processo voto tradicional. O sistema de voto eletrónico poderia mitigar as dificuldades encontradas nos sistemas tradicionais, sendo por isso a sua aplicação uma mais-valia para estes países[3].

- Uma grande quantidade de países vê vantagens na utilização de ecrãs tácteis para o voto eletrónico [3].

2.2.3 Tipos de Voto Eletrónico

O sistema de voto tradicional descrito anteriormente, implica obrigatoriamente a presença do eleitor em locais próprios para o efeito [11]. A votação eletrónica pode ser levada a cabo de duas formas:

- Presencial

Neste caso, o processo é iniciado tal como numa votação tradicional: o eleitor dirige-se a uma mesa eleitoral, na qual se encontram pessoas encarregadas de comprovar e registar a identidade do eleitor em questão. De agora em diante todo o processo difere de um processo de eleição tradicional. O eleitor deverá identificar-se perante uma máquina (por norma um computador) e realizar o seu voto, que será armazenado para a posterior contagem como apresentado na Figura 3, abaixo apresentada. A identificação nessa máquina poderá ser feita usando o bilhete de identidade ou umas credenciais próprias para

o efeito, obtidas aquando identificação da pessoa no sistema, de modo a evitar que a mesma pessoa vote mais do que uma só vez [8].

Neste tipo de votações o eleitor pode escolher a sua linguagem preferida, e aumentar ou reduzir o tamanho da fonte, conseguindo garantir deste modo um aumento da comodidade e acessibilidade na hora de votar [8].

Figura 3: Voto Eletrónico presencial [2].

- Não presencial

Na votação não presencial, a fase de identificação é informatizada, permitindo ao eleitor votar remotamente, sem existir a necessidade de se dirigir ao seu local assignado [11]. Assim, como referido anteriormente, se o eleitor tiver mobilidade reduzida ou necessidades especiais, este poderá realizar a votação de forma comoda. Com o sistema de voto

[2] http://www.larepublica.pe/17-10-2013/elecciones-municipales-contaran-con-voto-electronico-presencial

tradicional não é possível votar de forma não presencial, o que faria com que o processo de voto fosse incómodo, ou mesmo impossível, para alguns leitores.

O problema deste tipo de eleição diz respeito à impossibilidade de garantir a correta identificação do leitor, podendo existir casos de falsificação de identidade. Devido a este fator fundamental, ou seja, a garantia de que o eleitor não apresenta dados que não sejam verídicos aquando a confirmação da sua identidade, a votação não presencial não cobre tantos pontos como a votação presencial [8], contudo, este é um problema que afeta inúmeros sistemas, tais como *home banking*, declaração IRS, compras e vendas on-line, entre outros. A única forma de contornar este tipo de questão é responsabilizar o utilizador do sistema pela proteção dos seus dados pessoais (por exemplo, aquando a utilização de um determinado cartão de crédito, um banco não tem modo de saber se é de facto o seu dono que se encontra a utiliza-lo. O dono do cartão é responsável pela segurança do seu código de acesso, não sendo o banco responsável pela sua perda ou divulgação por parte do cliente.)

2.2.4 Princípios Gerais do Voto Eletrónico

Tal como acontece nos processos de voto tradicional, existem alguns princípios que devem ser atendidos nos processos de voto eletrónico, tais como:

- Cada pessoa só pode votar uma vez [3]. O voto eletrónico identificará cada eleitor de modo a garantir que este só possa efetuar um voto.

- O voto é privado [3], bem como toda a informação inserida por um eleitor aquando a votação, a qual deve ser estritamente privada. A privacidade, mais do que uma propriedade de segurança é um direito que assiste a todos os eleitores. Por esta razão, nenhum mecanismo deve negar este direito. Deve ser mantido o anonimato, tendo em conta a confidencialidade e integridade da informação em questão [11].

- Todos os votos são contados, pelo que o resultado obtido refletirá sempre o consenso de todos os eleitores [3].

- Os eleitores podem ter a confiança de que o seu voto vai ser contado [3].

2.2.5 Propriedades do Voto Eletrónico

Abaixo serão apresentadas e descritas algumas propriedades inerentes ao voto eletrónico. Estas propriedades encontram-se ilustradas na Figura 4, e são as seguintes:

- Confidencialidade:

Foi definida pela Organização Internacional de Estandardização (ISO), na norma ISO/IEC 27002, como sendo uma propriedade que "*garante que a informação é acessível só para aqueles que estejam autorizados a ela*" [13].

- Integridade:

Permite assegurar que os dados não foram falsificados, ou seja, que os dados recebidos ou recuperados são exatamente os que foram enviados ou armazenados, sem que tenham sofrido nenhuma modificação.

- Disponibilidade:

O sistema mantem-se em funcionamento eficientemente e é capaz de se recuperar rapidamente em caso de falha. O acesso a dados deve ser possível a todo momento e adequadamente.

- Autenticidade:

É a capacidade de verificar que os dados, sistemas e pessoas são legítimos e credíveis.
No caso das pessoas, estas tem de estar autorizadas a votar.

- Privacidade

O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto [8].

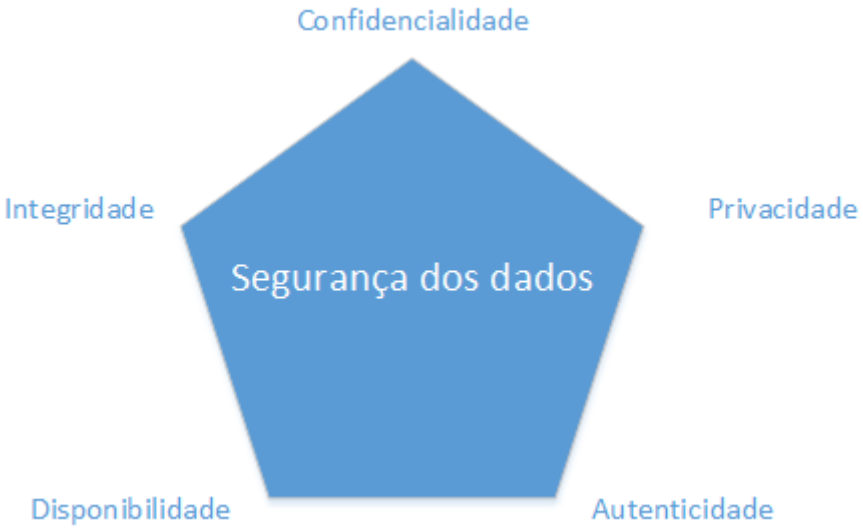


Figura 4: Modelo de propriedades da segurança de dados

2.2.6 Ameaças de segurança do Voto Eletrónico.

Um dos conceitos mais alarmantes e preocupantes do voto eletrónico é a segurança e as ameaças que podem surgir, por isso, é necessário ter uma preocupação mais cuidada neste tipo de problema, dado que um simples ataque bem-sucedido pode por em causa a aplicação e neste caso todo o processo eleitoral, invalidando assim a votação eletrónica. Danos de segurança na informação podem variar desde pequena -perdas para toda destruição do sistema de informação. Os efeitos das várias ameaças variam consideravelmente: alguns podem afetar a confidencialidade ou integridade dos dados, enquanto outros afetam a disponibilidade de um sistema [14].

Qualquer tipo de aplicação é vulnerável a ataques e cada vez são mais frequentes e mais variados, mas por outro lado atualmente existem mais regras e cuidados em todas as aplicações para evitar este tipo de problemas e existem mesmo áreas da informática e especialistas só orientados os parte de segurança de uma aplicação.
Nesta dissertação foi considerado este problema e foi elaborado um processo que dá especial atenção a este assunto usando mecanismos de segurança criptográficos para evitar qualquer tipo de falsificação do ato de voto nesta aplicação.

Ao longo dos tempos a tecnologia tem evoluído a passos largos, sendo hoje em dia considerado como sendo um bem indispensável, estando presente em vários aspetos do nosso dia-a-dia. A sua evolução tem sido exponencial e crê-se que assim continuará. Os computadores são um dos frutos dessa evolução, isto significa que de uma forma simplista, pode-se dizer que um computador é uma máquina cujo objetivo consiste em executar processos de forma mais rápida daquela de que um ser humano seria capaz. Contudo, tudo o que traz grande potencial acarreta grandes responsabilidades. O mau uso dos computadores pode levar a sérias falhas de segurança, que por si poderiam ter consequências catastróficas [11] [15].

Atualmente, existe uma preocupação crescente com estes aspetos, pois o crescimento exponencial do mundo tecnológico e o seu fácil acesso leva à necessidade de uma maior preocupação em proteger pessoas e informação.

Qualquer falha de segurança em uma eleição eletrónica pode corromper os resultados obtidos, podendo levar a graves consequências. É importante ter em conta a segurança do sistema de modo a garantir que este protegerá os dados de todos os envolvidos e que este produzirá resultados fiáveis.

Existem vários tipos de ameaças que podem por em risco sistemas de voto eletrónico [11]. Abaixo serão enunciados e explicados alguns tipos de ameaças que têm poder para afetar este tipo de sistemas.

- Negação de serviço (*Denial of Service - Dos*) - A1

Consiste, como o próprio nome indica, em negar o acesso a um determinado sistema através do congestionamento do mesmo. O sistema é sobrecarregado de pedidos, sobrecarga essa que fará com que o sistema falhe e seja impedido de fornecer o serviço devido aos seus utilizadores. Para levar a cabo este tipo de ataque, não são necessários grandes conhecimentos informáticos, o que torna este tipo de ameaça ainda mais perigosa. No contexto dos sistemas de voto eletrónico, um ataque deste tipo pode por em causa o direito ao voto dos eleitores [16].

- Cavalo de Troia – A2

Hoje em dia todos os utilizam a *Internet* já ouviram falar ou foram vítimas deste tipo de vírus informático. Tal como acontece no tipo de ataque descrito anteriormente, não requer

grandes conhecimentos para ser perpetrado e é bastante complicado saber qual a sua origem.

O cavalo de troia é um *software* malicioso que é executado como um programa aparentemente inofensivo. Este tipo de *software*, por norma, cria uma conexão remota para o equipamento infetado, permitindo ao atacante aceder e administrar esse mesmo equipamento. Após a sua execução, mesmo após ter sido detetado, é bastante complicado remover este tipo de *software* do sistema, pelo que deve haver uma especial atenção na prevenção deste tipo de ataques.

Este tipo de ataque pode impedir o acesso ao sistema de voto eletrónico, não sendo possível aos eleitores exercer o seu direito de voto [16].

- "*Spoofing*" – A3

Este tipo de ataque requer um pouco mais de conhecimento de informática que os anteriores. O seu objetivo principal consiste em falsificar a identidade de alguém de modo a obter o acesso a um determinado sistema. O atacante ilude o sistema fazendo-se passar por um eleitor com permissões de acesso, sendo assim capaz de alterar ou mesmo anular o voto da pessoa cuja identidade foi suplantada [16].

- Ataques internos ao sistema – A4

A corrupção nas eleições tradicionais vê-se refletida neste tipo de ataque. Uma pessoa pertencente à equipa do sistema de votação eletrónica pode ser o causador desta ameaça, dado que pode comprometer os resultados da votação ao adulterar os votos. Como são ataques muito difíceis de detetar, podem facilmente pôr em perigo todo o processo eleitoral [16].

- Vírus – A5

A privacidade é um dos fatores a ter em conta aquando a instalação de um sistema de voto eletrónico. Esta pode ficar comprometida caso ocorra algum tipo de ataque ao servidor provocado por um vírus informático, o que levará ao comprometimento dos dados que este armazena, i.e., dados dos utilizadores, dados relativos a votos [16].

- Alterações de configuração – A6

O direito de voto é um direito que todos os cidadãos possuem e que não pode ser negado contudo, com este tipo de ataques essa condição pode não ser verificada. O utilizador seria ludibriado, sendo reencaminhado para páginas não oficiais da eleição. [16].

- Comércio de votos automatizado – A7

Esta ameaça pode comprometer a democracia de uma eleição, já que permite a compra de votos de forma remota [16].

- Coercibilidade – A8

O eleitor pode ser coagido no momento de exercer o seu direito de votar, pondo em risco, novamente, a democracia da eleição e conduzindo a corrupção [16].

Qualquer um destes ataques pode por em risco o processo eleitoral, sendo que alguns deste tipo de ataques não necessitam de grandes conhecimentos informáticos por parte do atacante para serem executados. Como consequência poria em risco a garantia de privacidade, segurança e democracia do sistema de voto eletrónico
Na tabela 1 é apresentada a classificação das ameaças e a sua influência em cada uma das propriedades de segurança:

Propriedades/Ameaças	Caso 1	Caso 2	Caso 3	Caso 4	Caso 5	Caso 6	Caso 7	Caso 8
Confidencialidade		*		*		*		
Integridade		*		*	*	*		
Disponibilidade	*	*	*	*		*		
Autenticidade		*	*	*	*	*	*	*
Privacidade		*		*	*	*	*	*

Tabela 1: Classificação das ameaças / propriedades de segurança

2.2.7 Tecnologias de Segurança

O terrorismo é uma preocupação constante da sociedade, especialmente o terrorismo tecnológico. Devido a esse facto, as tecnologias de segurança são cada vez mais vistas como sendo imprescindíveis, tendo a sua importância crescido exponencialmente ao longo dos últimos anos.

Estes ataques terroristas têm, por norma, como principal alvo as tecnologias da informação e comunicação, que abrangendo diversos domínios da atividade económica e social, afetando o mundo inteiro.

Para proteger estas tecnologias, têm sido criados diversos sistemas que têm como finalidade garantir a segurança e os direitos dos eleitores nos sistemas de voto eletrónico [17]. Essas tecnologias são consideradas como sendo as mais usadas no contexto de organizações deste tipo [18] [19] [20]:

- *Firewall*

A *Internet*, tal como a conhecemos hoje, sofreu um enorme crescimento, crescimento este que será cada vez maior e mais veloz. Tendo em conta que foi originalmente criada como um meio de comunicação da informação, foi necessária a criação de um sistema de proteção que conferisse segurança ao modo de transmissão da dita informação. Com esta ideia em mente foi criada a *firewall* [21].

O termo *Firewall* é o produto da combinação da palavra inglesa *"Fire", que* significa "fogo", e da palavra inglesa "*Wall",* quer significa "parede". Combinando os significados de ambas as palavras, pode-se concluir que o termo *Firewall* significa literalmente *parede de fogo* [11]. Esta tecnologia pretende estabelecer e fazer cumprir funções de segurança numa rede [22], protegendo todos os elementos que estejam ligados a essa mesma rede [21].

As funções da *firewall* podem ser aumentadas com *hardware* ou com programas de *software* específicos para o efeito. São utilizadas nas organizações como um "filtro" entre a internet e a rede interna [11].

No caso do voto eletrónico, a *firewall* tem como função permitir a transmissão da informação que seja enviada pelos computadores que sejam reconhecidos e identificados pelo sistema [11].

- *Software* Antivírus

São aplicações que têm como função a deteção de vírus (como por exemplo o cavalo de troia, apresentado anteriormente) e código malicioso. Tendo em conta que estes ataques são difíceis de detetar (por norma executam de forma transparente para o utilizador), a sua disseminação é feita com facilidade e permanecem no computador caso não sejam tomadas medidas. De modo a garantir a proteção contra este tipo de ataque devem ser realizadas as seguintes ações: prevenção, deteção, isolamento e recuperação [11].

No contexto do presente estudo, o *software* antivírus deve estar presente tanto no servidor, como no computador em que o eleitor irá operar durante o processo de votação. Se o ataque for executado com sucesso, todo o processo eleitoral ficaria comprometido, levando à invalidação dos resultados do mesmo [11].

- Sistemas de Deteção de Intrusão

Este tipo de tecnologia de segurança consiste numa aplicação que analisa as ações tomadas perante o sistema de acordo com os privilégios dos atores e determina se é uma ameaça ou não [11]. A sua localização na rede influi na sua metodologia de deteção de intrusos, sendo capazes não só detetar um ataque, mas também prever a sua ocorrência [23].

No contexto dos sistemas de voto eletrónico, esta ferramenta de segurança é necessária para prever e/ou detetar ataques internos e ataques externos ao sistema [11].

- Lista de controlo de acesso

Este tipo de defesa está diretamente relacionada com a característica de não-repúdio referida anteriormente. O objetivo consiste em controlar todos os acessos ao sistema,

registando todas as ações executadas e o respetivo autor. Assim, caso seja levada a cabo uma ação considerada como sendo maliciosa para o sistema é possível encontrar o autor da mesma. Com este tipo de mecanismo, é possível assegurar a veracidade de cada voto introduzido no sistema, evitando situações de fraude [11].

- Cifra de dados em transporte

A comunicação entre dois computadores é normalmente aberta, vulnerável a entrada de terceiras pessoas que podem descobrir o conteúdo das mensagens. Por isso, tanto em um sistema de voto eletrónico, como em um contexto organizacional, é necessária a existência de mecanismos de proteção da informação, para que esta seja apenas acedida por aqueles que possuem permissões de acesso à mesma. Para garantir a segurança na transmissão dessa informação são utilizadas técnicas de encriptação. Ao aplicar técnicas de encriptação às mensagens, estas só poderão ser acedidas se contiverem a informação necessária. Assim, garante-se que a informação é transmitida apenas a quem tem permissões para a receber, sem que haja qualquer interferência por parte de terceiros [11]. Este tema será posteriormente abordado com mais detalhe no presente documento.

- Cifra de ficheiros

Esta técnica é bastante semelhante ao exemplo anterior, só que, ao invés de cifrar apenas a informação em si, são também cifrados todos os arquivos que a contêm. Deste modo, é possível negar o acesso a dados, a terceiros que não possuam permissões de acesso aos mesmos [11].

- Contas de utilizadores

O sistema de voto eletrónico não pode permitir a entrada a utilizadores que não possuem permissão para participar na votação. Com isso em mente, são criadas contas de utilizadores, para efeitos de autenticação. Deste modo, o utilizador é obrigado a autenticar-se com sucesso no sistema para que possa participar na votação. [24].

- *Smartcards*

Este é um dos possíveis métodos de autenticação a utilizar num sistema de votação eletrónico. *Smartcards* são cartões, com dimensões semelhantes a um bilhete de

identidade, com um chip integrado que contém toda a informação relativa à identidade do seu portador. Assim, é possível assegurar que apenas acedem ao sistema pessoas com permissão para tal[11].

- Infraestrutura de chaves públicas

Na criptografia assimétrica existem dois tipos de chaves: a chave pública e a chave privada. A primeira como próprio nome indica é pública, ou seja, qualquer pessoa pode ter acesso à mesma e é utilizada para cifrar a informação. A segunda chave é única, ou seja, apenas o seu titular tem acesso à mesma, e tem como finalidade decifrar informação cifrada com a chave anterior. [25].

Este tipo de tecnologia de segurança funciona da seguinte forma: cada ator (humano ou não) é possuidor de um par de chaves eletrónicas. Uma delas é pública e a outra privada. Quando o sujeito A envia informação para o B cifra-a com a chave pública do sujeito B. Este, ao receber a informação cifrada poderá decifrá-la através da sua chave privada e vice-versa. Falando no contexto do voto eletrónico, esta abordagem pode ser útil ao ser utilizada para o eleitor cifrar o seu boletim de voto, submetê-lo no servidor e apenas este último poderá, com a sua chave privada, decifrar o boletim e proceder ao seu armazenamento. O servidor não deve ter conhecimento do eleitor que o enviou, deve apenas ter conhecimento do computador que foi utilizado para a submissão do voto. Essa informação será posteriormente utilizada na fase de contagem de votos.

Em alguns casos utiliza-se uma urna eletrónica para fazer a contagem dos votos inseridos. Nestes casos, a urna terá em seu poder a chave privada, sendo apenas a ela permitido o acesso à informação dos votos introduzidos [26].

- Biometria

O termo *biometria* deriva dos termos gregos *bios* (vida) e *metron* (medida), e no contexto da autenticação diz respeito à identificação de um determinado individuo através de uma característica física (como por exemplo, a impressão digital) [27]. Este sistema pode ser considerado uma alternativa ou um complemento ao *smartcard* [11].

Hoje em dia são utilizadas muitas características físicas humanas para efeitos de autenticação em vários sistemas informáticos. Os métodos utilizados dependem de vários fatores, tais como: grau de fiabilidade, nível de conforto, nível de aceitação e custo de implementação [26].

Figura 5: Exemplo de autenticação por biometria [3].

2.2.8 Voto Eletrónico como *Software as a Service* (SaaS)

O *software as a service* é um modelo de distribuição de *software* que proporciona aos clientes um serviço, sem ter que ser comprado ou instalado, que é acedido através de um *browser* pela internet.

O utilizador não precisa de ter preocupações em relação a questões como a manutenção ou segurança do serviço, pois estas questões são da responsabilidade da companhia que fornece o serviço utilizado [28].

- Inícios do SaaS

[3] http://www.kimaldi.com/kimaldi_por/sectores/universidades/controlo_de_acesso_biometrico_ao_refeitorio_de_uma_residencia_universitaria

A primeira geração de entrega de *software* sob a forma de serviço surgiu nos anos 90. Esta primeira fase falhou em cumprir os requisitos de fiabilidade e qualidade exigidos pelos empresários. Contudo, os métodos de entrega posteriores foram funcionando melhor [29].

A segunda fase de *software as a service* introduziu uma inovação, transações entre os compradores e os provedores, incluindo aquisições, logística e gestão de as mudanças no fornecimento de recursos [29].

Mais tarde apareceu uma terceira oleada de aplicações. Esta foi mais crítica para o negócio que a oleada anterior no entorno no que se alojava o *software* para o seu desenvolvimento [29].

- Exemplo de SaaS [30]

Um empresário criou uma empresa que oferece serviços a aquelas pessoas que desejam comprar propriedades no estrangeiro. Concretamente oferece dois serviços: um deles oferece informação sobre as propriedades que estão disponíveis, o segundo encarrega-se da negociação real e da compra da propriedade.

O serviço de compra do empresário utiliza outros serviços para lidar com tarefas como a tradução, negociações legais e financeiras, o financiamento e a transferência de divisas.

O problema de oferecer estes serviços é que o empresário tem que especificar os términos, condições e a forma de prestações de esses serviços, junto com as regras que descrevem como serão outros serviços escolhidos para o caso.

No caso de *software as a service*, este poderia levar a cabo o mantimento e venta do serviço, deixando menos ocupado ao empresário.

3 Características e Evolução Histórica dos Sistemas de Voto Eletrónico

3.1 Origens e Evolução Histórica

A utilização de novas tecnologias nos processos eleitorais não é uma prática recente. A sua incorporação progressiva foi-se expandindo desde as décadas de setenta e oitenta ao século XX, abrangendo múltiplas modalidades variando consoante o seu grau de sofisticação e tipo de eleição usado [31].

O que é particularmente recente é a crescente popularidade do voto eletrónico. Apesar de ter apenas sido alvo de mais atenção nos primeiros 5 anos do século XXI, o voto eletrónico já era um conceito bem conhecido no final da década dos anos 90, tendo começado a ser mais aplicado quando começaram a ser desenvolvidos sistemas baseados em urnas eletrónicas na Europa (Bélgica, Suécia e Países Baixos) e América Latina (Venezuela e Brasil na liderança) [31].

Nestes países, os conceitos e ideias relacionados com a votação eletrónica variam bastante, existindo definições que apenas se inserem no contexto de urna eletrónica, enquanto outros são bastante mais abrangentes, incluindo sistemas de votação via *internet*, descrevendo-o como sendo uma ferramenta facilitadora da democracia digital [31].

Os grandes exemplos destes conceitos são os casos de aplicação nos Estados Unidos da América (EUA) e em França que, no final do século XIX e início do século XX, começaram a utilizar dispositivos mecânicos para votação. Desde o início do século XX, que os EUA começaram a usar legalmente urnas mecanizadas para a emissão e contagem dos votos [31].

Mais tarde, a partir dos anos 80, foram disponibilizados, por várias empresas envolvidas na conceção e implementação de novas tecnologias para o setor público, vários sistemas eletrónicos de votação para serem utilizados em eleições em municípios, distritos e estados [31].

3.2 Aplicação prática do sistema de Voto Eletrónico – Casos de Sucesso

Hoje em dia, é possível observar uma mudança nos sistemas de votação utilizados pelas organizações para levar a cabo as suas eleições internas. É notório um crescimento na preocupação por parte das grandes organizações em oferecer mais liberdade e flexibilidade aos seus eleitores, permitindo-lhes efetuar uma votação de forma simples, rápida e confortável, sem que tenham necessidade de trocar os seus hábitos.

Segundo o *Alpha Vote* o voto eletrónico permite às entidades realizar os seus processos de votação, reduzindo custos associados e aumentando a participação sem, no entanto, menosprezar o segredo do voto. No mesmo estudo é referida uma empresa, chamada STS Group, na qual se comprovou que as taxas de eleitores aumentam quando se lhes possibilita o voto eletrónico. Por exemplo, os advogados do Barreau de Bruxelas conseguiram aumentar o número de associados que votam nas eleições em aproximadamente 20%, sendo que 80% destes associados votam de forma eletrónica [32].

Segundo um estudo realizado em França, onde este sistema já se encontra amplamente implementado, consideram que este é um país que serve como um forte exemplo no que a voto eletrónico se refere, nas eleições de 2003 até 60% dos eleitores escolheram o votar via internet [32].

3.2.1 Exemplos de aplicação do Voto Eletrónico em contextos reais

3.2.1.1 Casos reais de aplicação do voto eletrónico na Europa

Existem vários casos reais de aplicação dos sistemas de voto eletrónico em alguns países europeus. De seguida, serão enunciados os países que mais se destacaram a este nível, apresentando, de forma breve, o contexto em que o sistema de voto eletrónico foi aplicado e qual o resultado desta aplicação.

- Portugal

Em Portugal ocorreram quatro experiências-piloto com o voto eletrónico entre as eleições autárquicas de 1997 e nas eleições legislativas de 2005.
Tanto num plano nacional como interno, o tema do voto eletrónico está longe de ser resolvido em parte pelos problemas de segurança nomeados anteriormente [33].

Em 2004 fez-se a primeira eleição eletrónica para o parlamento europeu, contudo, foram detetados alguns problemas, trazendo instabilidade a este tipo de abordagem, nomeadamente: [8]:

- Falta de procedimentos para corrigir situações de falhas imprevistas.
- Documentação insuficiente e não explicativa do funcionamento interno dos sistemas;
- Usabilidade dos dispositivos reduzida e sem cuidados específicos para eleitores com deficiências visuais;
- Potenciais associações entre voto e eleitor em pelo menos uma das soluções apresentadas;
- Imaturidade de algumas soluções apresentadas.

Estes problemas trouxeram instabilidade a este tipo de abordagem tornando-a, por isso, inviável.

A primeira experiência de voto eletrónico presencial realizada em Portugal em
2004 compreendeu 9 freguesias e contou com a participação de cerca de 9.500 eleitores (cerca de 20% do total de votantes nessas freguesias, nesse ato eleitoral específico).
Num estudo realizado posteriormente, 99% dos eleitores inquiridos gostaram da experiência e 97% revelaram-se dispostos a votar eletronicamente em futuros atos eleitorais [32].

- Bélgica

O voto eletrónico foi introduzido como uma parte das eleições de 1991, em que dois distritos foram selecionados para participar numa experiencia. Depois, em 1999, 44% dos votos foi registado eletronicamente, existindo o objetivo de conseguir que fossem registados 100% dos votos em 2006. Mais tarde, em 2003, nos distritos de *Waarschoot* e *Verlaine*, os

eleitores tinham a possibilidade de utilizar um ecrã com um *ticket* para registar o seu voto. Contudo, esta ideia tornou o processo de votação mais lento em comparação com a opção de voto eletrónico sem *ticket.* Além disso, em *Waarschoot* houve diferenças entre o número de *tickets* e os votos registados eletronicamente pelo que a eleição ficou invalidada. Por fim, a ideia de repetir a experiência foi rejeitada [34].

- Estónia

Em 2002 realizou-se o acordo para introduzir em 2005 o voto eletrónico na Estónia, sendo permitido aos eleitores trocar o seu voto tantas vezes quantas desejassem, durante os dias em que o sistema estivesse disponível.
Se um eleitor por alguma razão votasse de forma digital e em papel, apenas era considerado para a contagem de votos final o voto em papel. Uma vez que o eleitor fizesse a sua escolha pelo voto eletrónico, o voto eletrónico deste eleitor devera ser aprovado com uma assinatura digital.

Nas eleições de 2005 a participação rondou os 2% dos eleitores, o que foi considerado como sendo bom resultado. Em termos de localização de votação, a 54,5% dos votos foram submetidos a partir da residência dos eleitores, 36,6% a partir de locais de trabalho, 3,6% a partir da casa de um amigo, ou cibercafés, 3,2% a partir de um ponto público de acesso à internet e 1’9% a partir de uma oficina.

Esta experiencia prova que é possível obter bons resultados neste tipo de atos eleitorais já que o sistema de voto eletrónico funciona perfeita e legalmente [35].

3.2.1.2 América

- Brasil

Desde 1996 que o tema referente a voto eletrónico é abordado, contudo apenas a partir de 2002 estes sistemas se tornaram populares, sendo a taxa de adesão acima de 65 % da população, ou seja, 100 milhões de pessoas (mais do 65% da população). As razões para começar a usar este sistema neste país já foram nomeadas anteriormente: eliminar a fraude eleitoral, reduzir o tempo de recolha e contagem de votos e tornar o processo de votação mais fácil e acessível aos eleitores. O sistema utilizado foi uma urna com teclado digital [36].

- Venezuela

Desde 1998 que tem havido mudanças nos tipos de sistema de voto eletrónico implementados na Venezuela. Primeiro foram utilizados ecrãs *touch-screen* que, no final da votação, imprimiam um documento com a opção escolhida pelo eleitor, a data da eleição, o lugar onde foi realizado e a mesa eleitoral correspondente ao eleitor em questão [36].

- Estados Unidos

Na década dos 70 foi criada uma equipa de especialistas encarregues da implementação de um sistema de voto eletrónico para ser utilizado nas eleições presidenciais de 2000. Como resultado, 1.6% da população usou o voto tradicional, 9,1% utilizou o registo eletrónico direto, 27.3% utilizaram leitores óticos, 18,6% utilizaram umas máquinas com um sistema de alavancas para votar e os 34'3% utilizaram cartões perfurados.

Relativamente ao voto através da internet, nas semanas anteriores às eleições de 2000, foram realizadas umas provas piloto nas cidades de Arizona e Califórnia, nas quais milhares de soldados tiveram a possibilidade votar a partir daa sua localização geográfica. Para efeitos de verificação do envio bem-sucedido dos votos via eletrónica, foi também pedido aos eleitores o envio dos seus votos por correio [36].

3.2.1.3 Ásia

- Índia

Na Índia, em 2004, teve lugar o maior exemplo de utilização do voto eletrónico da história. Cerca de 380 milhões de indianos votaram em mais de 1 milhão de máquinas, revelando-se a adoção do método do voto eletrónico num caso de bastante sucesso. Com os sistemas eletrónicos, conseguiu-se o alcance de algumas melhorias, tais como a precisão e transparência no processo de contagem de votos [32].

3.3 Voto Eletrónico como um negócio

O sistema de *software* proprietário Vote Now[4] foi especificamente concebido por cientistas universitários para o uso nas eleições de organizações profissionais.
Com 16 anos de experiência na realização de eleições baseadas na Web, já fizeram eleições a centenas de organizações empresariais profissionais, grupos sem fins lucrativos e universidades com necessidades de eleições.

Eles afirmam que a experiência faz toda a diferença no que diz respeito à realização de eleições. A empresa já levou a cabo mais de mil trezentas eleições até a data atual (mais de um milhão de eleitores) [32].

[4] Vote Now (http://www.vote-now.com/)

4 Propriedades do voto eletrónico.

A tecnologia é um fator de peso no nosso dia-a-dia, sendo algo cada vez mais comum. Graças aos seus avanços, foi possível acelerar e automatizar processos que há bem pouco tempo exigiam bastante tempo e esforço daqueles que os executavam. Com o voto eletrónico pretende-se atingir o mesmo objetivo: poupar tempo e esforço a todos os envolvidos no processo de votação. Contudo, apesar de o grande objetivo dos sistemas de voto eletrónico se centrar na redução de tempo e de esforço, o mesmo não deve acontecer em relação à segurança: esta deve ser igual, ou preferencialmente maior, do que a segurança existente nos sistemas de voto tradicional. Os eleitores, aquando a utilização de um sistema de voto eletrónico, devem ser assegurados de que não haja qualquer hipótese de existência de corrupção dos votos. Devem ver o sistema como sendo algo fiável e seguro.

Apesar de a segurança ser um ponto bastante importante a garantir nos sistemas de voto eletrónico, existem outros fatores que devem ser igualmente assegurados, tais como: disponibilidade do servidor, utilidade, privacidade, integridade. Tendo isto em mente, pode-se definir um conjunto de requisitos que devem ser tidos sempre em conta no que diz respeito ao voto eletrónico. Os requisitos definidos são:

- Anonimato: a contagem de votos deve ser protegida de leituras externas no processo de eleição. A associação entre os votos contados e a identidade do eleitor deve ser completamente ocultada [24].

- Auditabilidade e certificado: O sistema de voto eletrónico deve ser auditado por pessoas externas e também ser corretamente comprovado e certificado por agentes oficiais [8].

- Defesa: o sistema deve possuir mecanismos de defesa contra possíveis atacantes, corrupção ou fraude [8].

- Disponibilidade: O sistema deve estar sempre acessível aos eleitores, ao longo de todo o processo eleitoral [8].

- Elegibilidade: deve ser garantido que apenas indivíduos registados no processo eleitoral tenham acesso ao sistema. Os eleitores devem efetuar a sua inscrição

antes do processo de votação, de modo a permitir a confirmação da sua identidade [37]. Para suportar este mecanismo de verificação de permissões para participar no processo eleitoral é necessária a existência de um sistema de autenticação que não consista num processo de autenticação básico, ou seja, com a utilização de uma simples senha, porque esta pode ser facilmente adivinhada por especialistas em informática [24]. Existe vários tipos de autenticação considerados seguros, que podem ser utilizados neste tipo de processo, sendo estes os seguintes: presencial, PIN, certificado digital, cartão inteligente ou biométrica [8].

- Integridade do sistema: não podem existir margens de erro. O resultado deve ser exato, refletindo exatamente a vontade dos eleitores, sem que haja nenhuma alteração. Só assim é possível garantir a integridade do processo [38].

- Integridade pessoal: Os indivíduos responsáveis por criar, operar e administrar o sistema de voto eletrónico devem ser íntegros, ou seja, indivíduos que não cometam corrupção e que sejam capazes de realizar a sua função sem colocar em perigo a segurança e integridade do sistema [24].

- Justiça: ninguém saberá o resultado da eleição antes do tempo certo, nem mesmo a pessoa responsável pela contagem de votos [37].

- Localização: os eleitores devem poder utilizar o voto eletrónico a partir de um local à sua escolha. No que diz respeito ao equipamento utilizado para a votação por parte do eleitor, este deve ter o ecrã orientado de forma que o eleitor se sinta o mais cómodo possível durante a sua utilização [8].

- Precisão: todos os votos, sem exceção, deverão ser contados. Nenhum voto pode ser alterado, apagado, invalidado ou copiado. Qualquer ataque a os votos deverá poder ser detetado [37].

- Privacidade: deve ser preservada desde o início até o fim da eleição e posteriormente [37].

Após o processo de autenticação inicial, o sistema deve comprovar a autenticidade dos dados introduzidos, ou seja, que a pessoa que se registou seja realmente essa pessoa e não outra.

- Registro: todas as operações devem ser monitorizadas, sem que a privacidade do eleitor seja violada. A monotorização deve incluir a gravação dos votos e todas as programações e operações administrativas devem ser comprovadas antes e depois da eleição [24]. Também, o sistema deve ter um registo da entrada e saída do sistema para os eleitores e de qualquer dado introduzido por estes [8].

- Robustez do sistema: nenhuma pessoa ou autoridade pode interromper ou influenciar a eleição e a contagem final dos votos. A robustez tem que estar assegurada de modo a garantir a fiabilidade dos resultados da eleição [37].
  A confiança depositada pelos utilizadores no sistema deve estar assegurada.

- Singularidade: Só é contado um voto por pessoa, de modo a garantir a validade dos resultados eleitorais. [37].

- Sistema anticorrupção: os eleitores não devem ter a possibilidade de mostrar a sua opção de voto a terceiros, de modo a evitar situações de compra de votos [37]. Além disso, o sistema de voto eletrónico deve ser capaz detetar qualquer tentativa de instrução de agentes externos e gerar alertas aos administradores do sistema.

- Transparência: o resultado do processo de votação deve ser totalmente transparente, devendo ser devidamente publicado para que todos os envolvidos sejam informados acerca do mesmo [37].

- Usabilidade: deve ser possível ao eleitor mudar o idioma conforme desejado, e deve ser também possível a alteração do tamanho da letra, de modo a garantir que o sistema cumpre os critérios mínimos de usabilidade [7]. Além disso, o sistema deve ser viável economicamente para todos os que o utilizam e possuir uma boa performance em termos de rapidez de contagem de votos e de divulgação de resultados [8].

5 Segurança

Um dos aspetos mais preocupantes atualmente numa eleição é a segurança, dado que uma eleição na qual seja possível adulterar os votos seria considerada uma eleição inválida, sem qualquer tipo de valor para todos os envolvidos. Este tipo de problema existe tanto nas eleições tradicionais como nas eletrónicas. Nas eleições tradicionais a preocupação cai mais na parte física, ou seja, é necessário ter em atenção a segurança das instalações nas quais decorrem os processos eleitorais, garantir que o processo de contagem de votos é livre de corrupção (tendo em conta que se trata de um processo manual, está só a corrupção por parte de terceiros, mas também a erro humano), e ter cuidados especiais com a forma como os votos são transportados.

Quando falamos de votação eletrónica existe um conjunto propriedades de segurança que devem ser considerados, embora se afastem do âmbito dos problemas de segurança físicos mencionados anteriormente, tornando este processo um pouco mais delicado face ao processo de votação tradicional. As propriedades são:

• Confidencialidade: Esta propriedade diz que é necessário manter os dados seguros, para que seja apenas possível aceder-lhes com a devida autorização.

• Autenticação: Serve para comprovar a origem de uma determinada mensagem.

• Integridade: Garante que a informação não foi alterada por intermediários que não deveriam ter acesso a essa mesma informação.

• Não-repúdio: É propriedade que permite garantir a autenticidade da identidade das entidades que enviam e recebem a informação [8]

Todas estas propriedades estão interligadas, podendo ser garantidas com a criptografia, técnica que será abordada com mais detalhe nos subcapítulos abaixo.

5.1 Criptografia

O termo *criptografia* deriva da combinação das palavras gregas *kripto* (oculto) e *grapho* (grafia), e é utilizado para descrever a ação de codificação de mensagens. Consiste na aplicação de uma fórmula, cuja complexidade pode variar consoante o algoritmo aplicado e quando aplicada a uma mensagem tem a capacidade de a codificar e descodificar [25].

Segundo o ISSO/IEC 27001:2005, um recurso é essencial para o negócio da organização, e consequentemente, necessita de ser devidamente protegido, ou seja, para qualquer organização há informação que é vital para essa empresa, pelo que, essa informação não pode estar disponível/pública para qualquer um. Essa informação deve estar devidamente protegida. Esses recursos ou informação podem ser digitais ou em papel.

Quando é necessário manipular essa informação para que possa ser usada é necessário existirem medidas apropriadas para lidar com essa informação, dependendo do tipo de informação que é necessário proteger. A informação em papel, pode ser protegida fisicamente, mas a informação digital, quando é enviada, está vulnerável a qualquer ataque.

A criptografia (ilustrada na Figura 6) é o estudo de técnicas matemáticas que possibilitam a transformação da informação, através da conversão de informação legível em informação inteligível e vice-versa. A este tipo de transformação, dá-se o nome de cifragem, à transformação contrária, dá-se o nome de decifragem.

.

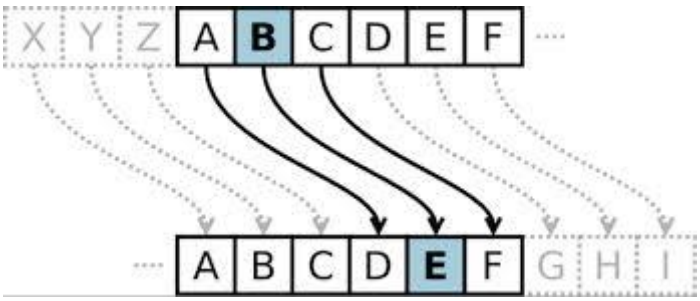


Figura 6: Criptografia

Para aplicar este tipo de transformações é necessário criar uma chave, que terá como finalidade a identificação do conjunto de informação a cifrar. Essa chave será única, sendo necessária para executar a cifragem e decifragem desse conjunto de informação. [39].

Este tipo de transformações de cifra e decifra podem ser classificadas segundo dois tipos: *cifragem simétrica* e *cifragem assimétrica*.

5.1.1 Cifragem Simétrica

A cifragem simétrica, ilustrada na Figura 7 é um tipo de cifragem na qual a chave utilizada para a decifragem da informação é a mesma, ou é derivada, da chave utilizada para efetuar a cifragem. Deste modo, quer a entidade que envia os dados, quer a entidade que os recebe irá ter conhecimento do valor da chave utilizada. [25]. A este tipo de chave dá-se o nome de chave secreta e, ao contrário da chave de sessão que apenas pode ser utilizada uma só vez para cifrar informação, pode ser utilizada em inúmeras cifras, durante a troca de informação entre as partes que conhecem a chave.

Tomemos como exemplo prático da utilização de uma chave secreta, uma conversa entre dois indivíduos, sendo que ambas as partes desejam manter secreto o conteúdo da comunicação. Ambas as partes trocam mensagens entre si que são codificadas e descodificadas utilizando uma chave secreta para o efeito, sendo que essa chave é apenas do conhecimento de ambos os intervenientes da conversa. [40].

Este tipo de cifragem possui limitações, pois nem sempre é possível ter certezas acerca da identidade do emissor da mensagem. A este tipo de vulnerabilidade dá-se o nome de não-repúdio.

Contudo, apesar de não responder ao critério de não repúdio, este tipo de cifragem é capaz de garantir as propriedades de confidencialidade e de integridade, pois apenas os detentores da chave secreta são capazes de proceder à descodificação da informação trocada.

Em termos de performance, este tipo de cifragem é considerada rápida. (performance não é só rapidez)

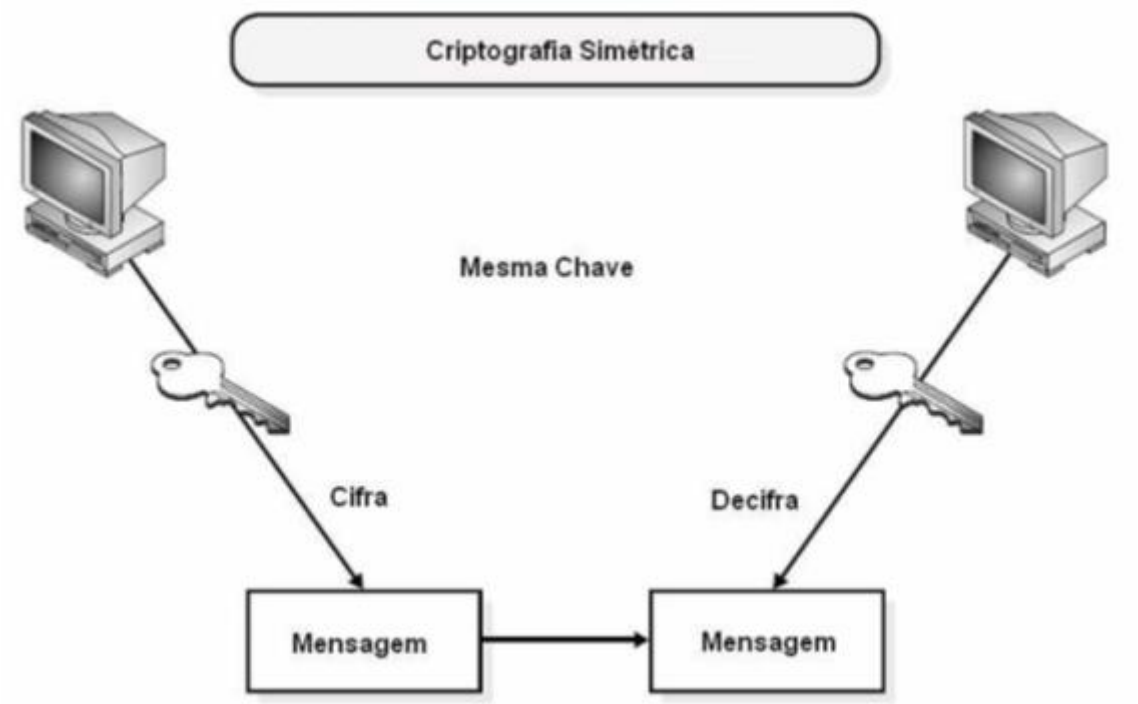


Figura 7: Criptografia Simétrica.

5.1.2 Cifragem Assimétrica

Na cifragem assimétrica o conceito é diferente, sendo utilizados no processo de cifragem e decifragem dois tipos de chaves: a chave *pública* e a *chave privada*.

- A chave pública é a usada na cifragem da informação e é partilhada e tornada pública, sendo deste modo possível a cifragem de informação por qualquer indivíduo [25].
- A chave privada, como o próprio nome indica é pessoal e intransmissível, não podendo sair da posse do seu titular. É utilizada no processo de decifragem, garantindo deste modo que apenas o seu portador é capaz de decifrar a informação que lhe é destinada. A chave privada não pode ser obtida a partir da chave pública, pelo menos em tempo útil. [25].

A grande diferença entra a cifragem simétrica e a cifragem assimétrica, em termos de segurança, centra-se no facto de que a última é capaz de garantir todas as propriedades de segurança, enquanto na cifragem simétrica, tal como fora referido anteriormente, não é

possível garantir a existência da propriedade de não repúdio. Através da chave pública é sempre possível saber qual a verdadeira identidade do autor da informação enviada.

Contudo, em termos de tempo de execução, este tipo de cifragem fica a perder em relação à cifragem simétrica.

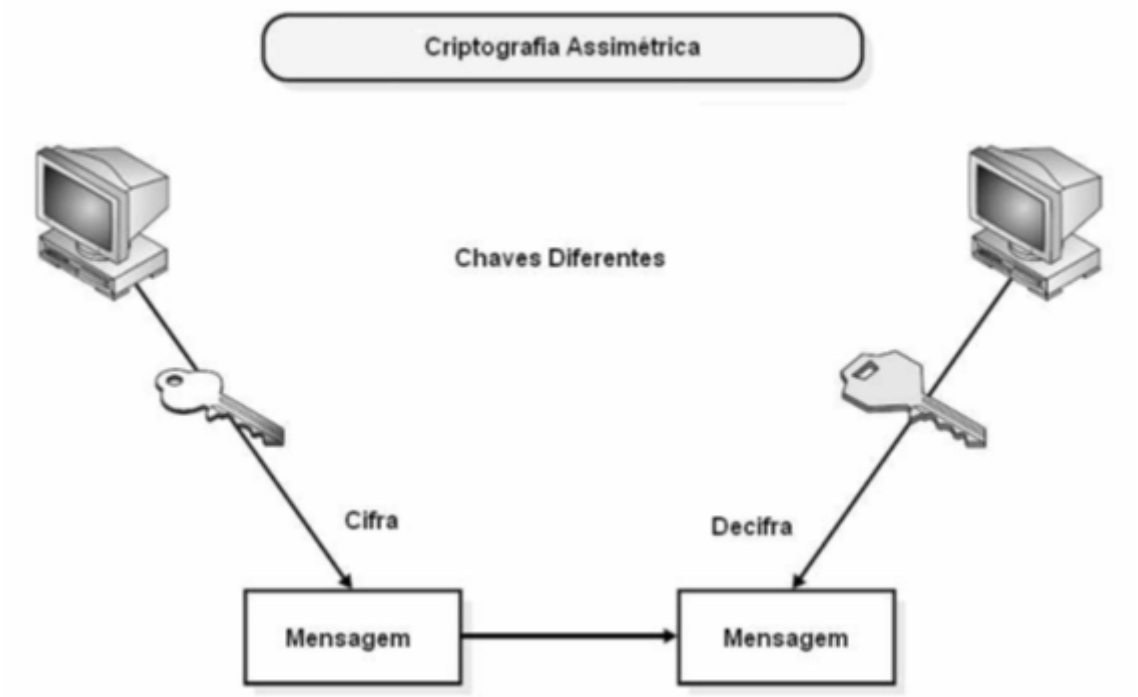


Figura 8: Cifragem Assimétrica

Neste tipo de cifragem também pode ser aplicado o processo inverso, ou seja, a chave privada pode ser utilizada para assinar dados, que por sua vez são verificados com a chave pública. A este tipo de abordagem dá-se o nome de *assinatura*. Contudo, esta abordagem não serve para cifrar dados, dado que, qualquer pessoa pode ter acesso à chave pública, tendo deste modo acesso à informação cifrada. O objetivo deste tipo de abordagem é apenas saber quem é que assinou os dados, ou seja, saber a origem da mensagem [40].

Como boa prática, devem ser seguidas ambas as abordagens de modo a obter dados assinados e cifrados.

6 Electronic Vote as a Service (e-VaaS)

Uma das preocupações iniciais com este sistema foi criar diferentes níveis de segurança dependendo da importância das eleições, evitando assim passos desnecessários na realização de todo o processo eleitoral e tornaria a eleição de maneira mais simples.

Assim criaram-se dois tipos de eleição, uma com um nível de segurança baixo e outra com um nível de segurança alto.

Quando falamos do tipo de eleição de segurança baixo falamos de um sistema normal que só contém a segurança normal de qualquer tipo de aplicação desta maneira a eleição decorreria de maneira mais rápida e simples.

Podemos dizer que esta dissertação baseia-se no tipo de segurança de alto nível que é um sistema distribuído com diferentes componentes ligados através de uma rede (ex.: LAN1 , MAN2 , WAN3), tal como se encontra ilustrado na Figura 8. O eleitor acede ao e-VaaS através da rede, apesar de as opções de presença ou não presença física estarem ambas disponíveis.

.

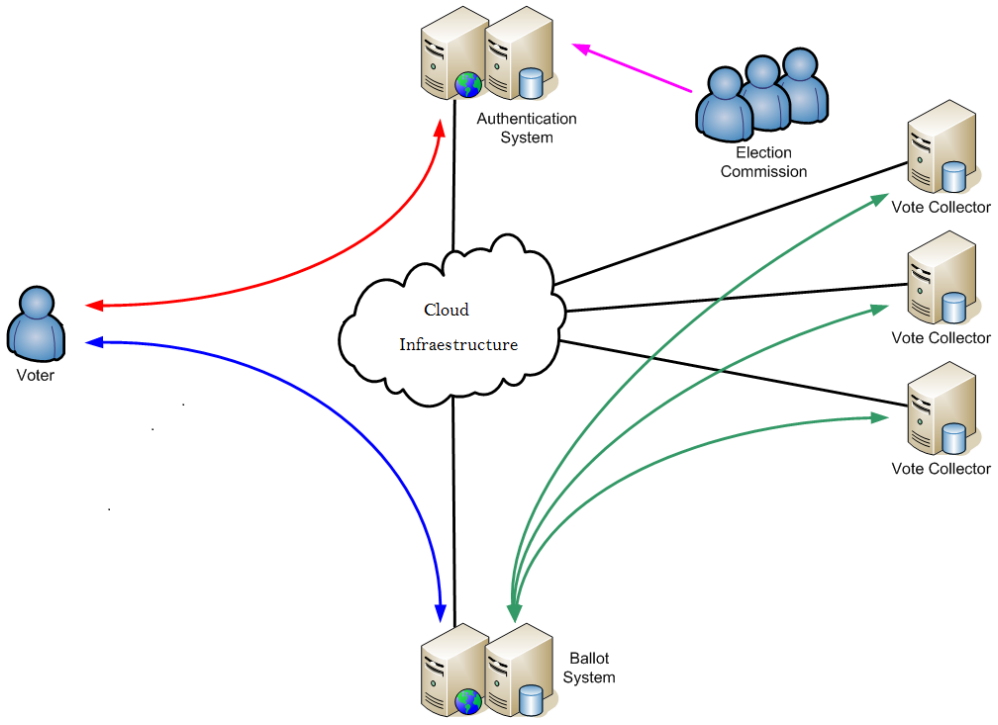


Figura 9: Plataforma de Voto Eletrónico

Seguidamente, serão apresentados e brevemente descritos os papéis de cada componente do sistema e-VaaS.

- O sistema de autenticação (AS) é responsável pela autenticação do eleitor durante a eleição, e pela entrega da credencial de voto anónima e da cédula eleitoral ao eleitor.

- O Ballot System (BS) chamado Cédula Eleitoral é responsável por receber votos encriptados, validando as credenciais a estes associadas, verificando se não foi usada anteriormente.

- Os votos que forem considerados válidos, são distribuídos para os Coletores de Voto (VC). Os VC só aceitam os votos provenientes do BS. Guardam os votos recebidos de forma aleatória e permitem fazer a contagem no final da eleição. Após a contagem, os votos ficam disponibilizados publicamente para recontagem.

A opção de se ter vários VC's, é uma funcionalidade essencial do sistema proposto, pois garante a existência de uma redundância geográfica adequada para os votos recolhidos. Existe também a possibilidade de replicar os componentes do AS e BS, de modo a alcançar a escalabilidade. Se a replicação se verificar, é possível segmentar o grupo de eleitores de acordo com a circunscrição eleitoral.

6.1 Software as a Service

Uma tarefa de grande importância é hospedar a plataforma. A plataforma desenvolvida, tal como próprio nome indica (Electronic Vote as as Service), será disponibilizada sob a forma de um serviço. O objetivo é minimizar as preocupações relativas à hospedagem do sistema, sendo que a empresa de tecnologias da informação na qual a plataforma vai ficar hospedada é que terá as preocupações relativas à segurança física da aplicação.

.

6.2 Papéis de Utilizador

Na solução proposta foram definidos alguns papéis de utilizador, nomeadamente:

- Administrador: O utilizador ao qual é atribuído este papel terá como função a criação de eleições e a seleção da comissão eleitoral.

- Comissão Eleitoral: As funções deste papel incluem dar início e fim às eleições, selecionar os candidatos e dar início às contagens.

- Eleitor: Os utilizadores aos quais é atribuído este papel têm como função exercer o seu direito de voto na plataforma.

6.2 Processo de Eleição

Para dar início ao processo de eleição (como explicado no Diagrama 1) é preciso haver uma sequência de passos:

- Passo 1 - O administrador cria a eleição e escolhe a comissão eleitoral.

- Passo 2 - A comissão eleitoral escolhe os indivíduos que irão participar na eleição. Finalizado este passo, é iniciado o processo de eleição.

- Passo 3 - Cada participante terá de se autenticar com sucesso na plataforma (e-VaaS), escolher a votação para a qual foi selecionado e usufruir do seu direito de voto.

  Seguidamente será mostrado e descrito em detalhe o processo de eleição, segundo os diferentes pontos de vista dos diferentes papéis de utilizador como mostrado na Figura 10 e explicado nas Tabelas que se seguem.

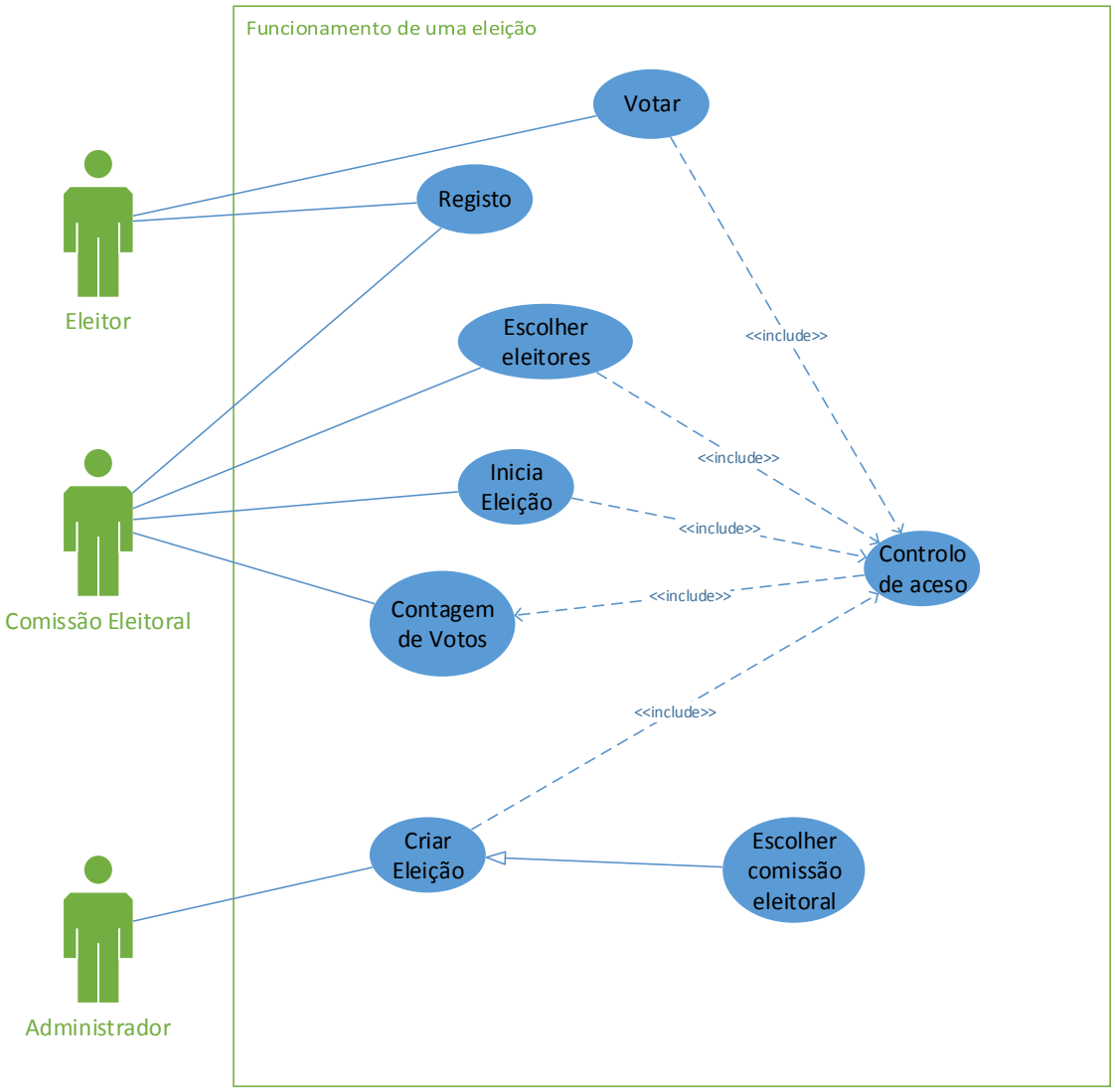


Figura 10: Diagrama Use Case do funcionamento de uma eleição.

Caso de Utilização	**Criar Eleição**

Ator(es)	Administrador
Pré-condição	Tem estar autenticado no sistema
Descrição	O ator em questão tem permissões para criar uma nova eleição.

Tabela 2: Descrição do caso de utilização “Criar Eleição”.

Caso de Utilização	**Registo**
Ator(es)	Utilizador
Pré-condição	N/A
Descrição	O ator pode efetuar um registo no sistema para eventualmente votar.

Tabela 3: Descrição do caso de utilização “Registo”.

Caso de Utilização	**Escolher Comissão Eleitoral**
Ator(es)	Administrador
Pré-condição	Tem estar autenticado no sistema
Descrição	O administrador pode escolher os membros pertencentes a comissão eleitoral.

Tabela 4: Descrição do caso de utilização “Escolher comissão eleitoral”.

Caso de Utilização	Escolher Eleitores
Ator(es)	Comissão Eleitoral
Pré-condição	Tem estar autenticado no sistema
Descrição	A comissão eleitoral pode escolher os eleitores que vão pertencer à votação.

Tabela 5: Descrição do caso de utilização “Escolher eleitores”.

Caso de Utilização	Inicia Eleição
Ator(es)	Comissão Eleitoral
Pré-condição	Tem estar autenticado no sistema
Descrição	A comissão eleitoral é o que tem os privilégios para iniciar as eleições.

Tabela 6: Descrição do caso de utilização “Inicia Eleições”.

Caso de Utilização	Votar
Ator(es)	Eleitores
Pré-condição	Tem estar autenticado no sistema
Descrição	Os eleitores podem exercer o seu direito a voto.

Tabela 7: Descrição do caso de utilização “Votar”.

Caso de Utilização	Contagem dos votos
Ator(es)	Comissão Eleitoral
Pré-condição	Tem estar autenticado no sistema
Descrição	A comissão eleitoral é o que tem os privilégios para iniciar à contagem dos votos.

Tabela 8: Descrição do caso de utilização “Contagem dos votos”.

6.3 Criação da eleição

Os passos necessários para a criação de uma nova eleição são os seguintes:

1) O administrador autentica-se na plataforma de voto eletrónico (e-VaaS) e cria uma eleição.
2) O administrador seleciona a comissão eleitoral que vai gerir as eleições de início a fim.
3) A comissão eleitoral terá de escolher os candidatos da eleição na plataforma de voto eletrónico (e-VaaS).
4) A comissão eleitoral terá de escolher os eleitores da eleição na plataforma de voto eletrónico (e-VaaS).
5) A comissão eleitoral é a responsável por dar inicio a eleição na plataforma de voto eletrónico (e-VaaS).
6) A comissão eleitoral é responsável por pedir a contagem dos votos na plataforma de voto eletrónico (e-VaaS).

6.4 Registo do Eleitor

O registo do eleitor deve ser iniciado antes do dia da eleição, de forma a ser possível averiguar, antecipadamente, quem tem permissão para participar. Um dos seguintes cenários poderá ser adotado [8]:

- **Cenário 1**: os eleitores necessitam de efetuar um registro prévio, por motivos eleitorais específicos. Neste cenário, podem ser usadas as técnicas usuais de registo, que poderão ou não requerer a identificação presencial do eleitor, dependendo das necessidades de autenticação e confidencialidade da eleição em causa [8];

- **Cenário 2**: os eleitores já possuem credenciais de acesso válidas em qualquer sistema que possa ser usado para fins eleitorais. Este cenário é o mais adequado para eleições de pequena dimensão e consequentemente menos críticas, nas quais os eleitores já se encontram de alguma forma registados para outros fins [8].

6.5 Inicialização e processo de voto

A Figura 8 apresenta a sequência de eventos e ações necessários para a inicialização e execução de um processo de votação completo. Como se poderá constatar, o sistema adota a utilização fiável de técnicas de criptografia assimétrica [41], [42] e usa de forma intensiva canais de comunicação seguros.

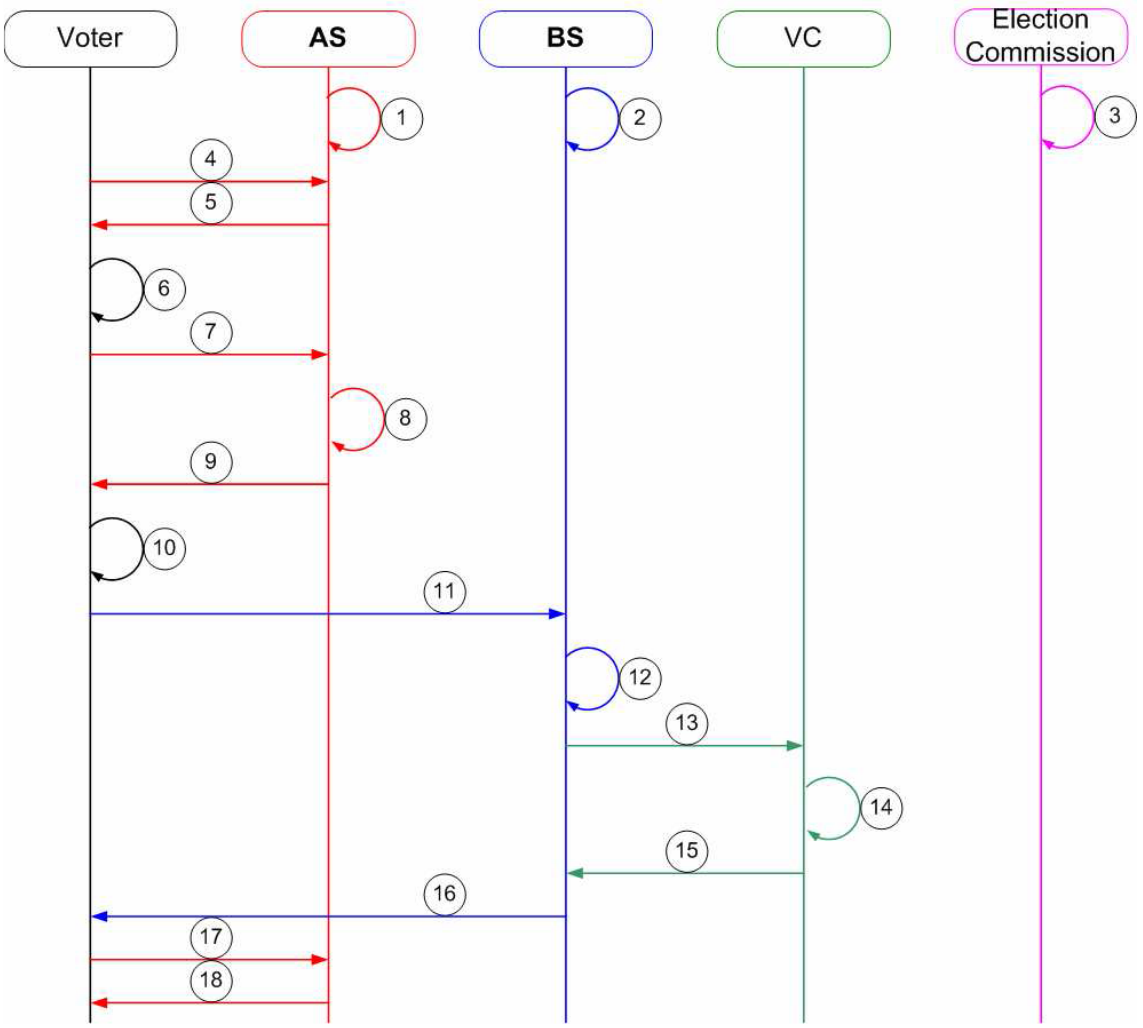


Figura 11: Diagrama de Sequência de uma Votação [8].

Cada um destes passos irá ser apresentado e descrito de forma individual, mas de uma forma geral, os passos 1 a 3 referem-se à fase de inicialização do sistema. Nos passos 4 a 9, o eleitor obtém a sua credencial e o seu boletim de voto. Nos passos 10 a 12, o eleitor submete o seu boletim de voto preenchido com a sua orientação ao BS. A replicação dos votos para os vários VC ocorre nos passos 13 a 15 e finalmente, nos passos 16 a 18, são entregues confirmações de votação concluída com sucesso ao eleitor e ao AS.
De seguida, será descrito cada um dos passos com mais detalhe:

1) **Inicialização do AS**. Neste passo é gerado para o AS um par de chaves assimétrico, constituído por uma chave pública e uma chave privada (ASprvK, ASpubK). Este par de chaves é usado para identificar inequivocamente o AS desde o início até ao fim das eleições. Como referido anteriormente, a chave privada nunca deverá sair da posse do

seu titular, e como tal, nunca deverá sair da posse do AS. A chave pública deverá ser tornada pública e irá ser utilizada quer pelo eleitor, quer pelo BS.

2) **Inicialização do BS**. De forma similar ao anterior, neste passo é gerado o par de chaves assimétrico para o BS (BSprvK, BSpubK), sendo este par de chaves usado para identificar inequivocamente o BS desde o início até ao fim das eleições. Como referido anteriormente, a chave privada nunca deverá sair da posse do seu titular, e como tal, nunca deverá sair da posse do BS e a chave pública deverá ser tornada pública e irá ser utilizada quer pelo eleitor para cifrar o voto, quer pelo VC para validar os votos.

3) **Inicialização do EC**. Neste passo também é gerado um par de chaves assimétrico para o EC (ECprvK, ECpubK). Este par de chaves é usado para identificar inequivocamente o EC desde o início até ao fim das eleições, principalmente na fase de contagem dos votos. A chave privada, neste caso em particular, deve ser dividida e distribuída pelos vários membros que constituem a EC (ECprvKn, n=1...N), e a máquina usada para a sua geração deverá ser selada e armazenada em local seguro. A chave pública deve ser tornada pública e ser utilizada pelo eleitor. A partir deste momento, o SVE está preparado para dar início à votação.

4) A partir deste passo, é iniciado o processo da votação propriamente dita. O eleitor começa por aceder à plataforma de voto eletrónico (e-VaaS) do AS e usa as suas credenciais de registo para se autenticar como eleitor.

5) O AS, após ter procedido à validação da autenticação do eleitor, fornece-lhe uma aplicação "*client-side (applet)*", e as chaves públicas do AS (ASpubK), BS (BSpubK) e EC (ECpubK), sendo este processo completamente automático. O eleitor tem apenas de dar início ao mesmo.

6) Seguidamente, a aplicação *"client-side"* gera um par de chaves assimétrico que permitirá identificar o eleitor (VprvK, VpubK).

7) A aplicação "*cliente-side*" envia a chave pública do eleitor (VpubK) para o AS, não podendo, após esta fase, submeter uma outra chave pública distinta.

8) O AS armazena a chave pública do eleitor (VpubK) na sua base de dados e gera uma *"hash" resultante* da combinação do *"username"* do eleitor e um número grande aleatório. De seguida, adiciona o *"Electoral Circumscription Identifier"* (ECI) do eleitor

(este servirá para identificar, por exemplo, o local onde o seu voto será contabilizado ou o seu peso) e assina os dados resultantes com a sua chave privada (ASprvK), criando a credencial (Cred). Esta é então cifrada com a chave pública do eleitor (VpubK) dando origem ao EncCred, de forma a somente ele conseguir aceder à informação que a mesma contém como apresentado na Tabela 2.

hash= SHA-256(username+rand(LongInt)	A
hashWithECI = SHA-256(hash,ECI)	B
SignedHashWithECi = Sign(hash, ASprvK)	C
Cred = (hashWithECI, ECI, SignedHashWithECI)	D
SymmCiph = SymmetricCipher(Cred)	E
AssymmCiphKey = AssymmetricCipher(SymmCiphKey, VpubK)	F
EncCred = (SymmCiph, AssymmCiphKey, ivSpec)	G

Tabela 9: Criação da EncCred

- Todas estas *strings* são guardadas com formatação XML.

- Todos os dados são codificados pelo base64 que é um sistema numérico que usa unicamente os caracteres ASCII imprimíveis, ou seja, é uma forma de evitar caracteres não legíveis ao passar dados.

- Para encriptar simetricamente foi usado o algoritmo AES, neste algoritmo é necessário criar um vetor de inicialização (ivSpec) e este vetor tem que ser o mesmo tanto na cifragem como na decifragem.

9) O AS devolve a credencial cifrada (EncCred) ao eleitor.

10) A aplicação *"client-side"* apresenta ao eleitor o boletim para este preencher e assim cumprir o seu direito de voto. Após esse passo, a aplicação "client-side" decifra a credencial (EncCred) com a chave privada do eleitor (VprvK), cifra o boletim e o ECI com a chave pública da EC (ECpubK) criando o *"ciphered ballot"* (CiB), a este junta a

credencial e cifra o resultante com a chave pública do BS (BSpubK), dando origem ao *"double ciphered ballot"* (dCiB) como mostrado na Tabela 3 abaixo apresentada.

SymmetricKey=AssymmetricDecipher(AssymmCiphKey, VprvK).	H
Cred = SymmetricDecipher(SymmCiph, SymmetricKey, ivSpec)	I
SymmCiph2 = SymmetricCipher(Ballot+ECI)	J
AssymmetricKeyCiph2= AssymmetricCipher(SymmCiph2Key, ECpubK)	K
CiB = (SymmCiph2, AssymmetricKeyCiph2, ivSpec2)	L
SymmCiph3= (SymmetricCipher(Cred+CiB)	M
AssymmetricKeyCiph3 = (AssymmetricCipher(SymmCiph3Key, BSpubK)	N
dCiB = (SymmCiph3, AssymmetricKeyCiph3, ivSpec3)	O

Tabela 10: Criação do dCiB.

11) A aplicação "*client side"* a correr na máquina do eleitor envia o dCiB ao BS (Neste momento envia o dCiB ao AS e o AS envia ao BS*).

12) O BS decifra o dCiB com a sua chave privada (BSprvK), valida se a credencial está assinada com a chave pública do AS (ASprvK) e se ainda não foi usada. De seguida, assina o CiB com a chave privada do BS (BSprvK), criando o *"signed ciphered ballot"* (SiCiB) e marca a credencial como já tendo sido usada como apresentado na Tabela 4.

SymmetricKey3=AssymmetricDecipher(AssymmetricKeyCiph3, BSprvK)	P
(CiB + Cred)= SymmetricDecipher(SymmCiph3, SymmetricKey3, ivSpec3)	Q
Result = Validate(Cred, ASpubK)	R
SiCiB = (CiB+Sign(CiB, BSprvK))	S

Tabela 11: Criação do SiCiB.

- Caso o resultado da validação retorne true, então é possível assinar o CiB, caso não retorne true, significa que não foi assinada com a chave privada do AS ou foram adulterados os dados, ou seja, fica invalidado o voto e não será possível avançar ao seguinte passo.

13) O BS envia o SiCiB para o VC, ou, preferencialmente, para múltiplos VC.

14) O VC valida se o SiCiB foi devidamente assinado com a chave privada do BS(BSprvK) e armazena-o aleatoriamente como mostrado na Tabela 5.

Result2 = Validate(SiCiB, BSprvK)	T

Tabela 12: Validação do SiCiB.

- Caso o resultado da validação retorne true, então é possível guardar o SiCiB guardar aleatoriamente em ficheiro o SiCiB para a sua posterior decifragem e contage, caso não retorne true, significa que não foi assinada com a chave privada do BS ou foram adulterados os dados, ou seja, fica invalidado o voto e não será possível avançar ao seguinte passo.

15) Cada VC deve confirmar perante o BS a correta receção do SiCiB.

16) O BS confirma a correta receção do CiB com uma credencial válida, uma vez que a mesma vem assinada com a chave privada do AS (ASprvK), ao eleitor.

17) O eleitor confirma ao AS que finalizou com sucesso o seu processo de votação.

18) O AS confirma ao eleitor que este finalizou corretamente todo o processo de votação, e como tal, que não será capaz de votar novamente.

O diagrama BPMN[5] abaixo, pretende demonstrar o fluxo do processo da aplicação de início a fim.

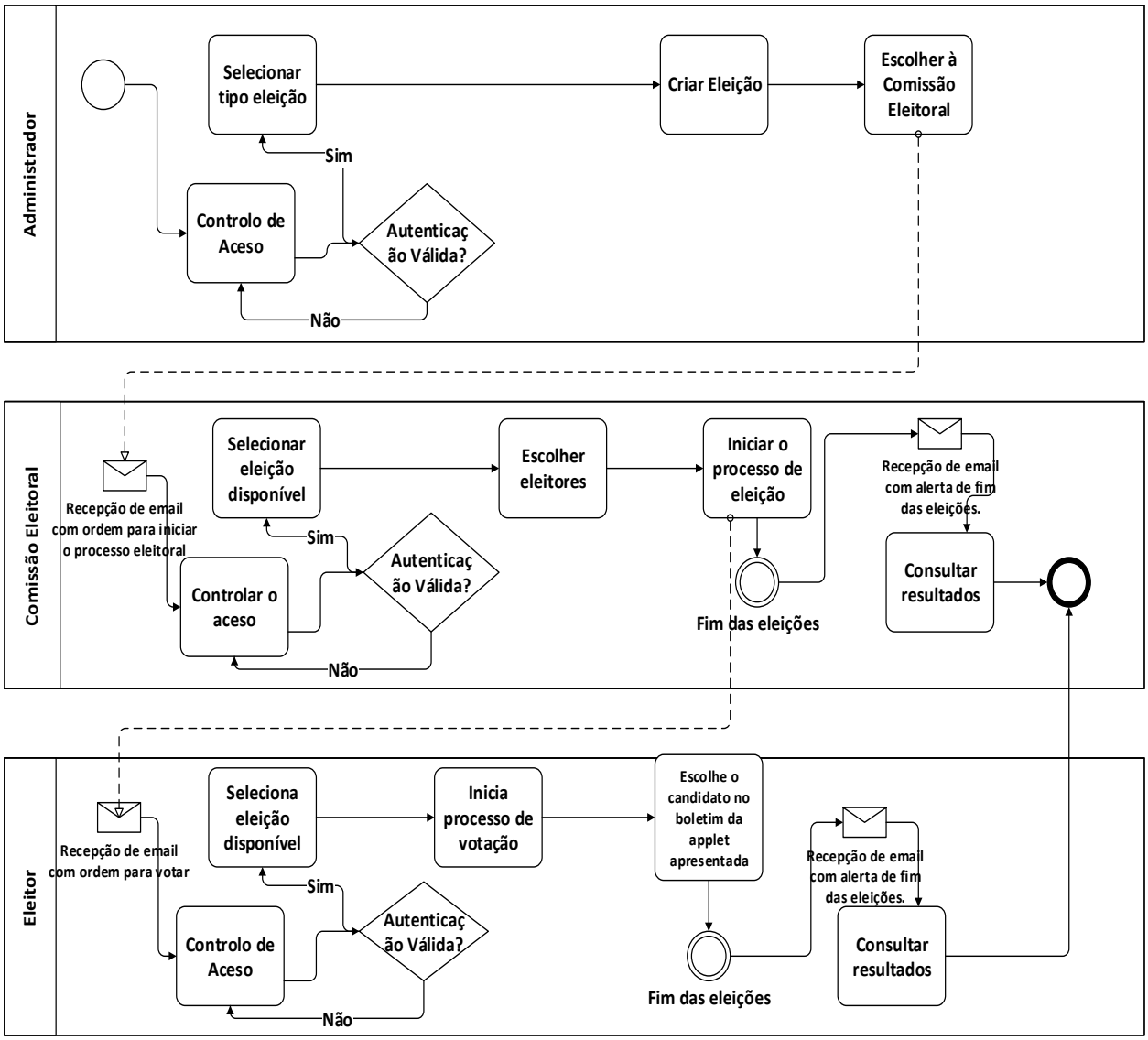


Figura 12: Diagrama BPMN do todo o processo da aplicação.

[5] http://www.bpmn.org/

6.6 Contagem dos Votos

A contagem dos boletins de voto é uma das tarefas mais críticas, sendo que deve garantir-se que o resultado desta contagem é verdadeiramente representativo da escolha dos eleitores. De forma a aumentar a fiabilidade e verificabilidade do sistema, sugerimos o uso da replicação distribuída dos boletins, tal como já fora mencionado na secção anterior [8].

Após o término das eleições, a chave privada da EC que havia sido dividida, é reunida e tornada pública. No entanto, a chave privada do BS (BSprvK) deve ser destruída primeiro, para se garantir a impossibilidade de alterar os votos já depositados. Nesta fase, uma vez que tudo é tornado público em cada VC, podem ser utilizadas aplicações diferentes para contagem dos votos, garantindo assim uma elevada transparência e fiabilidade do processo de contagem [8].

Adicionalmente, os votos de todos os VC podem ser unidos, de forma a eliminar duplicados e ultrapassar possíveis perdas esporádicas de votos em algum VC. Como resultado, obtemos um conjunto final de votos para contagem muito fiável.

As aplicações de contagem acima mencionadas não precisam de ser fornecidas pelo sistema de votação eletrónica, pois existirá informação pública suficiente para qualquer pessoa, caso o deseje, confirmar os resultados das eleições, acedendo para isso a todos os votos armazenados através dos múltiplos VC. No entanto, e embora os mesmos resultados devam ser obtidos, obviamente, os resultados oficiais da contagem dos votos deve ser levada a cabo pela EC e representantes de todas as partes envolvidas [8].

Este processo de contagem é totalmente seguro, pois todos os votos podem ser decifrados e validados, mas não podem ser alterados, uma vez que a chave privada do BS (BSprvK) foi previamente destruída.

Este processo de contagem é totalmente seguro, pois todos os votos podem ser decifrados e validados, mas não podem ser alterados, uma vez que a chave privada do BS (BSprvK) foi previamente destruída como mostrado na Tabela 6.

Result3 = Validate(SiCiB, BSprvK)	U

SymmetricKey2=AssymmetricDecipher(AssymmCiphKey2, ECprvK).	V
(Ballot, ECI) = SymmetricDecipher(SymmCiph2, SymmetricKey2, ivSpec2)	W

Tabela 13: Obtenção do boletim de voto (ballot) e do ECI.

A obtenção do boletim de voto é feita através da decifragem do SiCiB tal e como é explicado nas tabelas, este SiCiB foi guardado em ficheiro no passo 14.

- A obtenção dos votos é feita pela comissão eleitoral, ou seja, a comissão eleitoral pede a contagem de votos ao/aos Vote Collector(s) e recebe o resultado.

- É comparado o número de candidatos com o número de votos como forma de verificação. Se o número votos coincidir com o número total de eleitores, é finalizado o processo eleitoral, sendo os respetivos resultados tornados públicos, Se os números não coincidirem a eleição é considerada fraudulenta e, consequentemente, inválida.

6.7 Arquitetura da Solução e Tecnologias usadas

Nesta secção será apresentada e descrita a arquitetura da solução desenvolvida, assim como as tecnologias que a suportam. Na Figura 12 , encontra-se ilustrado um diagrama representativo do modelo da arquitetura desenhada para suportar a solução e-VaaS, que será descrito com mais detalhe de seguida.

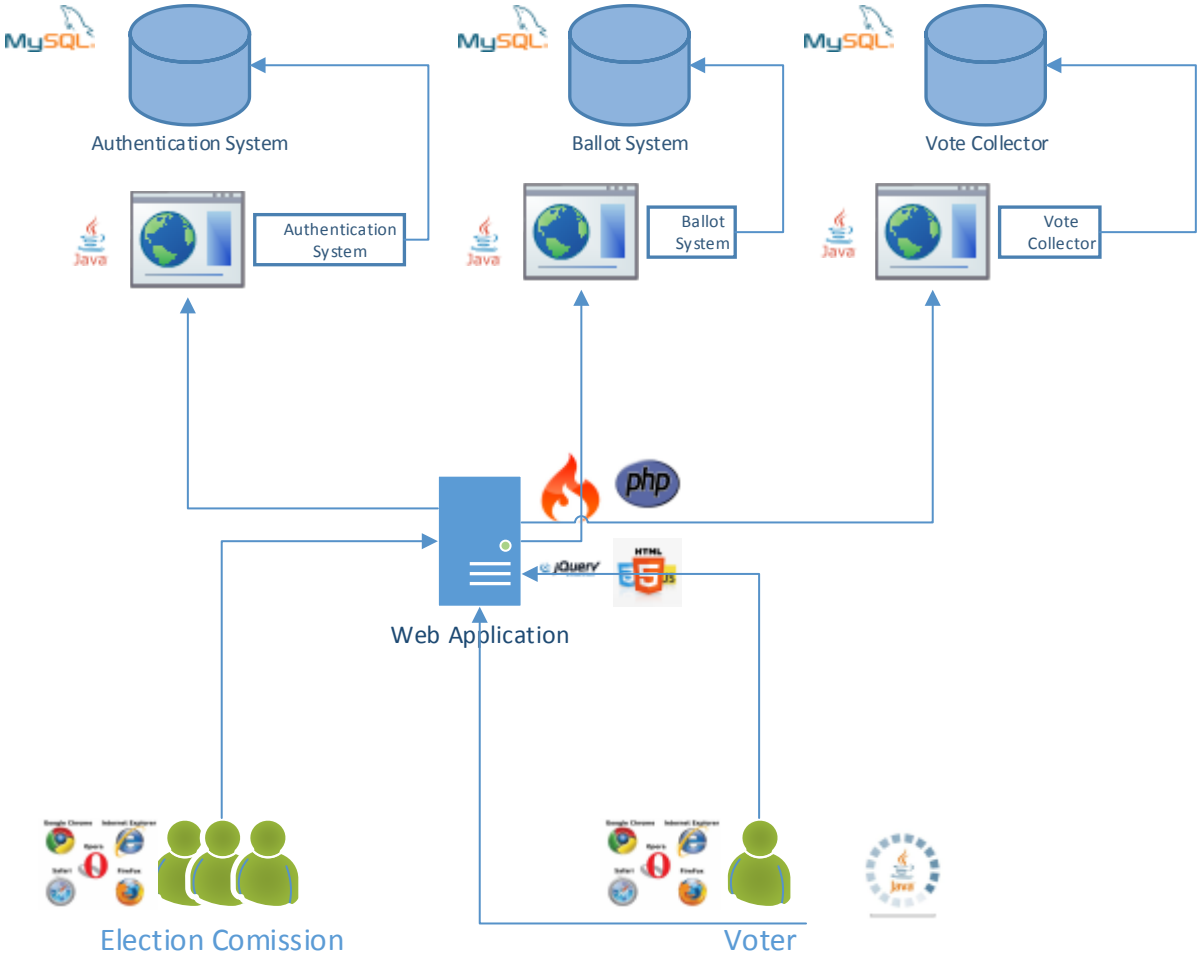


Figura 13: Arquitetura da Solução

O modelo da arquitetura, ilustrado na Figura 12 acima apresentada, pode ser dividido em três grandes camadas: o *frontend*, responsável pela interação do utilizador com o sistema de voto eletrónico, o *backend*, responsável pelo processamento de todos os dados relacionados com a votação e os seus intervenientes, e a camada de dados, responsável pelo armazenamento desses mesmos dados. De seguida, será descrita cada uma dessas camadas, apresentando cada um dos componentes que as compõem assim como as linguagens e/ou *frameworks* utilizados para os desenvolver.

6.7.1 Frontend do sistema e-VasS

Tal como já fora acima referido, o *frontend* é responsável pela interação do utilizador com o sistema. Neste caso específico, sendo o e-Vote um serviço distribuído via *web*, a interação dos utilizadores com o mesmo é feita através de navegadores *web*. O sistema desenvolvido é suportado pelos navegadores web mais populares, nomeadamente, o Internet Explorer[6], Google Chrome[7], Safari [8], Mozilla Firefox[9] e Opera[10].

Para o desenvolvimento da camada de *frontend*, recorreu-se às linguagens HTML[11] (*HyperText Markup Language*), CSS [12] (*Cascading Style Sheets*) e à *framework* de Javascript[13], JQuery.

6.7.2 Backend do sistema e-VasS

O *backend* do sistema, tal como já fora referido anteriormente, é a camada responsável pelo processamento de todos os dados relacionados com a votação e os seus intervenientes. Para a sua implementação recorreu-se à *framework* de PHP Code Igniter[14], que usa o padrão de *software* MVC (*Model View Controller*).

6.7.2.1 Serviços que suportam o e-VaaS

Para suportar um processo eleitoral, o sistema e-VaaS tira partido de um conjunto de serviços *web* para levar a cabo as suas funções, nomeadamente o AS (*Authentication System*), o BS (*Ballot System*) e o VC (*Vote Colector*).

O AS tem como função gerir o processo de autenticação do sistema. Além de responsável pela correta identificação do eleitor é também responsável pelo fornecimento de uma *applet "client-side"* a cada um dos eleitores, que por sua vez irá gerar um par de chaves assimétrico (VprvK, VpubK) que permitirá identificar o eleitor.

---

[6] Internet Explorer: (http://windows.microsoft.com/es-xl/internet-explorer)
[7] Google Chrome: (http://www.google.com/intl/es/chrome/)
[8] Safari: (https://www.apple.com/es/safari/)
[9] Mozilla Firefox: (https://www.mozilla.org/es-ES/firefox/new/)
[10] Opera: (http://www.opera.com/es)
[11] HTML: (https://developer.mozilla.org/es/docs/Web/HTML)
[12] CSS: (http://www.w3c.es/Divulgacion/GuiasBreves/HojasEstilo)
[13] Javascript: (https://developer.mozilla.org/es/docs/Web/JavaScript)
[14] Code Igniter: (https://ellislab.com/codeigniter)

O BS é responsável por receber os votos cifrados, validar as respetivas credenciais, verificar que não foram usadas previamente e distribuir os votos validados pelos vários “Vote Collectors” (VC);.

O VC aceita os votos provenientes apenas do BS, validando a sua origem através de técnicas criptográficas (assinatura), guardando-os aleatoriamente e permitindo a sua contagem após finalizada a eleição.

A *applet* será responsável pela geração das chaves do lado do cliente e permitindo o mostrando o boletim de voto, trazendo deste modo mais segurança ao sistema.

Todos estes serviços foram desenvolvidos como serviços externos recorrendo à linguagem Java[15].

6.7.3 Camada de Dados do Sistema e-VaaS

Para o armazenamento de todos os dados do sistema e-VaaS, recorreu-se a um conjunto de bases de dados.

Existem duas bases de dados distintas, que podem estar geograficamente distribuídas: uma que é responsável por dar suporte ao sistema de autenticação (AS), armazenando toda a informação do *backend,* e a responsável por dar suporte ao sistema de cédula (BS), armazenando as suas chaves e a chave pública do AS. Foi também criada uma base de dados adicional, designada coletor de voto (VC), que permite armazenar dados sobre este serviço adicional, cuja finalidade é ser invocado como um serviço *web* para fazer a contagem de votos e devolver os respetivos resultados.

Para a gestão destas bases de dados recorreu-se ao sistema de gestão de base de dados MySQL[16], devido ao facto de este ser uma opção gratuito, fácil de usar e bastante robusta, tendo já dando provas da sua qualidade no mercado [8].

6.7.3.1 Descrição de alto nível do modelo de dados

Nesta secção será apresentada uma descrição de alto nível de cada uma das bases de dados mencionadas anteriormente.

[15] Java: (https://www.java.net/)
[16] MySQL: (http://www.mysql.com/)

6.7.3.1.1 Modelo de dados do Authentication System.

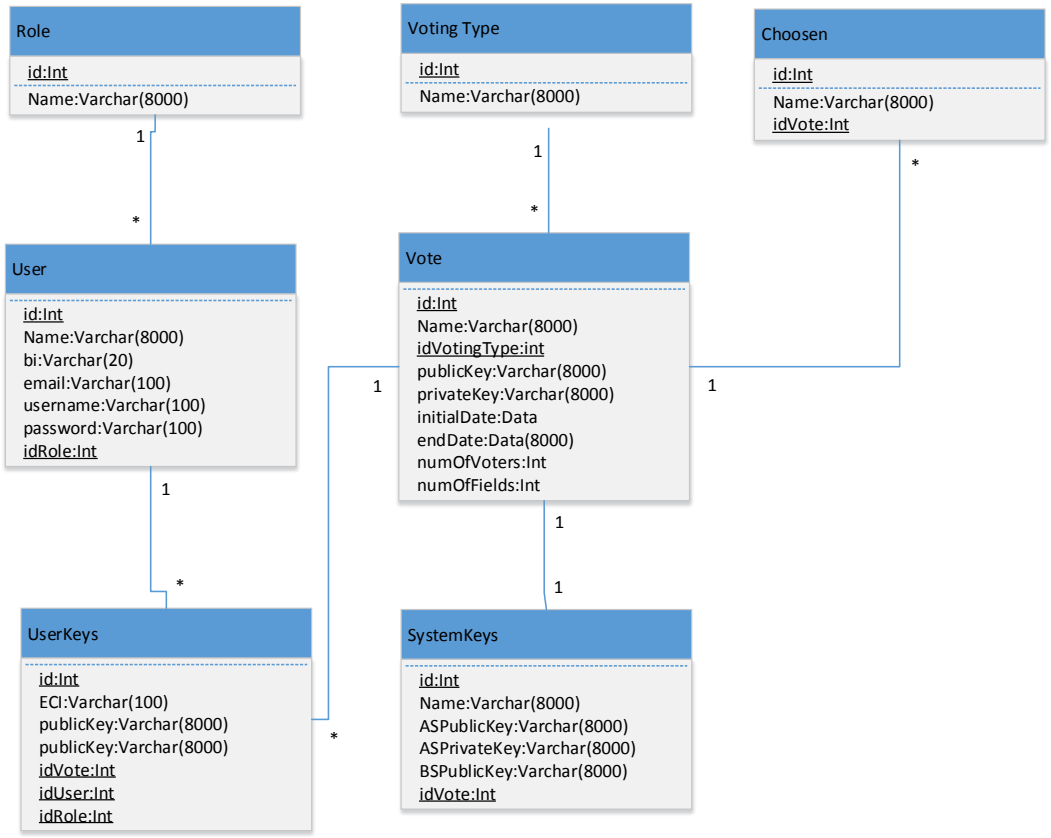


Figura 14: Base de dados do AS.

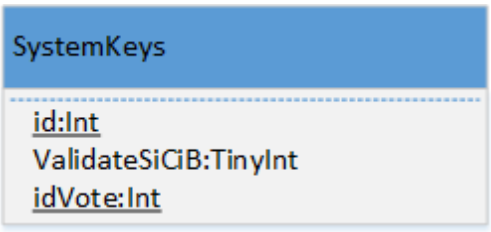


Figura 15: Base de dados do BS

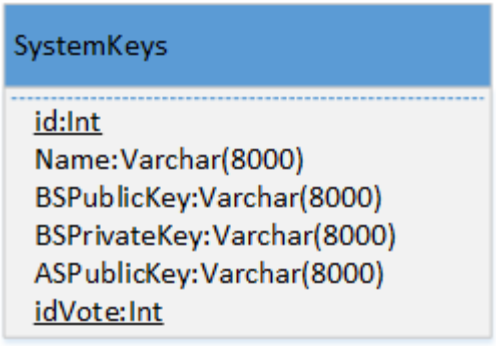


Figura 16*:* Base de dados protótipo do VS.

Seguidamente, será descrita cada uma das tabelas que compõem o modelo de dados acima apresentado.

Tabela *Role*

Esta tabela tem o objetivo de definir os papéis de cada utilizador que esteja autenticado na aplicação informática.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
Name	Varchar(100)	Não	Não	Não	Não

Tabela 14: Role do AS.b

Tabela *VotingType*

Esta tabela tem o objetivo de definir os tipos de votação existentes na plataforma de voto eletrónico.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?

Id	Inteiro	Não	Sim	Sim	Não
Name	Varchar(100)	Não	Não	Não	Não

Tabela 15: VotingType do AS.

Tabela *Vote*

Esta tabela tem o objetivo de guardar todos os dados necessários sobre uma votação eletrónica.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
Name	Varchar(100)	Não	Não	Não	Não
idVotingType	Inteiro	Não	Não	Não	Não
publickKey	Varchar(8000)	Sim	Não	Não	Não
privateKey	Varchar(8000)	Sim	Não	Não	Não
initialDate	Data	Não	Não	Não	Não
endDate	Data	Não	Não	Não	Não
numFields	Inteiro	Não	Não	Não	Não
NumberOfVoters	Inteiro	Não	Não	Não	Não

Tabela 16: Vote do AS

Tabela *SystemKeys*

Esta tabela tem o objetivo de guardar as chaves pública e privada do AS e a chave pública do BS.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
ASPublicKey	Varchar(8000)	Não	Não	Não	Não
ASPrivateKey	Varchar(8000)	Não	Não	Não	Não
BSPublicKey	Varchar(8000)	Sim	Não	Não	Não

idVote	Inteiro	Não	Não	Não	Sim

Tabela 17: SystemKeys do AS.

Tabela User

Esta tabela tem o objetivo de guardar toda a informação referente ao um utilizador da aplicação informática.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
name	Varchar(8000)	Não	Não	Não	Não
Bi	Varchar(20)	Não	Não	Não	Não
email	Varchar(100)	Não	Não	Não	Não
username	Varchar(100)	Não	Não	Não	Sim
password	Varchar(100)	Não	Não	Não	Não
idRole	Inteiro	Não	Não	Não	Sim

Tabela 18: User do AS

Tabela *Choosen*

Esta tabela tem o objetivo de guardar a informação básica sobre as pessoas que vão ser escolhidas para serem votadas.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
name	Varchar(1000)	Não	Não	Não	Não
idVote	Inteiro	Não	Não	Não	Sim

Tabela 19: Choosen do AS.

Tabela *UserKeys*

Esta tabela tem o objetivo de guardar informação sobre os utilizadores que vão participar em uma votação específica.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
publicKey	Varchar(8000)	Sim	Não	Não	Não
ECI	Varchar(100)	Sim	Não	Não	Não
idVote	Inteiro	Não	Não	Não	Sim
idUser	Inteiro	Não	Não	Não	Sim
idRole	Inteiro	Sim	Não	Não	Sim
publicKey	Varchar(8000)	Sim	Não	Não	Não

Tabela 20: UserKeys do AS

Tabela *SystemKeys* do modelo de dados do BS

Esta tabela tem o objetivo de guardar as chaves pública e privada do BS e a chave pública do AS.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
BSPublicKey	Varchar(8000)	Não	Não	Não	Não
BSPrivateKey	Varchar(8000)	Não	Não	Não	Não
ASPublicKey	Varchar(8000)	Sim	Não	Não	Não
idVote	Inteiro	Não	Não	Não	Não

Tabela 21: SystemKeys do BS

Tabela *SystemKeys* do modelo de dados do VC

Esta tabela tem o objetivo de validar se o SiCiB é valido, caso seja inválido a votação é fraudulenta e põe em questão todo o processo eleitoral, caso seja válido não haverá nenhum problema com a eleição.

Campo	Tipo	É nulo?	Auto Increment?	Chave primária?	Chave Estrangeira?
Id	Inteiro	Não	Sim	Sim	Não
ValidateSiCiB	tinyInt	Sim	Não	Não	Não
idVote	Inteiro	Não	Não	Não	Não

Tabela 22: SystemKeys do VC

7. Protótipo

7.1 Resultados

Uma das primeiras ações que é possível de executar ao tentar aceder a plataforma de voto eletrónico é efetuar o registo ou efetuar a autenticação no sistema, tal como se encontra ilustrado na Figura 17.

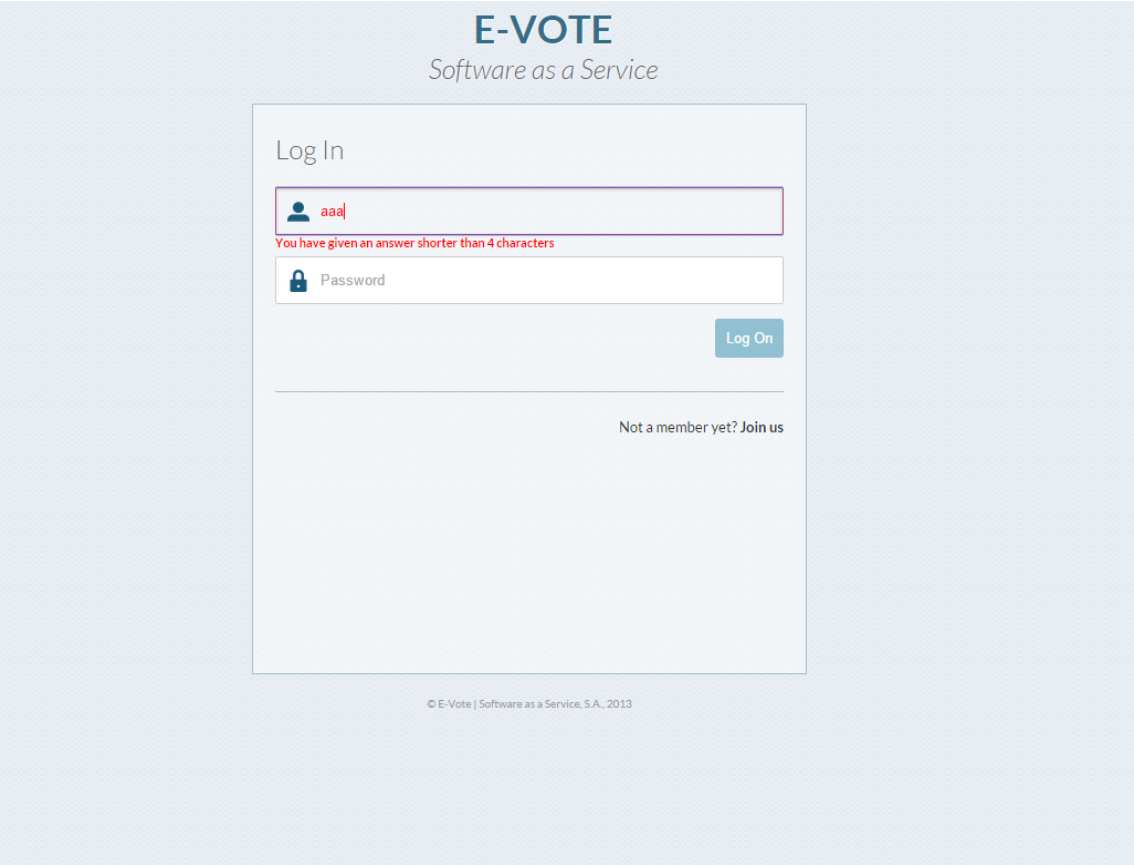


Figura 17: Página de autenticação da plataforma de voto eletrónico

Inicialmente, o administrador poderá autenticar-se no sistema e ver/criar/editar/apagar a eleição que pretender. Para o administrador será possível criar vários tipos de eleição e como tal aplicar vários tipos de segurança a cada eleição, tal como ilustrado na Figura 18.

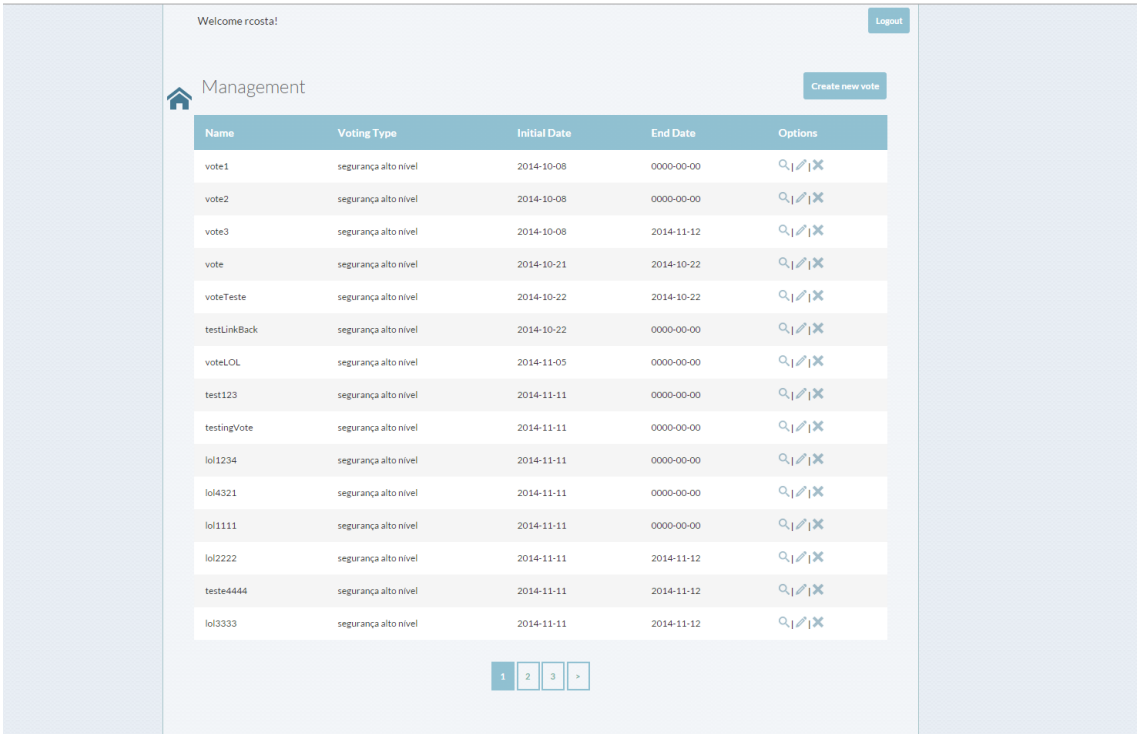


Figura 18: CRUD de uma eleição.

Uma vez criada uma eleição com um tipo de segurança de nível alto, será possível assignar os elementos que irão fazer parte da comissão eleitoral. Estes elementos têm de estar previamente registados na plataforma de voto eletrónica para poderem ser escolhidos para integrar na comissão eleitoral, tal como ilustrado na Figura 19.

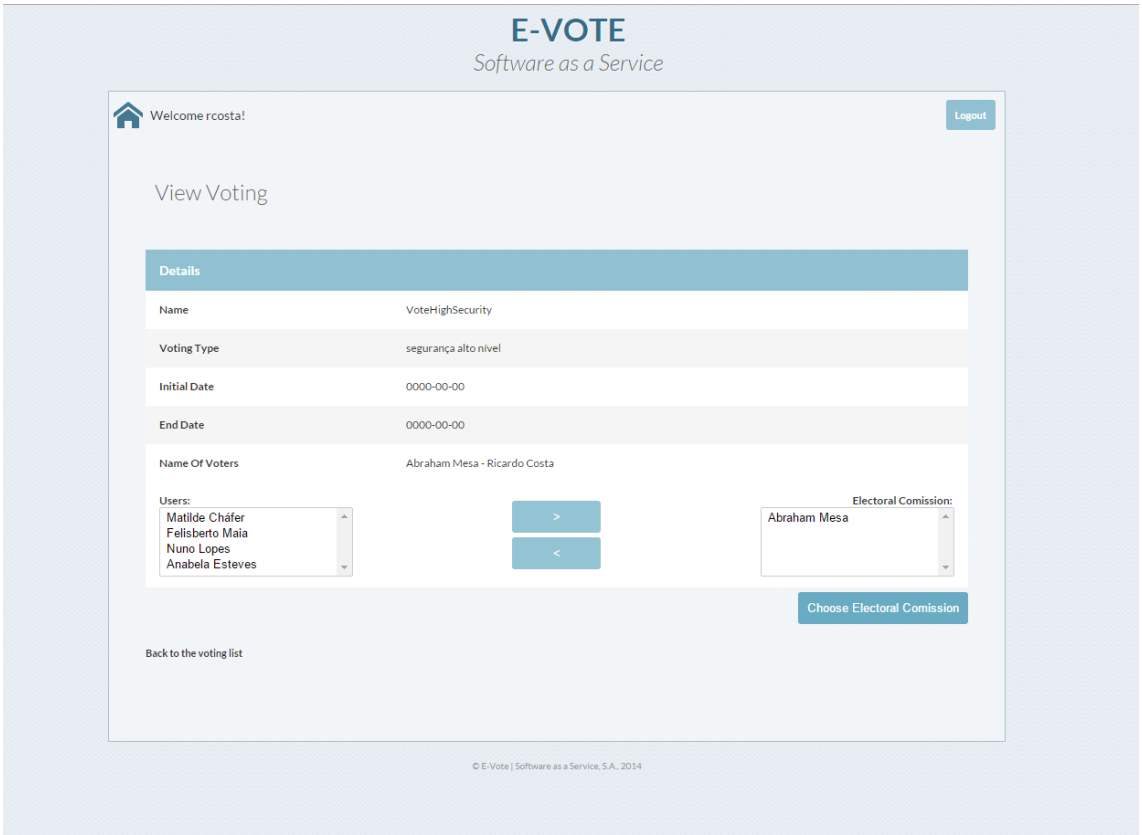


Figura 19: Processo de seleção dos elementos da comissão eleitoral.

De seguida, será explicado passo a passo o processo de eleição na plataforma de voto eletrónico. Uma vez autenticado um elemento da comissão eleitoral poderá dar inicio as eleições e escolher os utilizadores do sistema que fazem parte da eleição como mostrado na Figura 20.

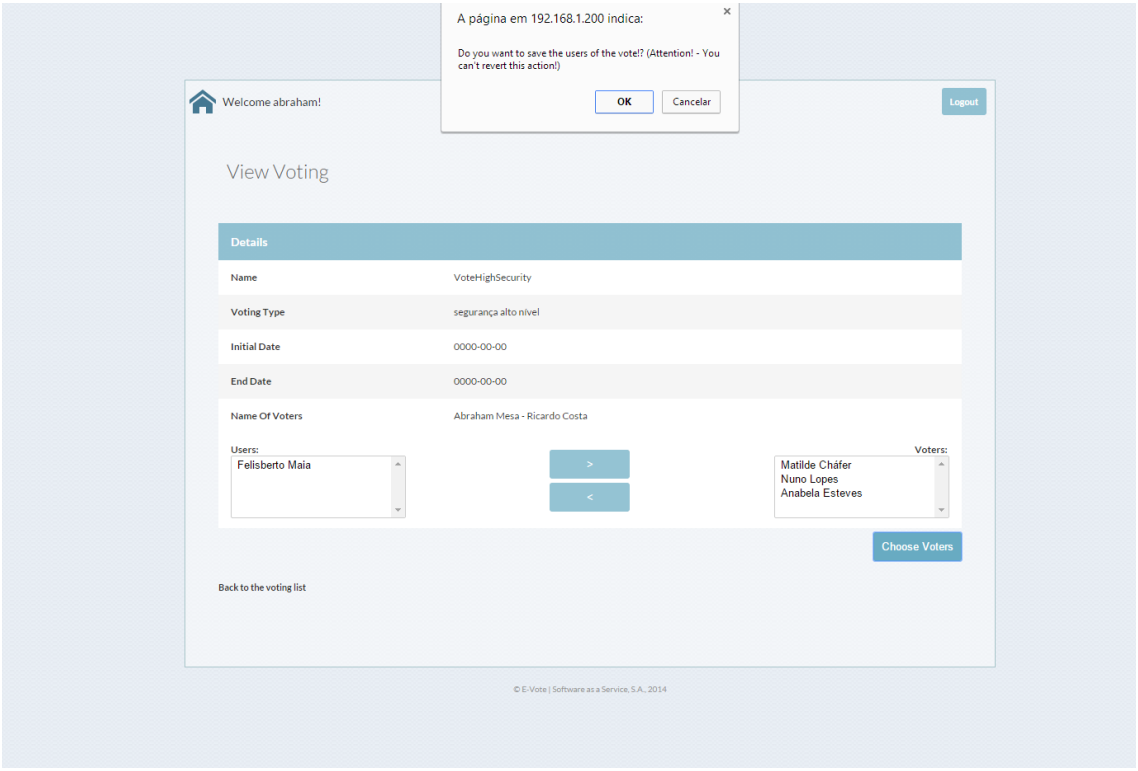


Figura 20: Processo de seleção dos elementos da eleição eleitoral.

Uma vez iniciada a eleição, um utilizador poderá autenticar-se na plataforma de voto eletrónico e selecionar a votação para o qual foi selecionado para participar como ilustrado na Figura 21.

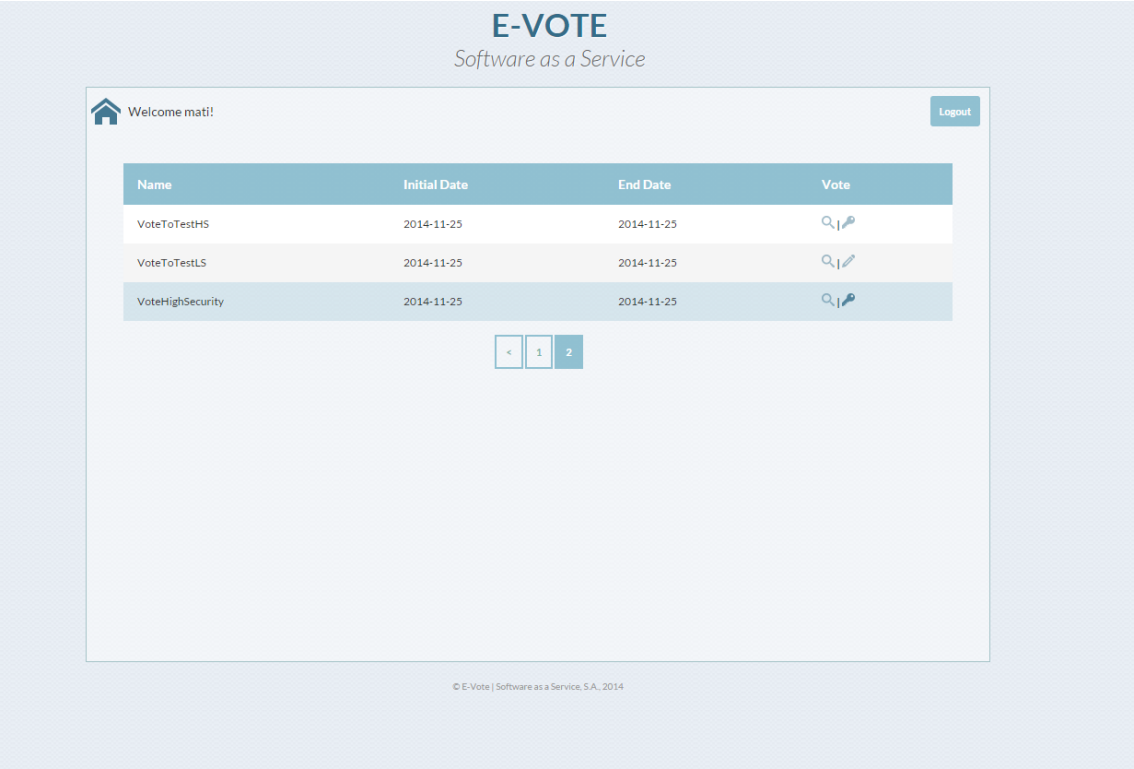


Figura 21: Eleitor inicia o seu processo de eleição.

Após o eleitor ter selecionado a votação em que pretende participar, ser-lhe-á presentada uma *applet* com o boletim de voto no qual poderá fazer a sua escolha. A partir desse momento, o eleitor terá que esperar até o final das eleições para saber os resultados e não poderá votar novamente.

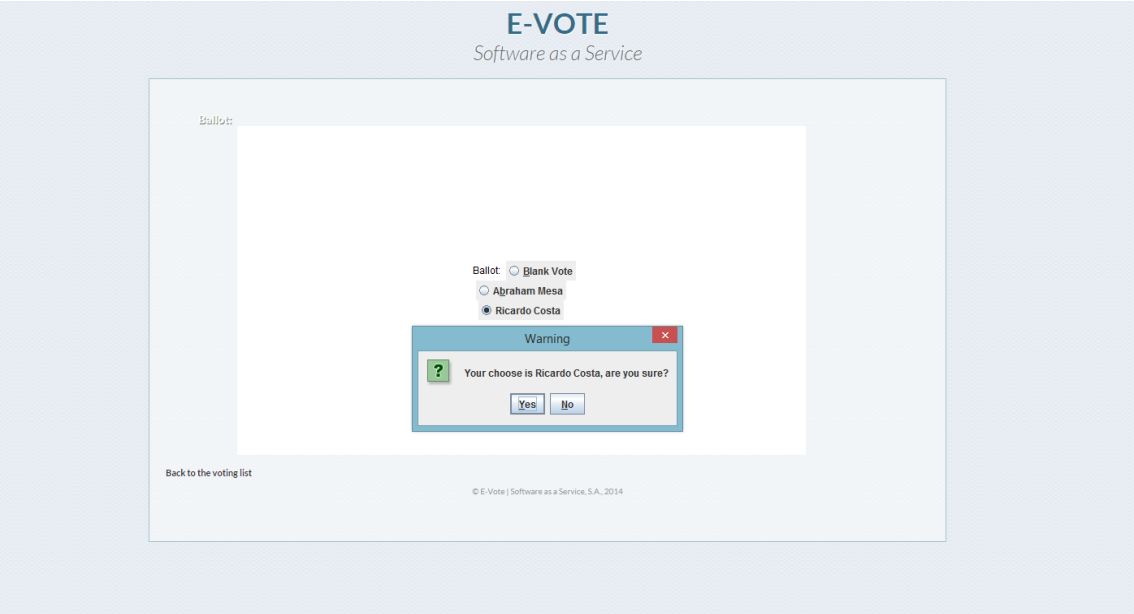
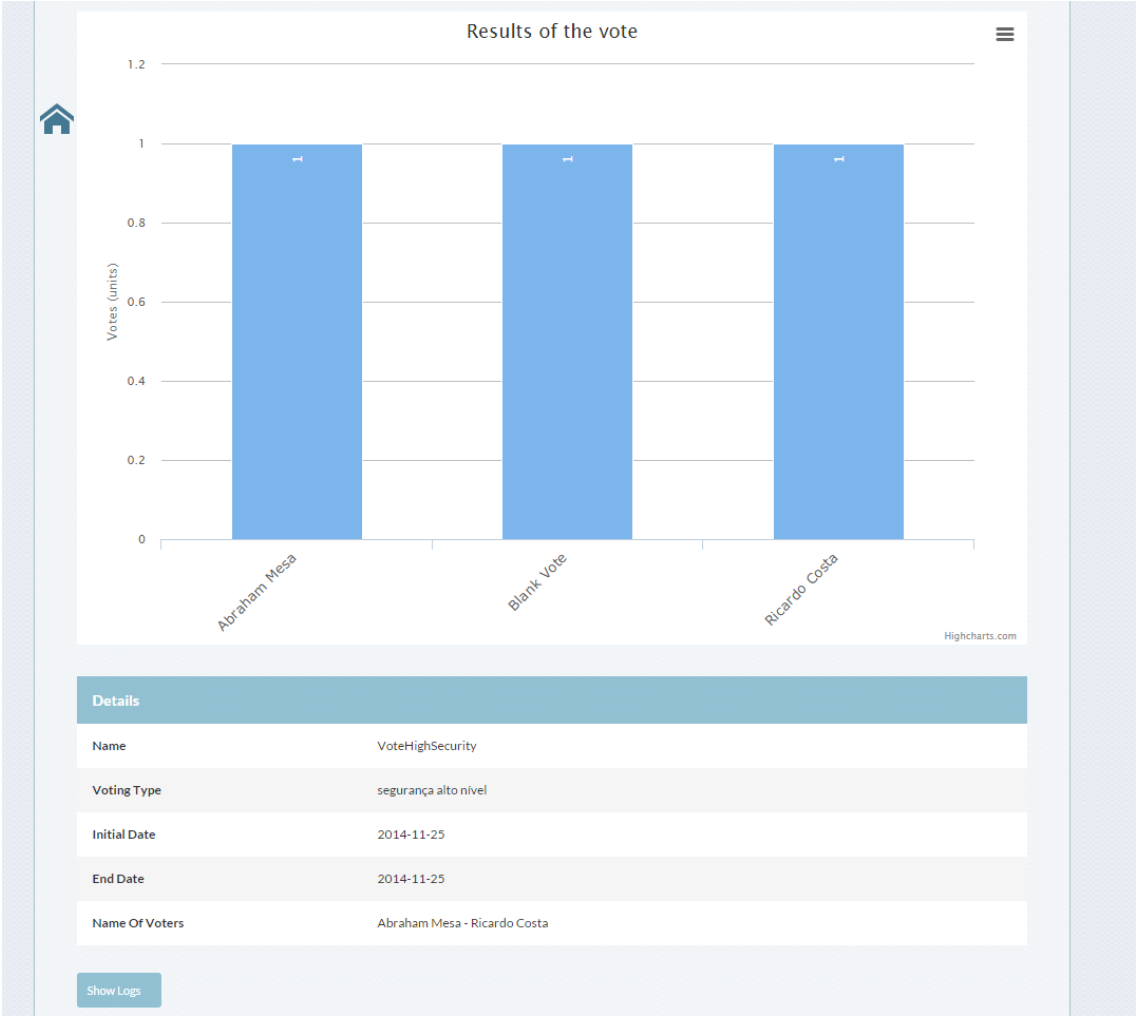


Figura 22: A plataforma de voto eletrónico mostra a applet com o boletim eletrónico.

Finalmente, tanto para os eleitores como para a comissão eleitoral será possível consultar o resultado da eleição. A comissão eleitoral terá uma opção para consultar os *logs* [17] das eleições de maneira a poder ter alguma informação sobre todo o processo eleitoral sem quebrar os pontos de segurança referidos anteriormente. Como mostrado na Figura 23.

[17] Log – Registo



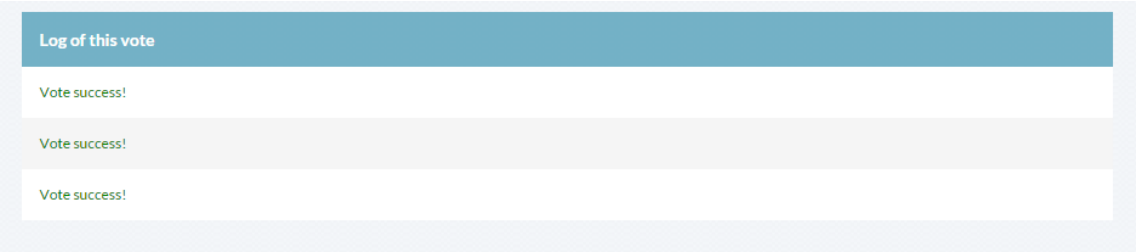


Figura 23: Resultado e log da eleição.

8. Conclusão

Este estudo teve como objetivo desenvolver uma plataforma eletrónica, segura e capaz de gerir todo o processo de eleição. Esta plataforma abrange três tipos de papéis de utilizador, nomeadamente: o administrador (responsável pela gestão da eleição), a comissão eleitoral (responsável por gerir o processo de eleição) e o eleitor (participante ativo no processo de eleição).

Foi criada uma interface gráfica que tem em consideração as melhores práticas e regras de usabilidade, tornando todo o processo eleitoral mais simples, eficaz e eficiente.

Conforme referido o âmbito deste trabalho teve como principal foco a segurança do voto eletrónico, devido ao facto de esta ser uma das questões chave em este tipo de sistema. Para tal, foram consideradas todas as propriedades de segurança de forma a garantir que a solução desenvolvida respondesse aos objetivos inicialmente estabelecidos. Pode concluir-se que todos os objetivos foram alcançados com sucesso e que a solução dá resposta aos seguintes critérios de segurança: (1) confidencialidade: nenhum tipo de dados pode ser acedido sem autorização adequada; (2) autenticação: Graças a criptografia assimétrica é possível cumprir a propriedade de autenticação e comprovar a origem de uma determinada mensagem dado que ao utilizar criptografia assimétrica é possível cifrar mensagens com a chave privada e decifrar com a chave pública, desta maneira é possível saber a origem da mensagem também chamada assinatura; (3) integridade: para cumprir com a propriedade de integridade, que garante que a informação não seja alterada por terceiros, foram utilizadas funções de hash, criptografia simétrica e assimétrica em conjunto e assinaturas; (4) não-repúdio: para garantir o cumprimento da propriedade não- repúdio recorreu-se à aplicação da técnica de criptografia assimétrica, utilizando chaves privadas e públicas para assegurar a autenticidade de todos os envolvidos no processo de votação eletrónica (indivíduos e componentes). Posto isto, pode concluir-se que o sistema atingiu os objetivos de segurança estabelecidos no início do desenvolvimento da plataforma de voto eletrónico E-VaaS.

Um dos pontos fortes deste sistema diz respeito à possibilidade de criar eleições consoante o tipo de segurança pretendido, sendo possível selecionar eleições sem nenhum tipo de criptografia envolvida e com um simples sistema de base de dados para guardar os votos, ou um sistema seguro com funções criptográficas simétricas, assimétricas e hash envolvidas. Além disso, este sistema é um sistema distribuído sob a forma de serviço, e tira partido das vantagens do modelo de distribuição SaaS.

Todos os componentes da aplicação podem ser alocados em diferentes localizações geográficas garantindo assim que a informação não fica alojada em um só ponto e aumentando desta maneira a segurança da solução.

Como trabalho futuro, sugere-se a execução de um conjunto de testes sobre a plataforma apresentada e a respetiva análise dos resultados, com o objetivo de determinar os pontos de falha e apresentar soluções para os mesmos. Sugere-se também a validação da plataforma através de um caso de estudo real que permita testar a plataforma em um ambiente real.

Referências

[1] Diccionario de la lengua española, *elección*. .

[2] Diccionario de la lengua española, “consenso.”

[3] D. Gritzalis, *Secure Electronic Voting: New trends, new threats, new options*. 2003.

[4] A. Oostveen and P. Van Den Besselaar, “Security as belief: user’s perceptions on the security of electronic voting systems,” *Electron. voting Eur. Technol. law, Polit. Soc.*, pp. 73–82, 2004.

[5] D. H. Melanie Volkamer, “From Legal Principles to an Internet Voting System.”

[6] D. R. Niels Meißner, Volker Hartmann, “Verifiability and Other Technical Requirements for Online Voting Systems.”

[7] M. Josep and R. Vilamala, “Ocho dudas razonables sobre la necesidad del voto electrónico.,” *Rev. D’Internet, Dret i Política.*, vol. 6, pp. 32–44, 2008.

[8] R. A. Costa, “Votação Electrónica,” 2005.

[9] R. Leenes, “The implementation of electronic voting in the UK, by Lawrence Pratchett,” *Inf. Polity Int. J. Gov. Democr. Inf. Age*, vol. 7, p. 167, 2002.

[10] S. (The W. B. Knack and M. (University of M. Kropf, “Voided Ballots in the 1996 Presidential Election : A County-Level Analysis,” *J. Polit.*, vol. 65, pp. 881–897, 2003.

[11] T. R. C. e Pereira, “Tecnologias de segurança no e-vote,” 2006.

[12] Z. Rjaskova, “Electronic Voting Schemes,” *Physics (College. Park. Md).*, vol. 7, p. 240, 2002.

[13] ISO/IEC 27002:2013, “Information technology -- Security techniques -- Code of practice for information security controls.”

[14] M. Jouini, L. B. A. Rabai, and A. Ben Aissa, “Classification of security threats in information systems,” in *Procedia Computer Science*, 2014, vol. 32, pp. 489–496.

[15] G. Whitson, “Computer security: theory, process and management,” *J. Comput. Sci. Coll.*, 2003.

[16] A. D. Rubin, “Security considerations for remote electronic voting,” *Communications of the ACM*, vol. 45. pp. 39–44, 2002.

[17] D. Malkhi, “Electronic Voting Protocols and Schemes,” *Hebr. Univ. Jerusalem, Isr.*, 2002.

[18] M. Kaeo, “Security Tecnhonologies,” *IinformIT*, 1999.

[19] T. Grance, “Guide to Selecting Information Technology Security Products, NIST,” *Natl. Inst. Stand. Technol.*, 2003.

[20] R. Richardson, “CSI computer crime and security survey,” *Comput. Secur. Inst.*, vol. 1, pp. 1–30, 2008.

[21] J. Christopher D. Coley, Ralph E. Wesinger, “Firewall system for protecting network elements connected to a public network.”

[22] W. P. S. Danny M. Nessett, “Multilayer firewall system.”

[23] E. T. Nakamura and P. L. de Geus, “Segurança de Redes em Ambientes Cooperativos.”

[24] P. G. Neumann, “Security Criteria for Electronic Voting,” *Computer Science Laboratory*, 1993. [Online]. Available: http://www.csl.sri.com/users/neumann/ncs93.html.

[25] R. R. Oliveira, “Criptografia simétrica e assimétrica : os principais algoritmos de cifragem,” *Online Magazine Digital Security - 5th edition and 6th edition*, pp. 1–9, 2012.

[26] M. R. Thompson, A. Essiari, and S. Mudumbai, “Certificate-based authorization policy in a PKI environment,” *ACM Transactions on Information and System Security*, vol. 6. pp. 566–588, 2003.

[27] P. S. Magalhães and H. D. Dos Santos, “Biometria e autenticação,” in *Actas da 4a CONFERÊNCIA DA ASSOCIAÇÃO PORTUGUESA DE SISTEMAS DE INFORMAÇÃO CAPSI 2003*, 2003, vol. 2003, pp. 2–9354.

[28] Á. Hernández Bravo, “El SaaS y el Cloud-Computing: una opción innovadora para tiempo de crisis.”

[29] A. Dubey and D. Wagle, “Delivering software as a service,” *McKinsey Q.*, vol. 6, pp. 1–12, 2007.

[30] M. Turner, D. Budgen, and P. Brereton, “Turning software into a service,” *Computer (Long. Beach. Calif).*, vol. 36, no. 10, pp. 38–44, Oct. 2003.

[31] F. Barrientos del Monte, “Dimensiones discursivas en torno al voto electrónico,” *Revista de ciencia política (Santiago)*, vol. 27. 2007.

[32] A. D. S. Mesa, “Electronic Vote - Software as a Service approach,” 2013.

[33] A. Morgado, Isabel Salema. Rosas, *Cidadania Digital*. 2010.

[34] B. De Vuyst and A. Fairchild, “Experimenting with electronic voting registration: the case of Belgium,” *Electron. J. e-Government*, vol. 3, pp. 87–90, 2005.

[35] Ü. Madise and T. Martens, “E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world,” *First Conf. Electron. voting*, pp. 15–26, 2006.

[36] P. Alejandro, “Consideraciones, aportes y experiencias para el Voto electrónico en Argentina,” 2005.

[37] O. Cetinkaya and D. Cetinkaya, “Verification and validation issues in electronic voting,” *Electron. J. e-government*, vol. 5, pp. 117–126, 2007.

[38] J. Rial, “Posibilidades y límites del voto electrónico,” 2004.

[39] S. Y. Yan, *Computational Number Theory and Modern Cryptography.* 2013.

[40] G. G. Paredes, “INTRODUCCIÓN A LA CRIPTOGRAFÍA,” *Rev. Digit. Univ.*, vol. 7, pp. 2–17, 2006.

[41] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, vol. 106. 1997, p. 780.

[42] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*. 1996, pp. 623–631.