



Universidade do Minho
Escola de Engenharia

Cristiana Rosa Loureiro Teixeira

**Especificação da adaptação da eVotUM ao
suporte expedito de votações, presenciais
ou à distância, de pequenos grupos**

Dissertação de Mestrado

Mestrado Integrado em Engenharia e Gestão de
Sistemas de Informação

Trabalho efetuado sob a orientação do

Professor Doutor Luís Alfredo Martins do Amaral

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição

CC BY

<https://creativecommons.org/licenses/by/4.0/>

AGRADECIMENTOS

Durante todo o processo de realização desta dissertação contei com o apoio, direto e indireto, de múltiplas pessoas, às quais estou profundamente grata. Quero, portanto, deixar aqui expressos os meus agradecimentos:

Ao meu orientador, Professor Luís Amaral, pela orientação prestada e pelo incentivo, disponibilidade e apoio que sempre me demonstrou.

À Eurotux, pelo conhecimento e auxílio continuamente facultados.

À família, pelo encorajamento oportuno e por estar sempre presente.

Às amigas, com quem ultrapassei inúmeros desafios ao longo de todo este percurso.

E a todos aqueles que, de algum modo, acompanharam e apoiaram a evolução deste trabalho.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

Especificação da adaptação da eVotUM ao suporte expedito de votações, presenciais ou à distância, de pequenos grupos.

A realização de votações pela Internet é uma necessidade crescente da sociedade atual, que se revigoreu, sobretudo, na mais recente pandemia mundial e nos anos que dela decorrem. Propõe-se analisar a eVotUM, vigente plataforma de voto eletrónico da Universidade do Minho, utilizada em eleições de vários órgãos da academia, e aferir a sua adaptabilidade para um novo contexto de votação mais expedito, através de reuniões presenciais ou à distância, com um número reduzido de intervenientes. Por meio de uma identificação e caracterização da atual arquitetura da plataforma, bem como dos seus componentes principais, procede-se ao levantamento dos requisitos funcionais e não funcionais indispensáveis à conceção da nova plataforma, eVotUM *light*, adaptada ao novo contexto de votação em que se insere. O estudo possibilita a especificação de tal sistema de votação, resultante do reaproveitamento de determinados componentes originais e da evolução ou simplificação de alguns outros.

Palavras-Chave: eVotUM, eVotUM *light*, Plataforma de voto eletrónico, Votação, Sistemas de votação eletrónica.

ABSTRACT

Specification of eVotUM's adaptation to support in-person or remote voting of small groups.

Voting through the Internet is a growing need in today's world, which has been invigorated, above all, in the most recent global pandemic and in the years that followed it. It is proposed to analyze eVotUM, the current electronic voting platform of the University of Minho, used in elections of several academic bodies, and to assess its adaptability to a new, more expeditious voting context, through face-to-face or remote meetings, with a reduced number of participants. Through an identification and characterization of the current platform architecture, as well as its main components, the functional and non-functional requirements essential to the conception of the new platform, eVotUM *light*, adapted to the new voting context in which it operates, are surveyed. The study allows for the specification of such a voting system, resulting from the reuse of certain original components and the evolution or simplification of some others.

Keywords: eVotUM, eVotUM *light*, Electronic voting platform, Votation, Electronic voting systems.

ÍNDICE

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS	ii
AGRADECIMENTOS.....	iii
DECLARAÇÃO DE INTEGRIDADE	iv
RESUMO	v
ABSTRACT	vi
1. INTRODUÇÃO	1
1.1 Enquadramento.....	1
1.2 Motivação e Importância da Investigação	3
1.3 Finalidade e Objetivos	4
1.4 Caraterização da Abordagem de Investigação.....	5
1.5 Estrutura da Dissertação	6
2. FUNDAMENTOS.....	8
2.1 Introdução aos Sistemas de Votação	8
2.2 Votação Eletrónica pela Internet	10
2.2.1 Riscos Associados	11
2.2.2 Modelos e Protocolos Criptográficos Existentes	14
2.2.3 Sistemas Vigentes.....	19
2.2.3.1 Helios.....	20
2.2.3.2 REVS [Robust Electronic Voting System].....	21
2.2.3.3 Sensus.....	24
3. CARATERIZAÇÃO DA PLATAFORMA EVOTUM.....	26
3.1 Visão Integral da Plataforma	26
3.1.1 Intervenientes	27
3.1.2 Processo de Votação pelo Eleitor.....	28

3.1.3	Gestão do Processo Eleitoral pela Comissão Eleitoral	29
3.1.4	Criação do Processo Eleitoral pelo Responsável Institucional	30
3.1.5	Gestão do Sistema pelo Administrador Técnico	32
3.1.6	Comunicação na Plataforma	32
3.1.7	Tipos de Eleição Autorizados	34
3.1.8	Arquivo do Processo Eleitoral	35
3.1.9	Diagramas de Estados	35
3.1.9.1	Processo Eleitoral	35
3.1.9.2	Eleição	36
3.2	Comportamento Funcional da Plataforma	37
3.2.1	Requisitos Funcionais	38
3.2.2	Requisitos Não Funcionais	42
3.3	Infraestrutura Tecnológica da Plataforma	43
3.3.1	Componentes de Software	43
3.3.2	Arquitetura da Infraestrutura	46
3.3.3	Fluxo de Comunicação	50
4.	ESPECIFICAÇÃO DA PLATAFORMA FUTURA – eVotUM light	57
4.1	Visão Integral da Plataforma	57
4.1.1	Intervenientes	58
4.1.2	Processo de Votação pelo Votante	59
4.1.3	Processos de Criação e Gestão da Votação pelo Secretário	61
4.1.4	Tipos de Votação Autorizados	63
4.1.5	Arquivo da Votação	63
4.2	Comportamento Funcional da Plataforma	63
4.2.1	Requisitos a Implementar	64
4.2.1.1	Requisitos Funcionais	65

4.2.1.2	Requisitos Não Funcionais	68
4.2.2	Casos de Uso	69
4.2.2.1	Autenticação do Utilizador na eVotUM <i>light</i>	70
4.2.2.2	Interação do Votante com a eVotUM <i>light</i>	71
4.2.2.3	Interação do Secretário com a eVotUM <i>light</i>	72
4.3	Comportamento Dinâmico da Plataforma	72
4.3.1	Manual de Utilização do Votante	73
4.3.1.1	Autenticação	73
4.3.1.2	Votação	74
4.3.1.3	Consultas	77
4.3.2	Manual de Utilização do Secretário	78
4.3.2.1	Criação da Votação	78
4.3.2.2	Gestão da Votação	81
4.4	Infraestrutura Tecnológica da Plataforma	85
4.4.1	Componentes de Software	85
4.4.2	Arquitetura da Infraestrutura	87
4.4.3	Fluxo de Comunicação	88
5.	CONCLUSÃO	90
	REFERÊNCIAS BIBLIOGRÁFICAS	92
	ANEXOS	94

ÍNDICE DE FIGURAS

Figura 1 - Arquitetura original REVS (Zúquete et. al., 2008)	23
Figura 2 - Diagrama de Estados referente ao Processo Eleitoral	36
Figura 3 - Diagrama de Estados referente à Eleição	37
Figura 4 - Diagrama Lógico da Arquitetura da eVotUM (Arquitetura da Infraestrutura, CCG, Eurotux & Devise Futures)	48
Figura 5 - Diagrama referente à redundância do sistema eVotUM (Arquitetura da Infraestrutura, CCG, Eurotux & Devise Futures)	49
Figura 6 - Fluxo de Comunicação detalhado referente a uma Eleição na eVotUM (Fluxos de Comunicação, CCG, Eurotux & Devise Futures)	51
Figura 7 - Diagrama de Caso de Uso referente ao Processo de Autenticação do Utilizador na eVotUM light	70
Figura 8 - Diagrama de Caso de Uso referente à interação do Votante com o Sistema de Votação da eVotUM light	71
Figura 9 - Diagrama de Caso de Uso referente à interação do Votante com o Sistema de Consultas da eVotUM light.....	71
Figura 10 - Diagrama de Caso de Uso referente à interação do Secretário da Reunião com a eVotUM light	72
Figura 11 - Formulário de Autenticação na eVotUM light	73
Figura 12 - Listagem de Votações do Votante na eVotUM light.....	74
Figura 13 - Passo 1: Selecionar Votação.....	74
Figura 14 - Passo 2: Selecionar Candidato	75
Figura 15 - Passo 3: Confirmar Seleção de Candidato	75
Figura 16 - Passo 4: Selecionar Mecanismo de Envio e Submeter Código PIN de Votação.....	76
Figura 17 - Passo 5: Finalizar Votação e Recolher Referência de Voto.....	77
Figura 18 - Consultar Referência de Votação.....	77
Figura 19 - Passo 1: Inserir Dados Gerais da Votação	78
Figura 20 - Passo 2: Definir Configurações da Votação	79
Figura 21 - Passo 3: Inserir Lista de Votantes na Votação	80
Figura 22 - Passo 4: Inserir Candidatos à Votação	80
Figura 23 - Passo 5: Configurar Boletim de Voto da Votação	81

Figura 24 - Painel de Votações	82
Figura 25 - Passo 1: Autorizar Início da Votação	82
Figura 26 - Passo 2: Aceder à Urna Eletrónica	83
Figura 27 - Passo 2: Visualizar Número Total de Boletins em Urna	83
Figura 28 - Passo 3: Autorizar Fecho da Votação	83
Figura 29 - Passo 4: Autorizar Escrutínio dos Votos	84
Figura 30 - Passo 4: Apresentação de Resultados no Painel do Secretário	84
Figura 31 - Passo 5: Autorizar Publicação de Resultados	84
Figura 32 - Fluxo de Comunicação detalhado referente a uma Votação na eVotUM light (Fluxos de Comunicação, CCG, Eurotux & Devise Futures)	89

ÍNDICE DE TABELAS

Tabela 1 - Requisitos dos Sistemas de Votação Eletrónica (Nogueira, J. A. P. M., 2011)	9
Tabela 2 - Intervenientes na Plataforma de Votação Eletrónica eVotUM	27
Tabela 3 – Passos referentes ao Processo de Votação pelo Eleitor	28
Tabela 4 – Passos referentes ao Processo de Gestão do Processo Eleitoral pela Comissão Eleitoral	29
Tabela 5 - Configurações disponíveis para uma Eleição na Plataforma eVotUM	34
Tabela 6 - Requisitos Funcionais implementados no âmbito do projeto da eVotUM	38
Tabela 7 - Requisitos Não Funcionais implementados no âmbito do projeto da eVotUM	42
Tabela 8 - Descrição detalhada dos Componentes de Software do Sistema eVotUM	44
Tabela 9 - Etapas referentes ao Processo de Votação numa Eleição na eVotUM	51
Tabela 10 - Intervenientes na Plataforma eVotUM light	58
Tabela 11 - Passos referentes ao Processo de Votação pelo Votante	60
Tabela 12 - Passos referentes ao Processo de Gestão da Votação	62
Tabela 13 - Requisitos Funcionais da eVotUM Light	65
Tabela 14 - Descrição detalhada dos componentes de Software da eVotUM light	86

LISTAS DE ABREVIATURAS E SIGLAS

CCG – Centro de Computação Gráfica

DDoS – Distributed Denial of Service

DOS – Denial of Service

DTSI – Direção de Tecnologias e Sistemas de Informação

E-Voting – Electronic Voting

eVotUM – Electronic Voting Platform of University of Minho

eVotUM light – Light Version of the Electronic Voting Platform of University of Minho

GPG - GNU Privacy Guard

HMAC - Hash-Based Message Authentication Code

MitM – Man-in-the-Middle

RSA – Rivest-Shamir-Adleman

WORM - Write Once Read Many

CAPÍTULO 1

INTRODUÇÃO

No presente capítulo é exposta a introdução ao tema da dissertação, pelo que serão apresentados o enquadramento, a motivação e importância da investigação, a finalidade e objetivos inerentes, a caracterização da abordagem de investigação e, por fim, a estrutura da dissertação. Este primeiro capítulo permite, portanto, situar o projeto no contexto do tema elegido, possibilitando a agregação de conhecimentos e compreensão do que irá ser aplicado ao longo da investigação.

1.1 Enquadramento

Sistemas de votação eletrónica têm vindo a incitar um crescente interesse no mundo atual, como meio de substituição do método tradicional. Rapidez no apuramento de resultados, reduzidos custos de implementação, possibilidade de o eleitor atestar se o seu voto é corretamente contabilizado e gestão centralizada de todo o processo associado à eleição são algumas das vantagens que podem ser promovidas na adoção destes sistemas. O facto de um sistema de votação eletrónico ser suportado pela Internet proporciona ainda comodidade para o eleitor, sendo que elimina a necessidade de este se deslocar a um local físico, potencialmente promovendo uma redução na abstenção. Contudo, a Internet não é um meio controlado e, por isso, é fundamental que um sistema de votação desta natureza possua meios de segurança que permitam preservar a integridade do voto e a privacidade do eleitor e, ainda, mecanismos de tolerância a falhas.

A Universidade do Minho desenvolveu, no início dos anos 2000, a plataforma de voto eletrónico eVote, concebida no sentido de promover as eleições dos órgãos da Universidade. O funcionamento da plataforma foi estabelecido por cerca de dez anos, com a consequente desatualização da infraestrutura tecnológica que a suportava, o que começava a acarretar custos adicionais de manutenção e condicionava potenciais evoluções e integrações.

No sentido de progredir e ultrapassar os obstáculos que dessa desatualização emergiam, a Universidade do Minho, em parceria com o Grupo Eurotux, com a Devise Futures e com o CCG (Centro de Computação Gráfica), promoveu, no ano de 2017, a implementação da plataforma de votação eletrónica eVotUM, solução essa que veio possibilitar a realização de eleições tradicionais via Web, mediante a utilização de um browser, instalado num computador ou smartphone. A reunião de arranque do projeto decorreu a 01/04/2016.

O Grupo Eurotux, responsável pela implementação da plataforma, é constituído por especialistas em planeamento, integração e implementação de sistemas informáticos. O grupo oferece soluções de tecnologias de informação construídas à medida das necessidades dos clientes e os seus projetos privilegiam critérios de segurança, tratamento adequado de situações de contingência e alta disponibilidade dos sistemas. As tecnologias utilizadas vão desde produtos open source, inerentemente transparentes, confiáveis e de elevado desempenho, a produtos proprietários de diversos fabricantes.

O sistema eVotUM permite, atualmente, diversas eleições simultâneas, com anonimato, segurança, transparência e singularidade, e está disponível para ser utilizado por qualquer unidade da universidade nos processos eleitorais, sejam estes atos eleitorais ou referendos de opinião. O sistema de votação eletrónica veio, assim, conferir uma maior celeridade e eficiência às operações de votação e apuramento, preservando todas as garantias de segurança e credibilidade inerentes a todo o processo.

No entanto, atualmente, a utilização deste sistema para contextos de votação em tempo real durante reuniões, sejam estas presenciais ou à distância, constituídas por um número de intervenientes reduzido, é muito pouco ajustada. A plataforma foi projetada para suportar votações que obedecem, rigorosamente, a um conjunto de fases integrantes de um processo eleitoral, fases essas que são, neste novo contexto, desnecessárias.

1.2 Motivação e Importância da Investigação

Na atualidade, a utilização de sistemas de votação eletrónica deixou de ser uma mera idealização e transformou-se numa necessidade incontestável e de aceitação e aderência crescentes. A pandemia global da COVID-19, que surgiu em 2020, suscitou uma mudança profunda no dia-a-dia das pessoas, organizações e instituições, alterando, fundamentalmente, o modo de viver e de trabalhar que se estabelecera até então. Dadas as adversidades, tais organizações e instituições viram-se forçadas a alterar os seus paradigmas de trabalho e a instituir mudanças a grande velocidade, através de novas práticas e modelos de organização.

Contudo, apesar de as metodologias de trabalho terem vindo a ser adaptadas para fazer face à nova realidade, estas detêm ainda um vasto potencial de evolução. A necessidade de serem promovidas votações, em tempo real, em contexto de reuniões remotas, fossem estas organizacionais ou institucionais, surgiu, e a realidade que se presenteava era muito pouco ajustada. A plataforma de votação eletrónica eVotUM, em particular, foi projetada para suportar votações que obedecem, rigorosamente, a um amplo conjunto de fases integrantes de um processo eleitoral aceite como convencional, fases essas que são, num contexto de votação mais simplificado, desnecessárias.

Posto isto, identificou-se a oportunidade de reimplementar a plataforma existente de tal modo que se ajuste à utilização no novo contexto de votação, reaproveitando, para tal, as componentes desenvolvidas até à data, simplificando as suas interfaces e ajustando todo o processo eleitoral. A plataforma que advirá dessa adaptação é, portanto, a eVotUM *light*. O aproveitamento desta oportunidade é o móbil da dissertação.

1.3 Finalidade e Objetivos

Como já referido, a eVotUM oferece diversas soluções de voto, no entanto, ainda não tem uma solução adaptada a um contexto de votação em reuniões, quer estas sejam em formato online ou até mesmo presencial, para oferecer aos seus utilizadores. Tal como foi evidenciado na introdução deste capítulo, as votações pela Internet estão a aumentar, assim como a procura destes serviços por parte de governos e organizações. Este protejo de dissertação foi realizado com o intuito de especificar uma nova solução, eVotUM *light*, dedicada a votações num novo contexto, preservando características como a rapidez, a fácil utilização e a alta segurança, que já detém.

Nesse sentido, no decorrer desta dissertação estão previstos, fundamentalmente, os seguintes objetivos e correspondentes resultados esperados:

- Procura de clarificação sobre quais as funcionalidades e arquiteturas projetadas para as plataformas de votação eletrónica atualmente dominantes, resultando numa revisão de literatura atualizada sobre as arquiteturas existentes e, ainda, sobre as características naturalmente intrínsecas a sistemas desta natureza;
- Identificação e caracterização da arquitetura atualmente implementada na eVotUM, resultando na descrição dos principais componentes da atual plataforma de votação;
- Levantamento dos requisitos funcionais e não funcionais necessários ao suporte de votações em reuniões, em formato online ou presenciais, resultando na caracterização dos requisitos indispensáveis à futura plataforma eletrónica, cingida ao novo contexto de votação;
- Especificação de uma nova plataforma que cumpra os requisitos funcionais e não funcionais previamente especificados, resultante de uma evolução e simplificação das componentes já existentes na eVotUM. O resultado associado é, portanto, a especificação funcional e não funcional da eVotUM *light* para contextos de votação, em tempo real, durante reuniões.

1.4 Caraterização da Abordagem de Investigação

Numa primeira instância, concernente à pesquisa inicial da dissertação, é efetuada uma revisão de literatura, isto é, um levantamento bibliográfico referente ao estado da arte no âmbito dos sistemas de votação eletrónica através da Internet, recorrendo, para tal, aos diversos repositórios de referência existentes, particularmente, o Google Scholar.

Numa segunda instância, é satisfeita uma análise detalhada da arquitetura da eVotUM, para que, posteriormente, pudesse ser efetuada a prescrição de uma nova solução em função do problema a resolver, isto é, uma variante da plataforma atual capaz de suportar, de forma expedita, votações presenciais ou à distancia por parte de pequenos grupos.

A investigação visa, portanto, gerar conhecimentos, para que, num futuro próximo, possa ocorrer a sua aplicação prática, com vista à solução de um problema específico. Nesse sentido, a pesquisa efetuada é do tipo aplicada e envolve interesses locais. Tal como previamente referido, os resultados produzidos pela investigação procuram satisfazer a necessidade atual de criação de uma nova plataforma de votação eletrónica através da Internet, adaptada para contextos de votação de pequena escala em reuniões e, para tal, é imprescindível efetuar a sua especificação, objetivo central da dissertação.

1.5 Estrutura da Dissertação

A presente dissertação encontra-se organizada em cinco capítulos, nomeadamente:

1. Introdução

No primeiro capítulo é exposta a introdução ao tema da dissertação, pelo que serão apresentados o enquadramento, a motivação e importância da investigação, a finalidade e objetivos inerentes, a caracterização da abordagem de investigação e, por fim, a estrutura da dissertação. Este permite situar o projeto no contexto do tema elegido, possibilitando a agregação de conhecimentos e compreensão do que irá ser aplicado ao longo da investigação.

2. Fundamentos

Ao longo do segundo capítulo são retratados diversos aspetos concernentes a sistemas de votação eletrónica. É, portanto, contextualizada a relevância da Internet no exercício da democracia e, posteriormente, expostos alguns dos riscos associados ao voto eletrónico pela Internet, enunciados os modelos de votação eletrónica existentes, bem como os sistemas de voto eletrónico vigentes na atualidade.

3. Caracterização da Plataforma eVotUM

No terceiro capítulo é, numa primeira instância, apresentada uma visão integral da atual plataforma eVotUM e, posteriormente, descrito o comportamento funcional e arquitetura tecnológica que a caracterizam, o que servirá de referência para a especificação da eVotUM *light*.

4. Especificação da Plataforma Futura

No decorrer do quarto capítulo é efetuada a especificação detalhada da futura plataforma de votação eletrónica, eVotUM *light*, adaptada, portanto, ao novo contexto de votação, de pequenos grupos, em reuniões presenciais, à distância e, sobretudo, híbridas.

Especificá-la passa, então, por descrever um variado conjunto de atributos que lhe são caraterísticos e, nesse sentido, o capítulo começa por introduzir uma visão integral da plataforma e, posteriormente, subdivide-se em três lógicas distintas, designadamente, o comportamento funcional, o comportamento dinâmico e a arquitetura tecnológica inerentes à plataforma.

5. Conclusão

Por fim, no último capítulo, são retiradas as principais conclusões associadas ao trabalho desenvolvido, anunciadas as dificuldades sentidas aquando da sua concretização e traçadas perspectivas futuras tendo por base a solução proposta.

CAPÍTULO 2

FUNDAMENTOS

Ao longo do presente capítulo são retratados diversos aspetos concernentes a sistemas de votação eletrónica através da Internet. Inicialmente, é efetuada uma introdução aos sistemas de votação eletrónica, nomeadamente no que diz respeito aos seus requisitos, às suas fases de votação e às entidades envolvidas no processo. De seguida, é contextualizada a relevância da Internet no exercício da democracia e a vigorosa tendência, na atualidade, de desenvolver sistemas de votação desta natureza. Posteriormente, são expostas diversas problemáticas referentes ao novo paradigma de votação, ou seja, alguns dos riscos associados ao voto eletrónico pela Internet. Posto isto, são enunciadas as premissas criptográficas de referência, os modelos existentes, bem como os sistemas de voto eletrónico vigentes na atualidade.

2.1 Introdução aos Sistemas de Votação

São múltiplas as vertentes inerentes aos sistemas de votação que requerem uma análise cuidada por parte dos investigadores, desde requisitos, arquiteturas e mecanismos de implementação, até questões legais e éticas suscitadas pela utilização desses mesmos sistemas. Um sistema de votação eletrónica deve, idealmente, transpor as características e funcionalidades que o sistema de votação tradicional oferece e deve, portanto, ser desenhado e arquitetado com foco na segurança. Este tem de cumprir e garantir diversos requisitos gerais, comuns a todas as eleições, recorrendo, para tal, a mecanismo de segurança, sendo que se trata de um sistema crítico. No entanto, apresenta necessidades e comportamentos distintos daqueles encontrados nos sistemas tradicionais.

Na tabela 1 são enumerados e descritos os principais requisitos, apontados pela literatura, para sistemas desta natureza.

Tabela 1 - Requisitos dos Sistemas de Votação Eletrônica (Nogueira, J. A. P. M., 2011)

Requisito	Descrição
Autenticidade	Apenas eleitores autorizados devem poder votar;
Singularidade	Cada eleitor deve poder votar uma única vez por eleição;
Anonimato	A associação entre o voto e o respetivo eleitor deve ser inexequível;
Integridade	O voto não deve poder ser alterado, falsificado ou eliminado;
Incoercibilidade	Nenhum eleitor deve ser capaz de provar o voto que emitiu;
Verificabilidade	Qualquer pessoa deve ser capaz de verificar que todos os votos foram corretamente contabilizados;
Auditabilidade e Certificabilidade	O sistema deve poder ser testado, auditado e certificado por agentes independentes;
Mobilidade	O sistema não deve restringir o local de votação;
Transparência	O sistema deve ser claro e transmitir rigor, precisão e segurança ao eleitor;
Disponibilidade	O sistema deve estar sempre disponível durante o período eleitoral;
Acessibilidade e Conveniência	O sistema deve ser acessível a pessoas com necessidades especiais, sem exigir equipamentos ou competências específicas;
Detetabilidade e Recuperabilidade	O sistema deve poder detetar erros, falhas e ataques, bem como recuperar informação até ao ponto de falha.

As fases de uma votação, suportada por um sistema de votação eletrónica, podem ser equiparadas às de uma votação tradicional. Existe, pois, uma grande variedade de processos de votação, processos esses que dizem respeito à realização de uma eleição. De um modo genérico, cada eleição, tradicional ou eletrónica, envolve cinco etapas (Burmester e Magkos, 2003; Wang K., 2017), nomeadamente:

1. **Registo:** Esta primeira fase contempla a compilação dos cadernos eleitorais com todos os eleitores elegíveis;
2. **Validação:** Esta etapa envolve a verificação das credenciais dos eleitores que tentam votar e só permite que eleitores registados, que ainda não votaram, prossigam;

3. **Reunião:** Esta terceira fase pressupõe a reunião dos votos de todos os eleitores;
4. **Verificação:** Na quarta etapa é verificada a validade dos votos, sendo que apenas os votos válidos passam à fase de contagem;
5. **Contagem:** É, portanto, na fase da contagem que se procede ao apuramento dos votos, sendo, por fim, publicado o resultado.

Importante será também referir que, em sistemas de votação que apresentem algum tipo de anonimização, as entidades envolvidas no processo de votação eletrónica são, tipicamente, as seguintes:

- **Votante;**
- **Emissor** de votos;
- **Recetor** de votos;
- **Anonimizador** de votos;
- **Contador** de votos.

2.2 Votação Eletrónica pela Internet

Parcela eminente da vida contemporânea ocorre no meio digital, através do qual as pessoas convivem, interagem e estimulam acontecimentos, usufruindo do ambiente virtual tanto para realização pessoal como social. É, hoje, improrrogável refletir sobre o exercício da democracia no novo contexto de votação na Internet, sendo que este vai adquirindo novos formatos ao longo do tempo, mediante novos panoramas.

O voto eletrónico assenta na utilização de recursos informáticos aquando do processo de votação, sendo que nos casos em que se procede à votação de forma remota é atribuída a designação de votação pela Internet. Sistemas de votação eletrónica pela internet facultam características melhoradas, comparativamente com sistemas de votação tradicionais, tais como precisão, conveniência, flexibilidade e mobilidade. O sistema de votação pela Internet é um sistema através do qual qualquer eleitor pode empregar o seu direito de voto a partir de qualquer parte do mundo, de forma segura, o que pode, em última análise, intensificar a

responsabilização. Os efeitos positivos potencialmente promovidos pela votação através da Internet são difíceis de quantificar, nomeadamente no que diz respeito à qualidade dos votos, sendo que por esta via não ocorrem votos nulos, nem erros na contagem, o que acontece, por vezes, pela via tradicional. A votação online é simples, atrativa e fácil de usar, além de reduzir esforços manuais e promover uma maior agilidade de análise da informação.

2.2.1 Riscos Associados

Apesar de todas as características proficientes referidas, subsistem alguns inconvenientes na utilização destes sistemas, nomeadamente a possibilidade de ocorrerem falhas no software, existir um acesso inseguro à Internet ou, até mesmo, a impertinência de o eleitor não estar familiarizado com o uso das tecnologias. O voto eletrónico, cumprido através da Internet, é utilizado, não obstante, na maioria dos países desenvolvidos em eleições não vinculativas, como a eleição de muitas comissões representativas, conselhos de administração, conselhos científicos, entre muitos outros, e podem, efetivamente, envolver um grande número de eleitores. Existe, portanto, uma necessidade urgente de oferecer sistemas de votação eletrónica seguros, fiáveis e de confiança (Zúquete et. al., 2008).

Sistemas de votação são, por natureza, extremamente sensíveis, e têm uma maior predisposição para sofrer ataques provenientes do exterior, isto é, representam um alvo de eleição por parte de entidades que pretendem influenciar, de forma ilícita, os resultados das eleições. O surgimento da votação eletrónica e, em particular, da votação pela Internet, veio potenciar a exploração de vulnerabilidades no software, ambiente de execução ou infraestrutura dos sistemas de votação e o esforço no sentido de ofender a integridade e privacidade da votação (Brioso, 2012).

Não existem, portanto, sistemas infalíveis e as abordagens ao desenvolvimento de sistemas de votação eletrónica devem considerar, desde a sua génese, a existência de riscos e a consequente necessidade de os gerir, seja através da prevenção, mitigação ou contenção das potenciais consequências. Uma visão sistémica é, então, imprescindível no entendimento de sistemas de votação eletrónica, isto porque não é possível dissociar o sistema técnico, infraestrutura de suporte, dos seus eleitores e operadores durante o processo eleitoral, e de

outros intervenientes, como auditores e técnicos, bem como da sociedade em geral, que impõe e garante a democracia. A falha de um destes componentes leva à falha de todo o sistema de votação (Zúquete e Almeida, 2008).

A votação, associada a estes sistemas, está, por conseguinte, sujeita a distúrbios que se evidenciam, essencialmente, nos três seguintes componentes:

- **Cliente:** através da manipulação do voto do eleitor, seja pelo ataque de um vírus, que adultera o conteúdo do voto, ou pelo ataque de uma entidade, responsável pela exploração remota das deficiências inerentes ao sistema de votação ou browser do eleitor;
- **Comunicação:** através da falsificação do website que promove a votação, por exemplo, o que poderá iludir o eleitor e resultar, consequentemente, no adultério do voto por parte da entidade atacante;
- **Servidor:** através de ataques semelhantes aos efetuados ao cliente de voto e, ainda, a eventualidade de ocorrerem ataques de DOS.

Os ataques aos componentes previamente enunciados podem, então, subdividir-se em três categorias distintas:

- Ataques ao **software do sistema de votação**, através de:
 - a. *Software Bugs*;
 - b. *Backdoor Malware*.
- 2. Ataques ao **ambiente de execução do sistema de votação**, através de:
 - a. *Trojan Horse Hacking*;
 - b. *Browser Rootkit Hacking*.
- 3. Ataques à **infraestrutura do sistema de votação**, através de:
 - a. DDoS;
 - b. *Phishing*;
 - c. *Spoofing*;
 - d. MitM.

Na primeira categoria, relativa ao software do sistema de votação, podem ocorrer ataques através de, por exemplo, *Software Bugs* ou, ainda, *Backdoor Malware*. O primeiro tipo de ataque consiste na utilização de *bugs*, o que poderá garantir, numa primeira instância, acesso ao software do sistema por parte de entidades não autorizadas e, concludentemente, a usurpação de informações privilegiadas ou, ainda, a instalação de *Backdoor Malware*, podendo ocorrer nas fases de desenvolvimento de software, preparação ou operação do sistema. O segundo tipo de ataque pode surgir, portanto, como consequência do primeiro e corresponde, essencialmente, a um qualquer método através do qual um dado utilizador consegue contornar as medidas de segurança existentes e obter acesso de alto nível ao software do sistema de votação. *Malware* é um termo genérico que aqui descreve qualquer software prejudicial ao sistema de votação.

Na segunda categoria, relativa ao ambiente de execução do sistema de votação, podem ocorrer ataques através de, por exemplo, *Trojan Horse Hacking* ou *Browser Rootkit Hacking*. O primeiro corresponde, fundamentalmente, a um tipo de *Malware* que, uma vez dentro do sistema, é capaz de extorquir, modificar ou até mesmo eliminar dados pessoais dos eleitores, bem como informação relativa à opção de voto, sem o seu conhecimento ou consentimento. O segundo corresponde a um *Malware* que se apodera do browser do eleitor de modo a espiar a sua atividade, durante o ato de voto, e adquirir dados potencialmente sensíveis. Na eventualidade de ataques desta natureza ocorrerem, requisitos do sistema de votação tais como anonimato e integridade, propriedades inerentes à democracia, serão comprometidos.

Por fim, na terceira categoria, relativa à infraestrutura do sistema de votação, podem ocorrer ataques de naturezas distintas, nomeadamente, DDoS, *Phishing*, *Spoofing* ou, ainda, MitM. O primeiro tipo de vulnerabilidade, DDoS, pode ocorrer nos servidores e clientes do sistema ou na infraestrutura de rede. Este trata-se de um ataque de rede que força a exaustão dos recursos do sistema através de solicitações sucessivas, isto é, inúmeros pedidos de comunicação, com a intenção de o sobrecarregar. No caso dos sistemas de votação que utilizam a infraestrutura Internet, os servidores de acesso ao sistema estão particularmente sujeitos a este tipo de vulnerabilidade. *Phishing* e *Spoofing*, por outro lado, representam dois tipos de ataque cujos atores se patenteiam como entidades de confiança, de modo a obterem acesso ao sistema de votação e iludirem potenciais vítimas na partilha de informação sensível, informação vital do sistema de votação. O último tipo de ataque, MitM, acontece quando o

ator da ameaça consegue intercetar ou alterar o tráfego entre duas entidades, sem que nenhuma se aperceba. Tais entidades podem, neste contexto, representar, por exemplo, a comunicação estabelecida entre o eleitor e o sistema de votação, através da internet.

Estas incursões podem ser praticadas por diversas entidades, com objetivos, incentivos, recursos e conhecimentos tecnológicos distintos, como, por exemplo, organizações políticas, grupos terroristas, Estados ou, ainda, entidades criminosas singulares, designadamente, *crackers*.

Os protocolos criptográficos existentes, na sua generalidade, facilitam a prevenção destes ataques do lado do servidor, garantido o seu correto funcionamento. No entanto, num sistema de votação eletrónica pela Internet, onde o cliente de voto não é controlado, nem é exequível a garantia de não convergência de vulnerabilidades, poucos protocolos conseguem assegurar o correto funcionamento do sistema do lado do cliente e, consequentemente, do sistema de votação como um todo (Brioso, 2012).

2.2.2 Modelos e Protocolos Criptográficos Existentes

Sistemas de votação eletrónica através da Internet devem ser concebidos tendo por base protocolos complexos, com o objetivo de garantir a segurança como propriedade intrínseca ao sistema. A conceção de protocolos seguros de votação eletrónica envolve, geralmente, a aplicação de primitivas criptográficas robustas, designadamente, a cifra simétrica e a cifra assimétrica. Criptografia é um termo proveniente da Grécia antiga e baseia-se na investigação de técnicas de codificação de mensagens. Através da aplicação de tais premissas criptográficas somente o detentor de uma chave secreta é capaz de tornar as mensagens recebidas legíveis (de Sousa Grilo, 2015).

A criptografia tem, por natureza, quatro objetivos primários (de Sousa Grilo, 2015):

- **Confidencialidade:** Apenas o detentor da chave secreta deverá ser capaz de ler o conteúdo da mensagem;
- **Integridade:** A mensagem enviada deverá ser corresponder à mensagem recebida, não existindo, portanto, uma adulteração do conteúdo da mesma;

- **Autenticação:** O recetor da mensagem deverá ter conhecimento de quem foi o autor e emissor da mesma;
- **Não-repúdio:** O emissor da mensagem não deverá fruir da capacidade de negar a autoria da mensagem.

Ademais, a criptografia encontra-se dividida em duas categorias distintas (de Sousa Grilo, 2015):

1. **Chave Simétrica:** Algoritmos de chave simétrica utilizam, para cifrar e decifrar mensagens, uma única chave secreta. Este tipo de criptografia é, habitualmente, denominado de convencional;
2. **Chave Assimétrica:** Algoritmos de chave assimétrica utilizam, em contrapartida, duas chaves distintas, uma para cifragem e outra para decifragem de mensagens.

Cada tecnologia de votação eletrónica pode deter uma construção diferente para que se possa adaptar a requisitos e características diferentes. No entanto, subsistem, pelo menos, três abordagens, classificadas pelos investigadores, exclusivas à conceção de protocolos baseados em criptografia forte, nomeadamente, assinaturas cegas, canais anónimos e cifra homomórfica (Haenni et al., 2008; Burmester e Magkos, 2003; Joaquim et. al., 2011; Wang K., 2017; Faria, 2013). As ideias-chave intrínsecas a essas técnicas são as subsequentes:

- **Assinaturas Cegas [*Blind Signatures*]:** Protocolos baseados no conceito de assinatura digital, através dos quais os votos são validados por uma autoridade eleitoral, emissora da assinatura cega, aquando da votação. Estes permitem que o voto seja totalmente dissociado do eleitor, respeitando a audibilidade do sistema e o anonimato. A ideia subjacente a esta técnica reside na aplicação de uma função *blinding function* que esconda o conteúdo da mensagem antes de a mesma ser enviada ao signatário, autoridade de contagem, através de um canal anónimo. No final do processo a assinatura é verificada utilizando a chave pública do signatário que descodifica e publica os votos recebidos, o que permite aos eleitores verificar se o seu voto foi, efetivamente, contabilizado. O esquema de assinatura cega e o canal de submissão anónimo impedem que a autoridade eleitoral, ou qualquer outra pessoa, consiga

associar o voto descriptado ao eleitor que o emitiu. Este sistema pode ser implementado com base num esquema simples, semelhante ao RSA;

- **Canais Anónimos [*Anonymous Channels*]:** Protocolos de votação eletrónica baseados em canais anónimos, isto é, que permitem o envio anónimo de mensagens. A técnica mais proeminente para a construção de canais anónimos baseia-se em *mix networks*, compilação de servidores de anonimização cuja tarefa é guardar, transformar, atrasar, misturar e reenviar uma sequência de mensagens encriptadas recebidas. Quando empregues numa votação, essas mensagens de input representam os votos dos eleitores. Não sendo, pois, possível efetuar a correspondência entre os inputs e os outputs, esta propriedade oferece privacidade ao eleitor aquando da votação eletrónica. Neste sistema, a comunicação é feita por camadas, onde cada camada recebe uma lista de mensagens parcialmente decifradas, de modo a obter o próximo destinatário, próxima camada. Tal como as assinaturas cegas, os canais anónimos são frequentemente utilizados como primitivas criptográficas para fornecer o anonimato nos protocolos de votação eletrónica;
- **Cifra Homomórfica [*Homomorphic Encryption*]:** Uma terceira categoria de protocolos de votação eletrónica é baseada em encriptação homomórfica, introduzida por Cohen e Benaloh (Benaloh, 1987). Esta cifra baseia-se em sistemas criptográficos que preservam operações como, por exemplo, a de multiplicação ou a de adição de blocos. A ideia consiste, portanto, em aplicar uma operação aritmética a números encriptados, sem que esses sejam previamente decifrados. A soma encriptada resultante, por exemplo, pode ser decifrada através de uma chave privada de descriptação. Os esquemas de encriptação homomórfica asseguram que os números individuais não possam ser descriptados apenas com recurso à chave de descriptação privada. Num esquema de votação baseado na encriptação homomórfica, os eleitores podem autenticar-se, abertamente, nos servidores de votação. Como nenhum voto individual necessita de ser revelado, não há necessidade de assinaturas cegas ou canais anónimos para assegurar a privacidade do eleitor. Resumidamente, a cifra homomórfica assenta na efetuação de correspondências. Na literatura, vários protocolos são baseados na encriptação homomórfica, mas poucas são as

implementações concretas. Um criptosistema parcialmente homomórfico é, por exemplo, o algoritmo El Gamal.

De facto, um sistema de votação eletrónica pode ser bastante complexo e requer, tipicamente, mais do que uma ferramenta criptográfica. As três primitivas analisadas são fundamentais na conceção de novos sistemas, porém, não respondem a todos os requisitos necessários. Posto isto, complementarmente às primitivas previamente referidas, é ainda importante efetuar uma breve descrição de duas outras (Burmester e Magkos, 2003; Wang K., 2017; Faria, 2013), designadamente:

- **Segredo partilhado [*Secret Sharing*]**: Se a encriptação homomórfica está para a composição de operações aritméticas, o segredo partilhado está, por sua vez, para a decomposição. Trata-se de uma ferramenta criptográfica que permite que um grupo de, pelo menos, k membros descodifiquem uma cifra. Cada membro possui uma coordenada única do polinómio e , nesse sentido, é impossível reconstruir o polinómio e calcular a chave privada a menos que haja, pelo menos, k membros a trabalhar conjuntamente. O segredo partilhado é, normalmente, utilizado num ambiente de múltiplas autoridades e baseia-se no pressuposto de que estas não conluiariam, no decurso da eleição, a contagem ou identidade dos votos. *Threshold Cryptosystem* é, a título de exemplo, um tipo de segredo partilhado (Bernhard e Warinschi, 2013);
- **Provas de conhecimento zero [*Zero-knowledge Proofs*]**: Introduzido, em 1985, por Goldwasser, Micali e Rackoff. Um protocolo deste carácter permite que um provador demonstre que uma afirmação é realmente o que é reivindicado sem revelar nenhum conhecimento adicional sobre ela. A cifra homomórfica não permite, no caso da contagem dos votos, verificar se o voto do eleitor foi efetivamente contabilizado, já através de provas de conhecimento zero tal é possível. Este é um método amplamente utilizado na criptografia, em esquemas de votação eletrónica, para fins de verificação. Este sistema utiliza chaves assimétricas e carece do auxílio de uma autoridade confiável. É habitual utilizar provas de conhecimento zero na votação eletrónica para fundamentar a correção das *mix networks* e a retificação da decifração dos votos em sistemas homomórficos.

Atualmente, são utilizados quatro modelos criptográficos fundamentais no âmbito da votação eletrônica, tendo em conta a técnica de anonimização utilizada (Burmeister e Magkos, 2003; de Sousa Grilo, 2015). Os sistemas *E-Voting* pertencem, então, a um dos quatro modelos seguintes:

1. **Modelo de Assinaturas Cegas:** As assinaturas cegas são utilizadas, neste modelo, para possibilitar o voto anónimo, dissociando o voto do respetivo eleitor. Este foi proposto, pela primeira vez, por Atsushi Fujioka, utilizado para resolver a problemática da validação de votos com respeito à privacidade do eleitor, sem recorrer, para tal, a canais anónimos. O modelo tem, no entanto, a particular desvantagem de exigir que o eleitor esteja ativo em duas fases do processo, a fim de garantir o correto funcionamento do protocolo;
2. **Modelo de Canais Anónimos:** Um canal anónimo esconde a correspondência estabelecida entre o remetente e a respetiva mensagem, ou seja, protege a sua identidade. O primeiro canal anónimo proposto na literatura por David Chaum (Chaum, 1981), *mix network*, consiste numa sequência de servidores, cada um dos quais recebe um conjunto de mensagens de entrada e produz um conjunto de mensagens de saída, numa ordem permutada, o que quebra a ligação entre o remetente e o destinatário e, em última análise, transforma o rastreamento da comunicação mais difícil. Representa, pois, um modelo que se serve de múltiplas camadas para assegurar o anonimato, isto é, de cada vez que o voto atravessa uma camada são geradas novas chaves secretas. Trata-se, portanto, de um método que providencia anonimato, mas requer, consequentemente, um profuso poder computacional (Danezis e Diaz, 2008);
3. **Modelo de Cifra Homomórfica:** Modelo proposto por Ronald Cramer (Cramer et al., 1997), que se baseia em propriedades e algoritmos de cifra homomórfica, previamente descritos. Funções homomórficas são, em modelos desta natureza, aplicadas para calcular o resultado da eleição, sem decifrar os votos individuais. O mecanismo de encriptação homomórfica baseia-se na aplicação de operações aritméticas a números cifrados. O resultado pode ser decifrado adotando uma chave privada, no entanto, não

é possível a decifragem dos números de forma individual recorrendo a essa mesma chave privada. Sucintamente, cada eleitor cifra o seu voto com a chave pública da autoridade de voto. Por sua vez, os votos cifrados, recebidos pelo sistema, são distribuídos pelos clientes de contagem, onde cada um decifra o resultado parcial e publica-o. Como os votos não são decifrados individualmente, os eleitores podem estar associados a um dado voto sem que percam a sua privacidade. Por conseguinte, deixa de ser necessária a utilização de assinaturas cegas ou de canais anónimos. Por fim, procede-se ao apuramento da votação, onde os resultados parciais são agregados e é obtido o resultado. A precisão da contagem final pode ser verificada por todas as partes, portanto, existe verificabilidade universal. Desfavoravelmente, o modelo carece de uma alta capacidade computacional;

4. **Modelo de Benaloh:** Exemplo da utilização do mecanismo de encriptação homomórfica, proposto por Benaloh (Benaloh, 2006), onde cada eleitor partilha uma fração do seu voto com múltiplas autoridades de voto, cifrada com a chave pública da autoridade recetora que a publicará. No final do processo de votação, as autoridades reúnem as respetivas frações para efetuar a apuração do resultado da eleição. Esquemas desta natureza, embora estruturalmente simples, acarretam custos elevados de comunicação, uma vez que cada eleitor necessita de submeter o seu voto através de múltiplos canais, tantos quanto o número de autoridades de voto em causa. O modelo utiliza o princípio do segredo partilhado.

2.2.3 Sistemas Vigentes

Existem, atualmente, múltiplos sistemas que possibilitam a realização de votações pela Internet. Nesta secção é apresentado um breve panorama, fundamentalmente centrado em aspetos arquiteturais, relativo aos sistemas de votação eletrónica mais relevantes propostos pela comunidade científica, à luz de alguns dos protocolos e modelos criptográficos referidos anteriormente. Em particular, os sistemas *Helios* e *Sensus*, considerados na análise, foram concebidos para efetivação de eleições de pequena escala, o que poderá servir de referência para a especificação da futura plataforma, objetivo central da dissertação. De um modo geral,

esta análise auxilia na compreensão das tecnologias utilizadas na implementação dos diversos sistemas de votação existentes, dos requisitos que os mesmos satisfazem e, ainda, das suas limitações.

2.2.3.1 Helios

Sistema de votação pela internet, *open-source*, *web-based*, que possibilita a auditoria dos votos, averiguação de que são recebidos e apurados de forma apropriada, por parte dos eleitores e, ainda, a verificabilidade universal, sendo um sistema *open-audit*. Desenhado com base no modelo de Benaloh (Benaloh, 2006), e com recurso às mais recentes tecnologias e mais avançadas técnicas criptográficas, de modo a assegurar a integridade dos votos e a privacidade do eleitor num ambiente inseguro como aquele facultado pela Internet (Wang K., 2017).

Trata-se, portanto, de um sistema passível de ser utilizado em votações organizadas por qualquer organização, grupo ou comunidade, que visa assegurar, entre outras propriedades, a verificabilidade e o sigilo do voto (Brioso, 2012). A verificabilidade, por sua vez, assegura a retificação do resultado, independentemente do software ou hardware em causa: o protocolo de votação fornece procedimentos de auditoria e provas criptográficas que permitem verificar a correção do resultado.

A verificabilidade é, frequentemente, dividida em três propriedades distintas (Brioso, 2012; Cortier et. al., 2019; Bernhard e Warinski, 2013):

1. **Verificabilidade individual:** Cada eleitor é capaz de verificar se o seu boletim de voto foi apurado;
2. **Verificabilidade universal:** Qualquer pessoa é capaz de verificar se o resultado corresponde a todos os boletins de voto publicados;
3. **Verificabilidade de elegibilidade:** Qualquer pessoa pode verificar se os boletins de voto advêm, apenas, de eleitores elegíveis.

A verificabilidade pode, ainda, ser dividida em três noções (Cortier et. al., 2019), de acordo com as diferentes fases da eleição, assegurando a verificabilidade *end-to-end*:

1. **Cast-as-intended**: A cédula encriptada inclui o voto elegido pelo eleitor;
2. **Recorded-as-cast**: O voto registado corresponde ao voto emitido pelo eleitor;
3. **Counted-as-recorded**: Todos os votos registados são corretamente contabilizados.

Posto isto, o Helios disponibiliza dois métodos de verificação, um a ser utilizado pelos eleitores, na correção do voto entregue ao *Ballot Preparation System*, e outro a ser utilizado pelos administradores. Apesar de estarem focados nos eleitores e administradores, todos os intervenientes, incluindo eleitores não elegíveis, podem auditar toda a eleição recorrendo a ambos os métodos (Joaquim et. al., 2011).

As premissas criptográficas aplicadas no Helios são a cifra homomórfica, modelo proposto por Ronald Cramer (Cramer et al., 1997), e o algoritmo El Gamal, sistema de chaves assimétricas, proposto por El Gamal (Taher Elgamal, 1984). O sistema é implementado com recurso a técnicas de encriptação homomórfica, focada em E-Voting, e ElGamal exponencial. É também utilizada a contagem através de mix networks, para assegurar a propriedade *count-as-recorded*, e o mecanismo de verificação proposto por Josh Benaloh (Benaloh, 2006), para garantir a propriedade de *cast-as-intended*. O sistema utiliza, ainda, *threshold encryption*, em detrimento da comum encriptação de chave pública, de modo a evitar qualquer ponto único de potencial contravenção de privacidade. *Threshold encryption* não admite a descriptação através de entidades individuais, sendo exigido um número mínimo pré-determinado de mandatários para o efeito.

2.2.3.2 REVS [Robust Electronic Voting System]

Sistema de votação concebido para ambientes distribuídos com falhas, como a Internet, para apoiar eleições em larga escala. O REVS cumpre as características desejadas dos sistemas de votação tradicionais, tais como exatidão, democracia, privacidade e verificabilidade e, ademais, permite um processo de votação seguro, mesmo num ambiente defeituoso.

Essencialmente, este é um sistema de votação pela internet tolerante a falhas e baseado no modelo de assinaturas cegas. Para além de tolerar falhas na rede, nos servidores e nos clientes de voto, através de uma arquitetura baseada na replicação de componentes, é também capaz de garantir, até certo nível, o correto funcionamento das entidades envolvidas e, consequentemente, do sistema em geral. Na arquitetura original, os canais anónimos, estabelecidos entre eleitores e servidores de votação, são implementados com recurso a servidores especiais, designados *Anonymizers* (Wang K., 2017; Eliasson e Zúquete, 2006).

O REVS utiliza uma arquitetura composta por quatro servidores, designadamente, *Ballot Distributor*, *Administrators*, *Anonymizers* e *Counters*. Existe, ainda, um *Voter's module*, utilizado pelos eleitores como apoio à sua participação e, ainda, um *Commissioner*, módulo responsável pela preparação da eleição (Eliasson e Zúquete, 2006). Os componentes descritos são, detalhadamente, os seguintes:

- **Comissário [*Commissioner*]:** Módulo utilizado para preparar a eleição, isto é, registar os eleitores e definir a configuração operacional para a eleição, ou seja, o par de chaves eleitorais, o voto, os endereços e chaves públicas dos servidores, o número de assinaturas necessárias, entre outros. O comissário também assina todos os dados eleitorais, para que qualquer pessoa possa verificar a autenticidade dos mesmos. Este pode ser visto como uma espécie de comissão eleitoral;
- **Distribuidor de boletins de voto [*Ballot Distributor*]:** Assegura a distribuição dos boletins pelos eleitores e é responsável pela configuração das chaves e assinaturas envolvidas no processo. Toda a informação que este distribui deve ser assinada pelo comissário, em que todos os eleitores confiam. Assim, podem ser replicados vários distribuidores o que, em última análise, além de reduzir a carga de trabalho em cada um, melhora a eficiência, em eleições de larga escala, e proporciona tolerância às falhas de comunicação, proporcionando robustez ao processo de distribuição;
- **Administradores [*Administrators*]:** Entidades eleitorais que têm o poder de decidir sobre a aceitabilidade de um voto de um eleitor. Um voto só é aceitável para a contagem final da eleição se tiver um conjunto mínimo de assinaturas de diferentes administradores. O eleitor utiliza uma chave diferente na autenticação com cada

administrador e, uma vez que o administrador não consegue derivar nenhuma outra chave a partir daquela que conhece, não pode, por si só, fazer-se passar por um eleitor;

- **Anonimizadores [Anonymizers]:** Fornecem anonimato ao eleitor, impedindo que um contador associe o voto ao respectivo IP da máquina. Estes servidores atrasam e misturam, aleatoriamente, os votos dos eleitores, antes de serem enviados para os contadores. A aleatoriedade nas submissões dos votos impede, portanto, a potencial associação entre votos e respectivos eleitores, tendo por base o tempo da participação na votação;
- **Contadores [Counters]:** Servidor que verificam a validade dos votos, ou seja, se contêm todas as assinaturas requeridas. Posteriormente, remove votos repetidos e efetua a contagem. Os eleitores enviam os seus boletins de voto finais aos contadores através dos anonimizadores, encriptados com a chave pública da eleição, impedindo assim os anonimizadores e os contadores de assistirem aos votos durante a eleição. No entanto, o sistema REVS pode ser também utilizado sem recurso a Anonimizadores e, nesse cenário, os eleitores enviam os seus votos diretamente aos contadores;
- **Módulo do eleitor [Voter's Module]:** Módulo utilizado pelo eleitor para participar na eleição. Realiza todas as interações adequadas com os servidores eleitorais, tais como obtenção do boletim de voto, aquisição da assinatura dos administradores e posterior submissão do mesmo. Este módulo é ainda responsável por gerar as chaves secretas do eleitor e controlar o correto preenchimento do boletim de voto.

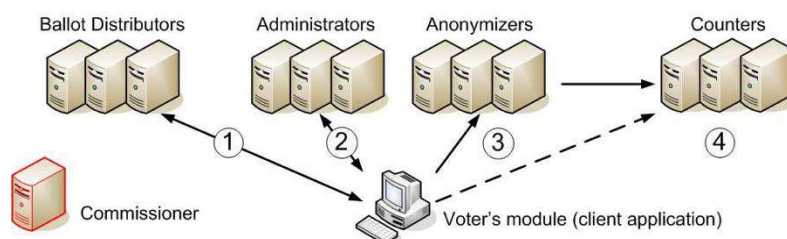


Figura 1 - Arquitetura original REVS (Zúquete et. al., 2008)

Analisando, então, a arquitetura inicialmente proposta para o sistema REVS, tal como ilustrado na Figura 1, o primeiro passo passa pela recolha do boletim, preparado pelo comissário, por parte do eleitor que, no segundo passo, é autenticado pelos administradores do sistema. Posteriormente, o eleitor recebe o seu voto cego assinado por mais de metade dos administradores e, já no terceiro passo, esse mesmo voto é submetido aos contadores através dos anonimizadores. Por fim, no quarto e último passo, os contadores totalizam e publicam os votos recolhidos (Zúquete e Almeida, 2008; Zúquete et. al., 2008).

2.2.3.3 Sensus

Sistema de votação eletrónica sugerido por Lorrie Cranor e Ron Cytron, (Cranor et al., 1997), na sequência do trabalho realizado por Fujioka, Inicialmente pensado para reproduzir a votação por correio tradicional, veio a revelar-se suficientemente flexível para permitir outros tipos de votação, nomeadamente eleições em pequena escala, isto é, com um número de intervenientes moderado. Utiliza assinaturas cegas de modo a assegurar que apenas eleitores registados possam votar e, ainda, que votem somente uma vez. O Sensus permite que os eleitores verifiquem se os seus votos foram contados de forma correta e anónima. Mesmo satisfazendo a maioria dos requisitos de segurança de um sistema de votação eletrónica, o Sensus permite que uma das entidades envolvidas no processo eleitoral possa emitir os seus próprios votos em nome da abstenção (Wang K., 2017).

O Sensus é, então, um sistema que apresenta quatro componentes essenciais (Zúquete et. al., 2008):

- **Registador [Registrar]:** Responsável pelo registo dos eleitores em cada eleição. Este deve selecionar uma lista de pessoas elegíveis para registo e uma lista de pessoas que se candidataram ao registo e cujas identidades foram verificadas. Através dessa seleção origina, depois, uma lista de eleitores registados. Os eleitores registados são, geralmente, listados pelos seus nomes ou códigos de identificação, uma chave pública de encriptação e, opcionalmente, um endereço de correio eletrónico;

- **Agente [Pollster]:** Atua como um agente de votação do eleitor, que apresenta os boletins de voto a cada eleitor e coleciona esses votos, sendo ainda responsável pelas operações criptográficas e entrega dos boletins de voto à urna. Trata-se, portanto, do único componente do sistema completamente confiável. Este pode também ser utilizado para ajudar os eleitores a verificar se os seus votos foram contados corretamente ou para concorrer a uma eleição;
- **Validador [Validator]:** Responsável por verificar o registo de eleitores e assegurar que apenas um voto é emitido por cada eleitor registado. O validador cria um certificado de validação cego ao assinar um boletim de voto cego. O eleitor, então, decifra o certificado de validação e submete-o ao contador juntamente com o voto. Este utiliza a lista de eleitores registados para obter a chave pública de cada eleitor e verificar as assinaturas nos seus boletins de voto. Com este método não é mantido qualquer registo da ordem em que os boletins de voto são validados;
- **Contador [Tallier]:** Responsável pela recolha dos votos, contagem e apuração dos resultados da eleição. Os eleitores submetem, primeiramente, os boletins de voto encriptados, assinados pelo validador, ao contador e este, por sua vez, verifica a autenticidade da validação e se o voto encriptado é único entre os recebidos até à data. Se o boletim de voto for válido e único, o contador emite um recibo assinado ao eleitor.

CAPÍTULO 3

CARATERIZAÇÃO DA PLATAFORMA EVOTUM

No presente capítulo é descrita a arquitetura atual da plataforma de votação eletrônica eVotUM, plataforma essa que servirá de referência, no próximo capítulo, para a especificação da futura plataforma de votação, adequadamente adaptada a contextos mais nuclearizados de votação em reuniões. Caracterizar o atual sistema de votação passa, então, por descrever um conjunto de atributos que o integram. Nesse sentido, o capítulo começa por apresentar uma visão integral da plataforma, isto é, uma descrição das suas principais características, funcionalidades e, ainda, intervenientes. Posto isto, o capítulo subdivide-se em duas lógicas distintas, designadamente, o comportamento funcional e a arquitetura tecnológica inerentes à plataforma de votação eletrônica eVotUM. A infraestrutura tecnológica da plataforma é, no segmento final do capítulo, repartida pela descrição das suas componentes de Software e Hardware, da sua arquitetura e, ainda, do seu fluxo de comunicação, para identificação das componentes mais relevantes e posterior reutilização em proveito da eVotUM *light*.

3.1 Visão Integral da Plataforma

Numa primeira fase de caracterização da eVotUM é apresentada uma visão integral da plataforma e, como tal, numa primeira instância, são especificados os seus intervenientes. Posteriormente, são discriminadas matérias referentes ao processo de votação por parte do eleitor, à gestão do processo eleitoral por parte da comissão eleitoral, à gestão do sistema por parte do administrador, a toda a comunicação estabelecida na plataforma, ao tipo de eleições autorizadas, entre outras. Por último, de modo a retratar as transições de estado associadas ao processo eleitoral e à eleição, são apresentados os seus respetivos diagramas de estado, recorrendo à ferramenta de modelação UML. É, portanto, descrito, sucintamente, o propósito da plataforma, todas as suas funcionalidades, e quem intercede em cada uma das mesmas. Os anexos contêm, ainda, o Guia do Eleitor, o Guia da Comissão Eleitoral, bem como o Guia do Responsável Institucional.

3.1.1 Intervenientes

Os agentes que interatuam com o sistema eVotUM desempenham funções diferenciadas e dispõem de restrições de acesso igualmente distintas, sendo, portanto, necessário clarificar quem são esses intervenientes e quais os papéis que desempenham na plataforma. Na tabela 2 são enumerados todos os possíveis intervenientes na plataforma e descrita a função que nela desempenham.

Tabela 2 - Intervenientes na Plataforma de Votação Eletrónica eVotUM

Interveniente	Descrição
Administrador Técnico	Responsável pela gestão das páginas de conteúdo informativo da plataforma, bem como pela emissão e correspondente carregamento de certificados digitais a serem utilizados pelo sistema eVotUM. Tem, para tal, acesso ao Sistema de Administração .
Público	Apto a aceder às páginas públicas do Sistema de Votação , com: • Informação genérica: Perguntas frequentes, Política de segurança de informação, Política de privacidade, Termos de utilização, Mapa do site e Contactos; • Consulta de Processos Eleitorais: Toda a informação disponibilizada pela Comissão eleitoral; • Verificação de Caderno Eleitoral: Podendo ser apresentada uma reclamação em caso de equívocos no mesmo.
Eleitor	Uma vez autenticado no Sistema de Votação , através das credenciais utilizadas na Intranet da Universidade do Minho, está apto para: • Alterar Dados Pessoais: e-mail, telemóvel, e modo de envio de chave de segurança; • Consultar os Processos Eleitorais dos quais faz parte do Caderno Eleitoral; • Comunicar com a Comissão Eleitoral; • Votar em cada uma das Eleições, caso esteja dentro do período de votação; • Verificar se o seu voto foi contabilizado na Eleição, através da introdução da Referência de Votação.
Comissão Eleitoral	Cada elemento da Comissão Eleitoral, depois de autenticado no Sistema de Gestão de Eleições , acede a uma área onde pode selecionar o processo eleitoral a gerir, de entre os processos eleitorais no estado Aberto, alterar os seus Dados Pessoais, e aceder ao Histórico de Ações.

Responsável institucional	Uma vez autenticado no Sistema de Gestão de Eleições , é responsável por criar o Processo Eleitoral, com indicação das várias Eleições, datas relevantes e elementos da Comissão Eleitoral respetivos. Efetuada a criação do processo, o sistema gera um par de chaves de cifra/decifra de votos e envia, automaticamente, as componentes da password às entidades devidas. É, ainda, responsável pela geração da Entidade de Certificação Raiz e pela assinatura de todos os Certificados Digitais emitidos para as componentes do sistema.
----------------------------------	---

3.1.2 Processo de Votação pelo Eleitor

Para participar numa votação através da plataforma de votação eletrónica eVotUM, o eleitor necessita de satisfazer determinadas pré-condições. De modo a esclarecer o processo associado à votação, são descritos, na tabela 3, todos os passos que o constituem. No **anexo I**, é possível analisar, em detalhe, todo o processo de votação, através do Guia do Eleitor.

Tabela 3 – Passos referentes ao Processo de Votação pelo Eleitor

Passo	Descrição
1. Autenticação	O Eleitor autentica-se no sistema eVotUM, sendo-lhe apresentado os Processos Eleitorais, no estado “Aberto”, dos quais faz parte;
2. Seleção de Eleição	Se, dentro desses Processos Eleitorais, alguma Eleição estiver em Período de Votação, é-lhe exibido o botão “Votar”;
3. Votação	A votação numa Eleição é constituída por cinco passos: • Seleção da Eleição do Processo Eleitoral a votar; • Seleção da lista/candidato; • Confirmação da lista/candidato (Se não tiver sido selecionada nenhuma lista/candidato no passo anterior, é solicitado que o Eleitor confirme o voto em branco); • Segunda Autenticação de votação, através do método escolhido; • Apresentação da informação de submissão de voto, incluindo a Referência de Votação (A informação é enviada por correio eletrónico).
4. Verificação de Referência de Votação	À posteriori, após o encerramento das urnas, o Eleitor poderá verificar se o seu voto foi contabilizado, verificando se a sua Referência de Votação se encontra nas Referências de Votação processadas.

3.1.3 Gestão do Processo Eleitoral pela Comissão Eleitoral

A gestão do processo eleitoral, efetuada por membros da Comissão Eleitoral, é composta por uma série de passos, enumerados, de seguida, na tabela 4. No **anexo II**, é possível estudar, em detalhe, todo o processo de gestão do processo eleitoral, através do Guia da Comissão Eleitoral.

Tabela 4 – Passos referentes ao Processo de Gestão do Processo Eleitoral pela Comissão Eleitoral

Passo	Descrição
1. Gestão de Operações do Processo Eleitoral	A gestão do Processo Eleitoral começa pela gestão de operações do Processo Eleitoral, em que é identificado o número de elementos da Comissão Eleitoral necessário para aprovar as diferentes ações. A Comissão Eleitoral pode determinar, consoante o nível de criticidade de cada ação, um dos seguintes níveis de segurança: • Simples – Um elemento (Qualquer elemento pode efetuar essa ação sem necessidade de apresentar a componente de segurança que recebeu); • Forte – Metade (+1) elementos (A ação só é aceite pelo sistema após metade (+1) dos elementos apresentarem as suas componentes de segurança); • Crítico – Todos os elementos (A ação só é aceite pelo sistema após todos os elementos apresentarem as suas componentes de segurança). As ações, a aprovar pelos membros da Comissão Eleitoral são, com nível de segurança por omissão entre parêntesis, as seguintes: • Abrir a Eleição com verificação de que a Urna está vazia (Forte); • Encerramento da Eleição/Urna (Forte); • Contagem de votos (Simples); • Publicitação do Processo Eleitoral (Crítico); • Alterar quem responde às mensagens (Crítico); • Configuração inicial do Processo Eleitoral (Simples); • Outros (Simples).
2. Edição do Processo Eleitoral	A Comissão Eleitoral, em contexto de edição do Processo Eleitoral, pode: • Adicionar informação geral referente ao Processo Eleitoral (Logótipo, Identificador, Descrição, Data de publicação e Documentação a apresentar ao público e eleitores), sendo que alguma fora previamente preenchida pelo Responsável Institucional;

	• Aceder, apenas com permissão de leitura, aos dados dos elementos da Comissão Eleitoral, introduzidos pelo Responsável Institucional.
3. Gestão da Eleição	A Comissão Eleitoral pode aceder ao painel de eleições do Processo Eleitoral, onde pode gerir cada uma das Eleições, em termos de: • Configuração geral (Identificador, Descrição e Tipo de eleição); • Calendário Eleitoral (Período de receção de proposituras, Publicação de Caderno Eleitoral provisório e definitivo, Período de Votação, Consulta de Referência de Votação e Publicação/Verificação da Ata Eleitoral); • Categoria/Peso dos votantes; • Carregamento e publicitação do Caderno Eleitoral (Pode ser corrigido pela Comissão Eleitoral até à publicação do Caderno Eleitoral definitivo); • Dados das Listas/Candidatos; • Elaboração e pré-visualização do Boletim de Voto.
4. Gestão de Operações da Eleição	A Comissão Eleitoral tem, ainda, acesso a um painel de Gestão de Operações da Eleição, a ser utilizado durante o período de votação, onde é possível: • Confirmar a data e hora de abertura da votação e a inexistência de votos em urna; • Verificar o número de total de votos em urna, durante o Período de Votação; • Confirmar a data e hora de encerramento da votação; • Iniciar o escrutínio dos votos e respetiva apresentação de resultados.

3.1.4 Criação do Processo Eleitoral pelo Responsável Institucional

A criação de um processo eleitoral é efetuada pelo Responsável Institucional, depois de autenticado na respetiva área do sistema eVotUM. A criação do processo eleitoral passa por definir uma série de parâmetros, designadamente:

- **Dados Gerais do Processo Eleitoral:** logótipo, identificador e respetiva descrição do processo eleitoral;
- **Dados Gerais da Eleição:** identificador e respetiva descrição da eleição;
- **Calendário Eleitoral:** período de receção de proposituras, publicação de caderno eleitoral provisório e definitivo, período de votação e, ainda, período de publicação de resultados e de homologação;

- **Membros:** identificação dos membros da Comissão eleitoral.

O processo de criação de um processo eleitoral tem ainda um conjunto de considerações a ter em conta, nomeadamente:

- Aquando da criação de uma eleição, toda e qualquer data de fim, a definir, terá de ser, necessariamente, posterior à data de início do respetivo período;
- As datas de início e de fim do período de reclamação referente ao caderno eleitoral têm de compreender, necessariamente, as datas de publicação de ambos os cadernos provisório e definitivo;
- O período de apresentação de listas candidatas antecede o período de publicação dos cadernos eleitorais provisório e definitivo, que antecede o período de votação que, por sua vez, antecede a data de publicação de resultados. Por fim, o período de homologação sucede a publicação de resultados, sendo, portanto, o último a definir;
- Os membros a nomear como parte integrante da comissão eleitoral têm de constar da lista de utilizadores da plataforma eVotUM. No caso concreto da eVotUM, tal corresponderá a todos os alunos, docentes, e membros da comunidade académica da Universidade do Minho, os quais já têm associado um contacto e endereço de correio eletrónico;
- Aos membros nomeados como parte integrante da comissão eleitoral tem de ser atribuída uma designação e, ainda, a sua função. A função poderá corresponder a uma distinção como presidente da comissão eleitoral, ou como membro regular;
- O presidente da comissão eleitoral é configurado, automaticamente, pelo sistema, como responsável pelo envio e resposta às mensagens da comissão eleitoral;
- Após a criação e submissão do processo eleitoral, o responsável institucional terá de efetuar uma segunda autenticação através da chave móvel digital;
- O sistema eVotUM gera, automaticamente, chaves de cifra e de decifra para cada eleição e divide a password de acesso à chave de decifra em N componentes, sendo N o número de elementos da comissão eleitoral. As componentes são enviadas a cada um dos elementos da comissão eleitoral através do correio eletrónico;

- No caso de os elementos da comissão eleitoral sofrerem alterações, o responsável institucional garante a edição do processo eleitoral respetivo. A edição dos membros só é exequível até à data de publicação do processo eleitoral, uma vez que a geração de novas chaves de eleição poderá impedir a decifra dos votos;

No **anexo III**, é possível analisar, com detalhe, todo o processo de criação de um processo eleitoral, através do Guia do Responsável Institucional. Este contém, ainda, orientações adicionais relativas à geração de certificados de eleição e *Secret Shared Keys* do responsável institucional.

3.1.5 Gestão do Sistema pelo Administrador Técnico

O administrador técnico do sistema tem acesso ao Sistema de Administração, sistema esse que dispõe das seguintes funcionalidades:

- Gestão de páginas estáticas;
- **Carregamento de certificados** emitidos para serviços do sistema, tais como: *Root self-signed Certificate*, *Root Private key*, *Validator Service Certificate*, *Validator Service Private key*, *Counter Service Certificate*, *Counter Service Private key*, *Voting System Certificate* e *Voting System Private key*;
- Monitorização de todas as componentes do sistema.

O sistema incorpora, ainda, um conjunto de alarmes que atuam, proactivamente, sobre o mesmo, sendo o administrador técnico avisado, automaticamente, sempre que os diferentes parâmetros do sistema não se encontrem nos valores ótimos de processamento.

3.1.6 Comunicação na Plataforma

Na plataforma de votação eletrónica eVotUM é disponibilizado um sistema de mensagens que admite correspondências entre diferentes intervenientes, designadamente:

- Comunicação entre o Eleitor, ou utilizador não autenticado, e a Comissão Eleitoral;
- Comunicação entre a Comissão Eleitoral e o Eleitor, ou conjunto de eleitores. O conjunto de eleitores é agrupado por processo eleitoral, eleição e/ou categoria do eleitor.

Para enviar mensagens, através da plataforma, o utilizador tem de seleccionar um ou mais destinatários, segundo uma conduta de busca específica, de acordo com o seu desígnio:

- Enviar mensagem a todos os membros da **Comissão Eleitoral**: Pesquisar pelo nome do Processo Eleitoral;
- Enviar mensagem a todos os **Eleitores**: Pesquisar pelo nome da Eleição;
- Enviar mensagem a **Eleitores** com **peso de voto específico**: Pesquisar pelo nome da eleição ou pelo peso de voto em causa;
- Enviar mensagem a um **Eleitor** ou membro da **Comissão Eleitoral**: Pesquisar por nome ou e-mail.

O sistema de comunicação que se estabelece na plataforma conta, ainda, com diversas outras particularidades, nomeadamente:

- As mensagens concebidas na plataforma são enviadas para a caixa de correio do sistema eVotUM e, ainda, para o e-mail de comunicação identificado pelo eleitor, público ou membro da Comissão Eleitoral;
- Não é possível responder ou enviar mensagens para o sistema a partir de e-mails externos ao mesmo;
- Todos os elementos da Comissão Eleitoral têm permissão para visualizar a caixa de correio respetiva, mas apenas um dos elementos, configurado através do painel de eleições do processo eleitoral, pode responder e/ou enviar mensagens em nome da Comissão;
- O sistema de mensagens mantém um histórico/arquivo de todas as mensagens enviadas e recebidas.

3.1.7 Tipos de Eleição Autorizados

A plataforma de votação eletrônica eVotUM oferece, aos seus eleitores, uma ampla variedade de eleições. Cada parâmetro associado a uma determinada eleição é configurado de acordo com as necessidades inerentes ao respetivo ato eleitoral. A configuração da eleição está, pois, ao encargo da Comissão Eleitoral. Na tabela 5 são enumeradas as configurações disponíveis no sistema, passíveis de serem aplicadas numa eleição.

Tabela 5 - Configurações disponíveis para uma Eleição na Plataforma eVotUM

Configuração	Descrição
Categoria do Eleitor	Cada eleitor pode ser detentor de um “peso” diferente, isto é, a influência do seu voto pode ser inferior ou superior à de um outro eleitor, consoante a categoria a que pertencer.
Formato de Visualização	A visualização das Listas/Candidatos, no boletim de voto, pode surgir em dois formatos distintos: • Formato de Lista - Listas apresentadas sequencialmente. O eleitor seleciona a lista de interesse e, posteriormente, surge uma cruz na opção selecionada; • Formato Dropdown - Cada linha do boletim de voto contém uma lista, em formato Dropdown. O eleitor seleciona a lista de interesse e essa torna-se visível.
Limite de Escolhas Assinaláveis	O eleitor pode escolher uma ou mais Listas/Candidatos.
Funcionalidade Write In	O eleitor pode escolher um candidato cujo nome não consta no boletim de voto. Para tal, deve preencher, no local assinalado, o nome do candidato.
Método D’Hondt	O método D’Hondt, também conhecido como método dos quocientes, é aplicado nas eleições com mais de um lugar em disputa. É um sistema matemático que permite distribuir o número de mandatos pelos candidatos elegíveis.
Votação Ordenada	Os eleitores classificam as Listas/Candidatos de acordo com a sua ordem de preferência.

3.1.8 Arquivo do Processo Eleitoral

O processo eleitoral é arquivado, de forma automática, seis meses após a última homologação da ata da eleição nesse processo, ocorrendo as seguintes ações:

- O processo eleitoral, tal como todas as suas eleições, passa para o estado Arquivado;
- Todos os dados de votação são apagados do sistema eVotUM. É apagado o estado da votação no *Validator Service*, os votos guardados e decifrados no *Counter Service* e a referência de votação guardada no *Anonymizer Service*.

Toda a informação remanescente ao processo, bem como respectivas eleições, continua a poder ser acedida pelo público e pelos eleitores.

3.1.9 Diagramas de Estados

A ferramenta de especificação UML prevê um diagrama exclusivo para a modelação do comportamento interno de um determinado objeto, subsistema ou sistema global, durante o seu ciclo de vida. A esse diagrama é concedido o nome de Diagrama de Estados ou, ainda, Diagrama de Máquina de Estados.

Através da sua utilização é possível retratar os diferentes estados de um objeto, as correspondentes transições entre estados, os eventos que fazem desencadear tais transições, bem como as operações, ações e atividades, que são executadas dentro de um estado ou durante uma transição. Os objetos evoluem, ao longo do tempo, através de um conjunto de estados, como resposta a eventos e à passagem de tempo.

3.1.9.1 Processo Eleitoral

O Processo Eleitoral passa, necessariamente, por quatro estados, designadamente:

- **Novo:** Após a criação do Processo Eleitoral pelo Responsável Institucional;

- **Aberto:** Após a publicitação automática do Processo Eleitoral, em data/hora definida pela Comissão Eleitoral;
- **Fechado:** Após o fecho de todas as eleições do Processo Eleitoral;
- **Arquivado:** Seis meses após a transição para o estado Fechado.

Nos estados Fechado e Arquivado, tanto o público como o eleitor, continuam a ter acesso aos dados do respetivo processo eleitoral. Na figura 2, ilustra-se o diagrama de estados referente ao Processo Eleitoral, para uma melhor compreensão.

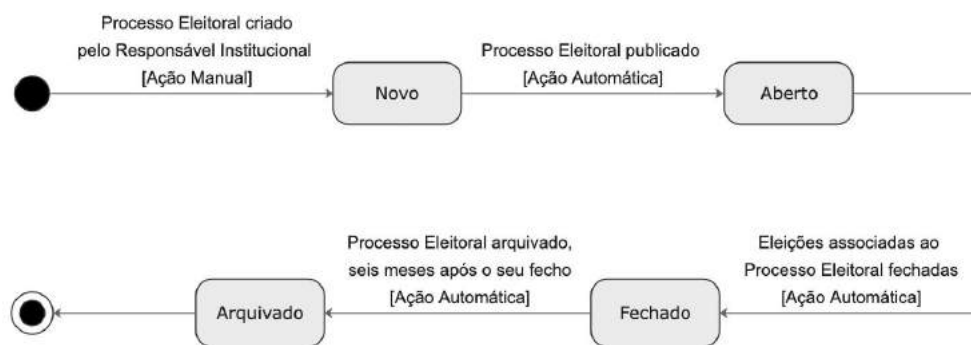


Figura 2 - Diagrama de Estados referente ao Processo Eleitoral

3.1.9.2 Eleição

Todas as eleições passam, obrigatoriamente, por nove estados, designadamente:

- **Novo:** Após a criação da Eleição pelo Responsável Institucional;
- **Aberto:** Após a publicitação automática do Processo Eleitoral, em data/hora definida pela Comissão Eleitoral;
- **Caderno Eleitoral Provisório:** Após iniciação do período de verificação do caderno eleitoral, em data/hora definida pela Comissão Eleitoral;
- **Caderno Eleitoral Definitivo:** Após finalização do período de verificação do caderno eleitoral, em data/hora definida pela Comissão Eleitoral;

- **Em votação:** Após iniciação do período de votação, em data/hora definida pela Comissão Eleitoral;
- **Em contagem:** Após finalização do período de votação, em data/hora definida pela Comissão Eleitoral;
- **Votos escrutinados:** Após escrutinação dos votos pela Comissão Eleitoral;
- **Ata em homologação:** Após disponibilização da ata pela Comissão Eleitoral;
- **Fechada:** Após finalização do período de verificação da ata, em data/hora definida pela Comissão Eleitoral.

No estado Fechado, tanto o público como o eleitor, continuam a ter acesso aos dados da respetiva eleição. Na figura 3 é ilustrado o diagrama de estados referente à Eleição, para uma melhor compreensão.

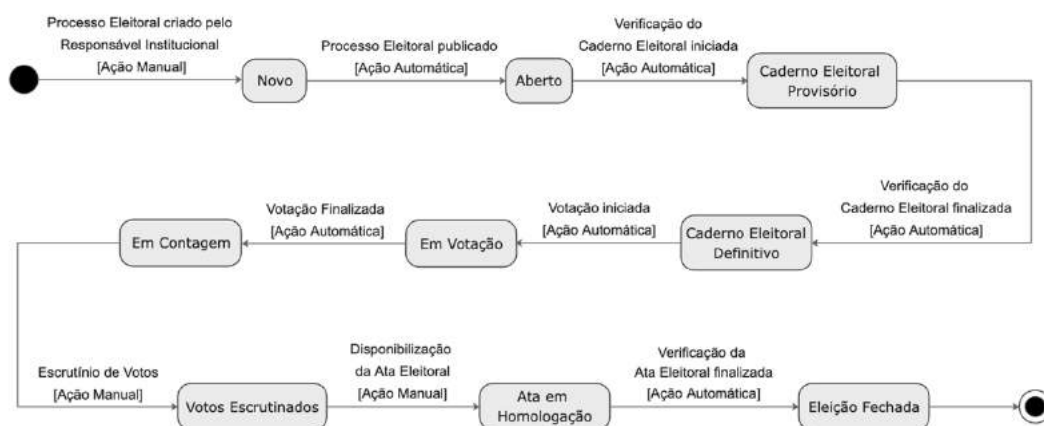


Figura 3 - Diagrama de Estados referente à Eleição

3.2 Comportamento Funcional da Plataforma

A plataforma de votação eletrónica atual, eVotUM, pode ser caracterizada através de uma especificação funcional do seu comportamento, que consiste, essencialmente, na enunciação dos requisitos funcionais e, ainda, dos requisitos não funcionais implementados no âmbito do projeto.

Os requisitos do sistema constituem o conjunto de condições que definem a estrutura e comportamento do software. Requisitos convenientemente delineados e documentados são essenciais para qualquer projeto de engenharia de software bem-sucedido. Os requisitos são, portanto, declarações articuladas de forma clara sobre o que o sistema deve ser capaz de fazer para satisfazer as necessidades e condições dos utilizadores. Estes são definidos em duas categorias distintas, designadamente, requisitos funcionais e requisitos não funcionais, sendo que os primeiros descrevem o comportamento e funções do sistema, e os últimos descrevem os critérios que podem ser empregues na avaliação do funcionamento do mesmo.

3.2.1 Requisitos Funcionais

Requisitos funcionais pormenorizam comportamentos específicos que o software deve ser capaz de satisfazer, sendo, portanto, definidos como requisitos que especificam o que sistema deve, necessariamente, fazer. O conceito também pode ser entendido através da revisão do sistema em termos de entradas e saídas, isto é, especifica o que o sistema deve fazer em resposta a diferentes entradas.

Os requisitos funcionais, implementados no âmbito do desenvolvimento da plataforma eVotUM, são devidamente especificados no **anexo IV**, passível de ser consultado no final do presente documento, segundo as suas respetivas categoria e subcategoria, e aliados a uma descrição pormenorizada. De seguida, através da Tabela 6, é possível visualizar a informação referente ao primeiro requisito de cada uma das categorias existentes.

Tabela 6 - Requisitos Funcionais implementados no âmbito do projeto da eVotUM

Requisito	Categoria	Subcategoria	Descrição
REQ 1.1	Geral	Design	O tema genérico deve estar adaptado aos browsers Internet Explorer 11, Firefox 34, Chrome 40, Safari, e versões superiores.
REQ 2.1	Sistema de Consultas	Página Inicial	A Homepage deve apresentar a informação seguinte:

			• Logótipo eVotUM e frase estática “Sistema de Votação Eletrónica da Universidade do Minho”: Redireciona para a Homepage ao clicar; • Menu Estático: Processos Eleitorais [REQ 2.8], Como Funciona [REQ 2.11], Contactos [REQ 2.12]; • Texto estático sobre a plataforma; • Botão "Verificar cadernos eleitorais": Redirecionada para a listagem de processos eleitorais [REQ 2.8]; • Botão "Autentique-se para votar": Redireciona para a página de autenticação [REQ 2.6].
REQ 3.1	Sistema de Votação	Passo 1: Selecionar Eleição	O eleitor autenticado ao clicar no botão "votar" que surge no detalhe do processo eleitoral ou na listagem dos meus processos eleitorais, é redirecionado para a área de votação. O sistema de votação é constituído por 5 passos [REQ 3.1 a REQ 3.6]. No passo 1 são apresentadas todas as eleições associadas ao respetivo processo eleitoral, das quais o eleitor faz parte do caderno eleitoral. Para cada eleição é apresentada a seguinte informação: • Nome da eleição; • Descrição da eleição; • Período de Votação (Data de início de Data de fim); • Botão "Votar": Está ativo quando o período de votação está em curso, enquanto o eleitor não votar. Ao clicar no botão o eleitor é redirecionado para o "Passo 2". Antes da listagem de eleições é, ainda, apresentada uma mensagem informativa sobre o número total de eleições e o número de eleições que estão ainda disponíveis para votação.
REQ 4.1	Sistema de Gestão de Eleições	Pedido de criação do processo eleitoral: Dados Gerais	O responsável institucional acede ao formulário para pedido de criação do processo eleitoral através do endereço. O formulário é composto pelos passos de inserção de dados gerais e de membros. O passo dos Dados Gerais apresenta a seguinte estrutura: [Processo Eleitoral] Informação básica do processo eleitoral: • Logótipo: Dimensão mínima de 135x100px; • Identificador do processo eleitoral; • Descrição do processo eleitoral; [Eleições] Devem ser inseridas as várias eleições associadas ao processo eleitoral. Por defeito é apresentado o

			formulário de inserção de uma eleição com a seguinte estrutura: • Calendário eleitoral: Formulário de inserção dos dados do caderno eleitoral [REQ 4.2]; • Identificador da eleição (limite de caracteres: 100); • Descrição da eleição (limite de caracteres: 260); • Botão "+": Ao clicar é adicionado um novo bloco com os campos referidos acima, para que seja criada uma eleição. Ao clicar no botão "Seguinte", são submetidos os dados inseridos até ao momento e o responsável institucional passa para a criação de membros [REQ 4.3].
REQ 5.1	Integrações	Autenticação	O mecanismo de autenticação deve ser integrado com o mecanismo utilizado pela DTSI, que corresponde ao ADFS da Microsoft. No momento de login são transferidos, como parâmetros para o endpoint a fornecer pela DTSI, os seguintes dados: • Email; • Password. São recebidos os seguintes dados como resposta: • Sucesso ou Insucesso do login; • Nome do utilizador; • Número de telefone; • Forma de envio de PIN: SMS ou Email; • Foto. Apesar de o design apresentar o botão "recuperar senha", essa funcionalidade não estará disponível na plataforma. Para recuperar senha o utilizador deve comunicar diretamente com a DTSI. Os testes relativos a esta integração só podem ser efetuados na Intranet da Universidade do Minho.
REQ 6.1	Notificações	Sistema de Consultas	No sistema de consultas existem as seguintes notificações: • Envio de email com a referência de voto após uma votação; • Envio de email quando o utilizador altera o email de comunicação. É enviada uma notificação para o email antigo a informar que foi inserido um novo email de comunicação e é enviada uma notificação também para o novo email.
REQ 7.1	Mensagens	Listagem	Ao aceder à área de mensagens é apresentada, por defeito, a listagem de mensagens recebidas. Esta área a

			contém as tabs "Recebidas" e "Enviadas", apresentando o total de mensagens existentes em cada listagem. [Recebidas]: Apresenta a lista de todas as mensagens recebidas pelo utilizador autenticado; [Enviadas]: Apresenta a lista de todas as mensagens enviadas pelo utilizador autenticado. Nas listagens de mensagens, para cada mensagem é apresentada a seguinte informação: • Remetente da mensagem; • Data de envio da mensagem; • Assunto da mensagem; • Texto da mensagem: São apresentados X caracteres (Definir de forma a preencher uma linha) • Botão para responder à mensagem; • Botão para eliminar a mensagem. Ao clicar no botão para responder à mensagem, abre o formulário de submissão de mensagens [REQ 7.2] com os seguintes campos pré-preenchidos (Não editáveis): • Nome utilizador autenticado; • Email do utilizador autenticado; • Destinatário da mensagem de origem; • Assunto: Texto "Re:" seguido do assunto da mensagem de origem. Ao clicar no botão "eliminar mensagem", a mesma passa para o estado "Lixo", e deixa de aparecer na listagem visível para o utilizador. Ao clicar no assunto da mensagem o utilizador é encaminhado para uma página que apresenta a seguinte informação: • Assunto da mensagem; • Texto da mensagem completo; • Botão "Voltar": Ao clicar redireciona novamente para a lista de mensagens. No topo da listagem surge o botão "Nova", que abre uma página com o formulário de submissão de mensagens [REQ 7.2].
REQ 8.1	Sistema de Administração	Autenticação	A página de autenticação é composta por um formulário igual ao da autenticação do sistema de consultas [REQ 2.5], composto pelos seguintes campos: • Email; • Password. O mecanismo de autenticação deve estar integrado com a autenticação da DTSI [REQ 5.1].

3.2.2 Requisitos Não Funcionais

Requisitos não funcionais descrevem o modo de funcionamento do sistema, ou seja, estão centrados na forma como o sistema desempenha uma determinada função. Quando equiparados com requisitos funcionais, tendem a ser vistos como menos relevantes, mas desempenham um papel igualmente vital para o sistema, sendo, sobretudo, essenciais para o seu bom desempenho. Um requisito não funcional deve ser mensurável, ou seja, deve ser possível verificar se está ou não a ser atendido pelo software.

Na Tabela 7, apresentada de seguida, enumeram-se e descrevem-se todos os requisitos não funcionais caracterizadores da plataforma de votação eletrónica atual.

Tabela 7 - Requisitos Não Funcionais implementados no âmbito do projeto da eVotUM

Requisito	Descrição
Autenticidade	Somente pessoas com a devida permissão podem exercer o direito de voto;
Unicidade	Todo e qualquer eleitor está apto a votar uma única vez;
Anonimato	Não é possível associar um voto a um eleitor, nem associar um eleitor a um voto;
Integridade	Nenhum voto pode ser modificado ou destruído;
Irrevelável	Nenhum eleitor detém a capacidade de comprovar a matéria do voto exercido;
Verificabilidade	É possível verificar, de forma independente, que todos os votos foram contabilizados corretamente;
Auditabilidade	O sistema de votação eletrónico pode ser testado e auditado por entidades independentes;
Mobilidade	O sistema de votação eletrónico não restringe o local de votação;
Transparência	O sistema de votação eletrónico é claro, exato, preciso e seguro;
Disponibilidade	O sistema de votação eletrónico está sempre disponível durante o período de votação;

Deteção e Recuperação	O sistema de votação eletrónico deteta erros, falhas e ataques e recupera a informação até ao ponto de falha.
------------------------------	---

3.3 Infraestrutura Tecnológica da Plataforma

A caracterização da plataforma atual é dada por concluída, neste segmento final, com a descrição da infraestrutura tecnológica que lhe é própria. A descrição engloba, naturalmente, a caracterização de todas as suas componentes de Software e Hardware, a arquitetura da sua Infraestrutura e, ainda, o fluxo de comunicação que se estabelece, no processo de votação, para cada eleição.

A eVotUM é, como já foi referido, um sistema de votação eletrónica via Web, suportada, exclusivamente, por operações que envolvam um navegador Web, sendo, por isso, estabelecidas comunicações através de redes abertas, não seguras por definição. Os eleitores podem, portanto, interagir com a plataforma mediante a utilização de um browser, instalado num *desktop*, computador portátil, *tablet* ou *smartphone*. Face a esse leque de dispositivos, o sistema é capaz de adaptar a sua interface às condições de visualização e interação impostas.

A eVotUM está preparada para realizar diversas eleições em simultâneo, encontrando-se ao dispor de qualquer órgão ou unidade da Universidade do Minho em matéria de processos eleitorais. Este sistema permite, ainda, a interação com os seus utilizadores tanto em língua portuguesa como inglesa e disponibiliza um mecanismo de simulação de votação, para efeitos de demonstração e prática de utilização do sistema.

3.3.1 Componentes de Software

Estruturalmente, o sistema eVotUM é suportado por quatro tipos distintos de serviços, designadamente, o **Validator Service**, equivalente à tradicional mesa eleitora, o **Filter Service**, o **Anonymizer Service** e o **Counter Service**, equivalente à urna habitual. Estes quatro serviços constituem o Back-end do sistema e atuam como um sistema distribuído, com vista a diminuir o conluio e, ainda, dispor redundância, com vista a ser tolerante a falhas.

Todos estes serviços, envolvidos no processo de votação, armazenam *logs*, onde são registadas todas as transações. Os *logs* são utilizados na auditoria e diagnóstico de problemas em sistemas, e podem, nesse sentido, ser entendidos como provas digitais. No caso de serem detetadas anomalias ou irregularidades no sistema, é possível, através desses *logs*, verificar como decorreu o processo, eventuais tentativas de intrusão e, indiretamente, a eficácia das técnicas de segurança implementadas. O conteúdo dos *logs* nunca colocará em causa os requisitos de uma votação, nomeadamente, em termos de anonimato.

Existem, ainda, no sistema, quatro componentes de apoio, nomeadamente, o Sistema de Administração, o Sistema de Gestão de Eleições, o Sistema de Consultas e o Sistema de Votação. Na tabela 8 explana-se cada um dos componentes do sistema previamente enunciados.

Tabela 8 - Descrição detalhada dos Componentes de Software do Sistema eVotUM

Componente de Software	Descrição
Validator Service	Este serviço, equivalente à tradicional mesa eleitoral, é responsável por validar os votos dos eleitores, recolhidos através do sistema. O <i>Validator Service</i> possui, tal como a eleição, um certificado digital de chaves pública e privada. Através da chave privada, o <i>Validator Service</i> procede à assinatura do voto cifrado e cegado, que recebe do eleitor, validando-o. A assinatura, por sua vez, é guardada sem qualquer associação do voto ao respetivo eleitor. A ação do <i>Validator Service</i> termina com a devolução do voto, já assinado, ao eleitor.
Filter Service	Este serviço está localizado entre o eleitor e o <i>Anonymizer Service</i> do sistema eVotUM, e funciona como um filtro único para os votos dos eleitores, antes de os mesmos serem enviados ao <i>Anonymizer Service</i> . A sua finalidade consiste em ocultar a origem do voto, pelo que, para o <i>Anonymizer Service</i> , os votos terão todos a mesma origem. O <i>Filter Service</i> aplica, ainda, verificações fortes aos pacotes que recebe e não guarda nenhum voto ou informação relativa ao mesmo. A ação do <i>Filter Service</i> acaba com o envio do pacote para o <i>Anonymizer Service</i> .
Anonymizer Service	O <i>Anonymizer Service</i> recebe um pacote, proveniente do <i>Filter Service</i> , constituído pelo voto cifrado, e pela respetiva assinatura, proveniente do <i>Validator Service</i> . Posto isto, procede à anonimização do mesmo.

	Todos os votos dispõem de etiquetas temporais, <i>timestamps</i>, com vista à aceitação de votos, pelo Anonymizer Service, depois de findo o período de eleição, de modo a admitir votos que ainda estejam em transição no sistema e já tenham passado a fase do <i>Validator Service</i>, no período válido de votação. Este procedimento passa por receber o pacote, guardá-lo de forma aleatória e misturá-lo, de imediato, com os votos previamente recolhidos. Os votos são guardados numa estrutura, tecnologicamente não ordenada, referenciados apenas por um número aleatório, gerado quando é recebido. Tem-se, assim, um tuplo constituído por <número, pacote>, guardado em posição desconhecida. Posteriormente, a estrutura é misturada.
Counter Service	O <i>Counter Service</i> recebe os votos, misturados, do <i>Anonymizer Service</i>. Os votos podem ser enviados, para o serviço de contagem, em lotes, durante o período de eleição, ou, então, de uma só vez, no final da eleição. É, então, neste serviço que os votos são decifrados e contabilizados, no final da eleição.
Sistema de Administração	O sistema de administração constitui o instrumento através do qual o administrador da plataforma eVotUM tem permissão para gerir as páginas de conteúdo informativo e carregar os certificados utilizados pela plataforma. Algumas operações sobre o sistema eVotUM só podem ser permitidas em articulação com a comissão eleitoral, responsável por uma dada eleição. De igual modo, o armazenamento de determinadas informações, em repositórios, deve ser resistente a ataques, quer sob a forma de operações passivas ou ativas, por parte de utilizadores com perfil de administração. O papel de administrador do sistema eVotUM não deve, portanto, estar restrito a um indivíduo com a capacidade para reter o sistema.
Sistema de Gestão de Eleições	O sistema de gestão de eleições concede apoio às comissões eleitorais e, ainda, ao responsável institucional, em interfaces distintas. Para que a criação ou gestão de um processo eleitoral se torne mais intuitiva, o sistema de gestão de eleições assenta o seu funcionamento num modelo de fluxo de trabalho, <i>workflow</i>, que guia o utilizador nas diversas tarefas conexas ao ato eleitoral. O sistema eVotUM fornece, ainda, uma <i>checklist</i> que aponta à comissão eleitoral o que já foi feito em termos de preparação do ato eleitoral e o que ainda está pendente.
Sistema de Consultas	O sistema de consultas permite, ao eleitor, verificar o caderno eleitoral de uma determinada eleição, o programa das listas ou candidatos concorrentes à eleição, o calendário do processo eleitoral, bem como o correspondente regulamento. O sistema permite que qualquer eleitor possa contactar a respetiva comissão eleitoral para reclamar sobre a composição do caderno

	eleitoral, solicitar um esclarecimento ou comunicar uma anomalia, por exemplo. O eleitor pode, ainda, verificar se o seu voto foi contabilizado na eleição depois desta terminada. A verificação é feita através de um número único atribuído ao voto no momento da votação. Este número é apenas do conhecimento do eleitor e constitui a única informação exibida, sendo que a expressão do voto nunca é revelada.
Sistema de Votação	O sistema de votação é o meio através do qual o eleitor participa numa eleição, podendo expressar a sua escolha através do voto. Para que tal seja possível, o sistema requer que o eleitor se autentique no sistema, recorrendo, então, aos dados de autenticação. Uma vez efetuada a autenticação, o eleitor tem acesso à lista de eleições nas quais pode participar. Quando o eleitor seleciona uma eleição é-lhe apresentado um boletim de voto com as listas/candidatos concorrentes e, ainda, uma lista/candidato denominado “branco”, que mais não é do que a possibilidade de votar em branco. No caso de a eleição permitir resposta livre, <i>Write In</i>, surge, no boletim de voto, uma área destinada à introdução de texto livre. O boletim será, ainda, constituído por uma barra que exibe a progressão da votação até à sua conclusão. No final da votação é apresentado, ao eleitor, o número único atribuído ao seu voto, o qual deverá ser guardado para posterior verificação no sistema de consultas, após a contabilização dos votos no final da eleição.

3.3.2 Arquitetura da Infraestrutura

A eVotUM é um sistema lógico composto por várias camadas de processamento, cada uma das quais dedicada a uma função específica. Em termos de camadas físicas, cada camada descreve a configuração real do hardware, as peças de equipamento e a função de cada uma.

As componentes de hardware do sistema devem assegurar as seguintes características:

- **Disponibilidade média** de **99,9%** em períodos de votação e **90%** nos restantes períodos. Na conceção de mecanismos redundantes de alta disponibilidade pode ser feito, ou não, recurso a máquinas virtuais;
- Em situação de **anomalia grave**, designadamente, serviços da plataforma indisponíveis, inviabilizados de serem utilizados ou que não permitam satisfazer os

níveis de serviço contratados, a **recuperação do serviço**, pelo mesmo sistema, ou por um sistema redundante, deve ser feito em **menos de uma hora**;

- Em caso de falha grave, a plataforma deve dispor de mecanismos que limitem a perda de dados;
- O sistema deve ser capaz de recuperar de interrupções externas, tais como, falhas de energia ou falhas de canais de comunicação, sem que sejam perdidos dados ou integridade funcional;
- Capacidade de **processamento** mínimo de **150 votos/minuto**;
- Ocorrência em simultâneo de múltiplas eleições, com um **agregado total de trinta mil eleitores**.

A plataforma utiliza diversos tipos de servidores, que transparecem uma separação funcional lógica. O **WebServer**, também referido como servidor *Front-end*, é o nível com o qual o navegador web do utilizador comunica, e trata apenas de pedidos HTTP. Tipicamente, HTTP utiliza a porta 80, ligação não segura, e 443, ligação segura, mas pode ser configurado para utilizar outras portas. O **DBServer**, por outro lado, executa o processo da base de dados, onde os dados são armazenados, e utiliza a *Structured Query Language*, SQL, para armazenar e recuperar dados. Os **Application Servers** utilizados suportam o objetivo de dotar a plataforma de uma arquitetura orientada a serviços *Web*. A arquitetura dos *Application Servers* é, também ela, dotada de mecanismos de redundância e balanceamento de carga adequados, no sentido de assegurar altos níveis de fiabilidade e desempenho.

Através da Figura 4 é possível visualizar o diagrama lógico referente à arquitetura da infraestrutura. A figura é, também ela, exemplificativa da comunicação que se estabelece na plataforma.

NTP:

- A Firewall atualiza pelo Observatório Nacional
- Os servidores atualizam pela Firewall.

Acessos Externos:

- Utilizador Final: **https**
- Gestão da Plataforma Web: **https**
- Gestão da Infraestrutura: **ssh**
[Acesso exclusivo de IPs autorizados, com chave pública e dupla credenciação]

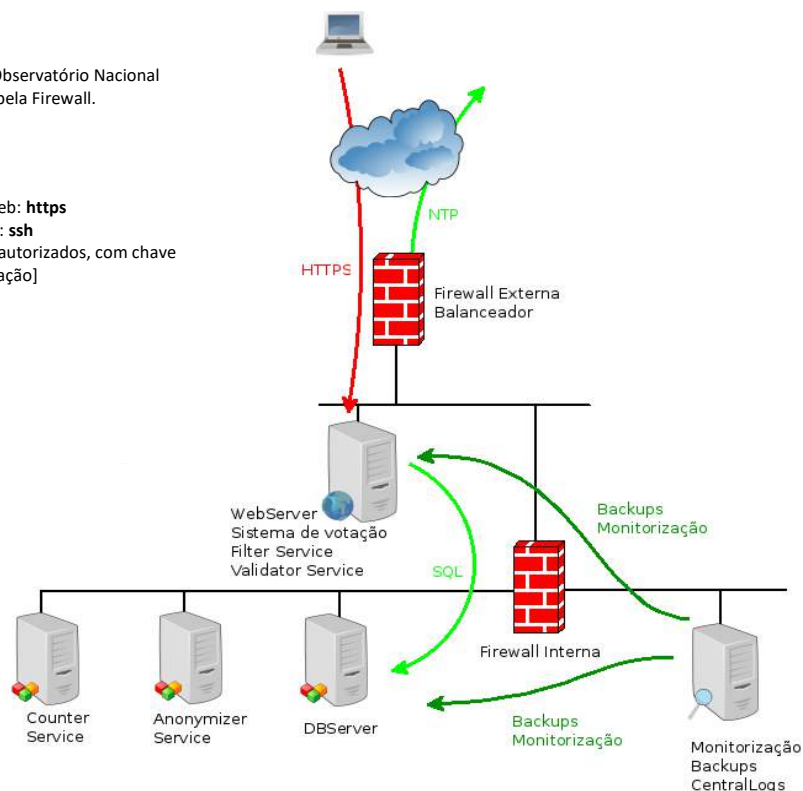


Figura 4 - Diagrama Lógico da Arquitetura da eVotUM (Arquitetura da Infraestrutura, CCG, Eurotux & Devise Futures)

No que respeita à redundância da infraestrutura física tecnológica da eVotUM, certos componentes, como Firewalls e Web Servers, são replicados e balanceados. Relativamente à base de dados, também são utilizadas tecnologias como replicação no sentido de garantir uma alta disponibilidade do serviço. De modo a garantir a alta disponibilidade do sistema, o mesmo é, então, duplicado e, na eventualidade de ocorrer uma falha, o sistema secundário assume o encargo. A redundância encontra-se de tal modo relacionada com a tolerância a falhas que o termo mais comumente empregue a um sistema dessa natureza, tolerante a falhas, é **sistema redundante** (Storey, 1996). Neste modelo, quando uma componente falha, a tarefa é enviada para componente complementar. O objetivo é, portanto, garantir a utilização ininterrupta do sistema e evitar a perda de dados.

Na Figura 5, é possível observar o diagrama referente à redundância aplicada ao sistema eVotUM. Através do recurso a máquinas virtuais, são mantidas, sempre, duas versões idênticas dos diversos servidores e Firewalls inerentes à plataforma.

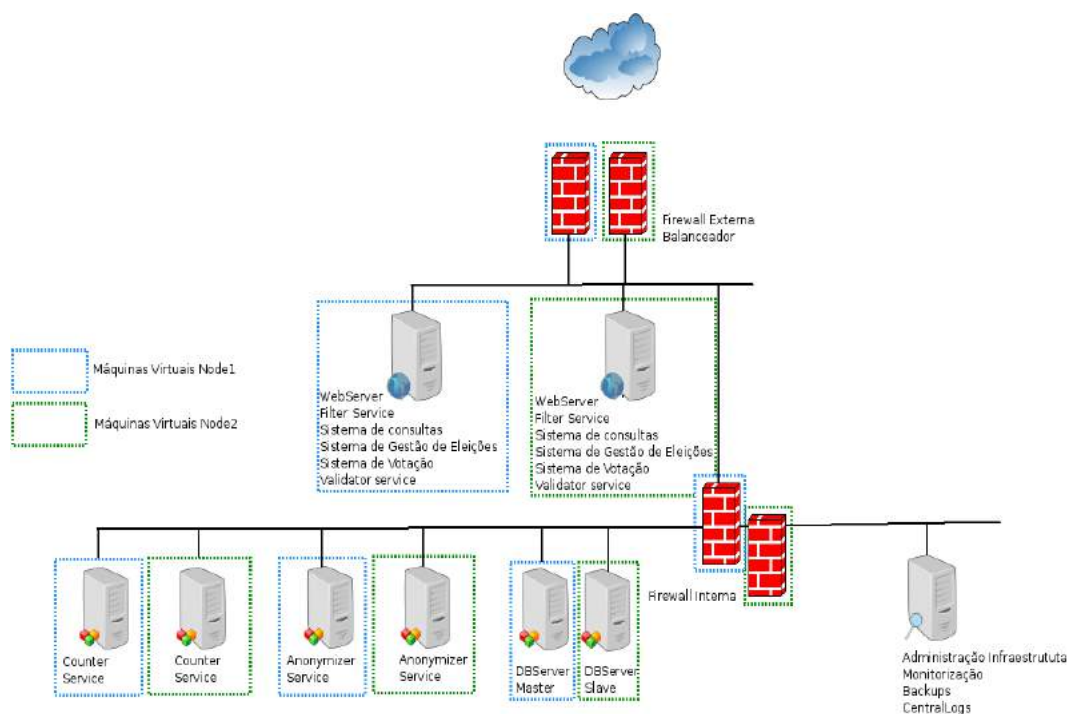


Figura 5 - Diagrama referente à redundância do sistema eVotUM (Arquitetura da Infraestrutura, CCG, Eurotux & Devise Futures)

Como também é possível averiguar, na Figura 5, o sistema contempla, ainda, um servidor de gestão, responsável por efetuar as cópias de segurança, cumprir a monitorização e manter a centralização de *logs* da infraestrutura.

Os *Backups* são efetuados a partir do servidor de gestão e enviados, cifrados, através da chave GPG, para local externo. O tempo de retenção das cópias de segurança é determinado consoante o espaço disponível, o volume de dados a salvar, a política de *Backups* e os requisitos legais. É efetuado um *Backup* total mensalmente, e um *Backup* incremental com periodicidade diária. Estes são efetuados à base de dados, aos *logs* e à aplicação Web.

A monitorização é efetuada através da plataforma *icinga*, que permite monitorizar elementos da infraestrutura e da aplicação. O sistema de monitorização da eVotUM deverá detetar eventuais anomalias, antes dessas mesmas comprometerem, significativamente, o desempenho da plataforma e, depois, deverá ativar o pedido de intervenção, através do envio de alertas, via e-mail ou SMS, para os endereços enunciados. A monitorização fornece, ainda, um conjunto de estatísticas e indicadores que servem de base à obtenção de informações relativas à operação, qualidade, segurança, eficiência e eficácia da plataforma, quer ao nível

dos elementos de rede, como de serviços e aplicações. Entre os diversos indicadores, destaca-se o *uptime* dos vários equipamentos e serviços aplicativos que constituem a plataforma.

Será importante referir que todos os sistemas, tal como o eVotUM, geram *logs* de registo de atividade, designadamente de acessos remotos, comandos executados, entre outros. Todos estes *logs* são enviados, após escrita em disco local, para um servidor central, responsável por aglomerar os registos. É, então, através da centralização de *logs* que o comprometimento de um qualquer servidor é mitigado. Os *logs* são preservados em disco WORM.

As atualizações na plataforma seguem as boas práticas, sendo, portanto, efetuadas, primeiramente, em ambiente de qualidade e, após validação, em ambiente de produção. Ademais, com vista à mitigação de ataques físicos é utilizada uma sala-cofre onde o acesso é permitido desde que N (onde $N > 1$) pessoas se encontrem na sala (custódia múltipla). Não é possível a saída de qualquer elemento da sala se não ficarem N pessoas na sala a qualquer momento. O sistema de base de dados permanece em servidor separado e sem acesso físico concorrente com os restantes servidores.

Finalmente, no que respeita à integridade da base de dados, todos os dados inseridos são assinados com HMAC, o que garante que os dados não sejam alterados pelo administrador da base de dados. É, ainda, cumprida uma separação de privilégios, ou seja, o gestor do servidor da aplicação não pode ser gestor do servidor da base de dados.

3.3.3 Fluxo de Comunicação

Cada ato eleitoral pode ser constituído por uma ou mais eleições. No processo de votação, para cada eleição, existe um fluxo de comunicação. Como se pode verificar na Figura 6, o diagrama exibido faz referência ao fluxo de comunicação que se estabelece na plataforma eVotUM aquando da realização de uma eleição.

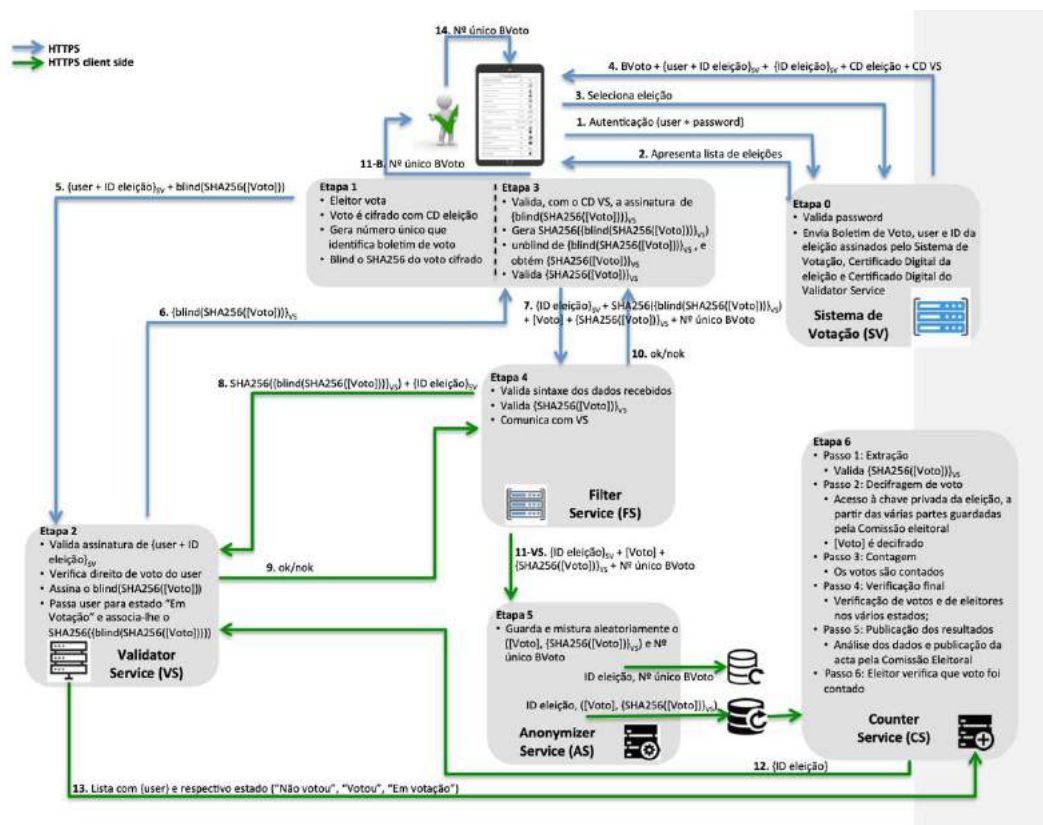


Figura 6 - Fluxo de Comunicação detalhado referente a uma Eleição no eVotUM (Fluxos de Comunicação, CCG, Eurotux & Devise Futures)

De modo a complementar a informação já ilustrada na Figura 6, serão clarificadas, na Tabela 9, cada uma das etapas do processo de votação:

Tabela 9 - Etapas referentes ao Processo de Votação numa Eleição no eVotUM

Etapa do Processo	Descrição
Etapa 0	- Para iniciar o processo de votação, o eleitor acede ao sistema eVotUM e autentica-se (<i>passo 1 da Figura 6</i>) pela introdução do user e password no Browser, que as envia ao Sistema de Votação (SV); - O SV valida a password do eleitor, e envia a lista de eleições nas quais pode participar (eleições no estado “aberta”); - O eleitor seleciona eleição a participar (<i>passo 3 da Figura 6</i>); - O Browser recebe do SV (<i>passo 4 da Figura 6</i>): - BVoto – Boletim de Voto; $\{user + ID eleição\}_{SV}$ – ‘user’ do eleitor e identificador da eleição ‘ID eleição’ do BVoto, assinado com a chave privada do SV (único modo de na Etapa 2, o Validator Service (VS) ter a certeza que quem está a votar é um eleitor que foi autenticado pelo SV para uma determinada eleição). O ‘user’ e ‘ID eleição’ são assinados em conjunto (numa estrutura json) de modo a serem fornecidos (<i>passo</i>

5 da Figura 6) ao VS. Se fossem assinados em separado, poderia ser efetuado um ataque de Denial of Service (DoS), no passo 5, enviando {user}_{SV} e {ID eleição}_{SV} que já conhecesse ao VS (a blind signature poderia ser uma string qualquer, já que o VS não tem meios para validar o seu conteúdo, sintaxe ou semântica);

- {ID eleição}_{SV} – Identificador da eleição do BVoto, assinado com a chave privada do Sistema de Votação (único modo de na Etapa 4, 5 e 6 ter a certeza que o voto pertence à eleição ‘ID eleição’);
- CD eleição – Certificado digital da eleição, necessário para cifrar o voto respeitante ao BVoto;
- CD VS – Certificado digital do VS, de modo a validar a blind signature do VS na Etapa 3.

Etapa 1

1. O Browser apresenta o boletim de voto ao eleitor, que expressa a sua intenção de voto;
 2. Após o eleitor indicar que efetuou a votação, o Browser transforma o voto para formato json, adicionando um campo com SHA256 ({user + ID eleição}_{SV}). Este campo tem como único objetivo garantir que duas cifras do voto de dois eleitores distintos que tenham votado da mesma maneira, não são iguais;
 3. O Browser interpreta o voto em json e apresenta-o ao eleitor, pedindo-lhe para confirmar a votação. A importância de o browser interpretar json e de o eleitor confirmar a votação é garantir que o voto é corretamente transformado para este formato;
 4. O voto, em formato json, é cifrado com a chave pública da eleição (passando a ser representado por [Voto]) contida no ‘CD eleição’ recebida do SV na etapa 0;
 5. É calculado o SHA256 ([Voto]), já que este será o ‘token’ sobre o qual se irá aplicar a blind signature, de acordo com a literatura das blind signatures que refere que a mesma deve ser efetuada sobre um Hash criptográfico e não sobre a mensagem original, devido a potenciais ataques que poderiam ser efetuados com sucesso se a blind signature fosse sobre a mensagem. Como vantagem adicional, o [Voto] não tem de ser comunicado ao VS;
 6. O número único que identifica o boletim de voto (designado por ‘Nº único BVoto’) é calculado como o SHA256 (SHA256([Voto]) + SHA256 ({user + ID eleição}_{SV})). Poderá ser calculado de outro modo, mas esta forma garante a aleatoriedade e unicidade desejada, não sendo possível, a partir do mesmo, estabelecer qualquer relação com o voto ou com o eleitor. Este identificador não é colocado dentro do voto cifrado, de modo que o Anonymizer Service (AS), na etapa 5, possa colocar o voto cifrado numa tabela/BD e o número único do boletim de voto noutra, não havendo, deste modo, qualquer hipótese de os relacionar após essa etapa;
 7. É aplicada a blind signature sobre o SHA256 do voto cifrado, representando-se por blind (SHA256 ([Voto]));
 8. É enviado pedido para o VS, com os seguintes dados (*passo 5 da Figura 6*):
-

-
- $\{user + ID\}_{sv}$ – de modo ao VS ter a certeza que quem está a votar é o eleitor ‘user’ que foi autenticado pelo SV para a eleição ‘ID eleição’;
 - $Blind(SHA256([Voto]))$ – blind signature que irá ser assinada pelo VS.

Etapa 2

1. O Validator Service/Mesa Eleitoral (VS) valida:
 - A assinatura de $\{user + ID\}_{sv}$;
 - Se o certificado de assinatura SV é um certificado de Sistema de Votação emitido pela hierarquia eVotUM;
 - Se o certificado de assinatura SV e o certificado raiz da hierarquia eVotUM estão dentro da validade e não foram revogados.
2. Seguidamente, o VS valida se a eleição ‘ID eleição’ está dentro do período/horário de votação e verifica o direito de voto do eleitor ‘user’ para a eleição ‘ID eleição’.
3. Caso o estado do eleitor ‘user’ na eleição ‘ID eleição’ seja “Não votou” ou se já estiver no estado “Em votação”, o estado passa a “Em votação” sendo-lhe associado a hora em que passou a esse estado.
4. O VS assina a blind signature, sendo tal representado por $\{blind(SHA256([Voto]))\}_{vs}$.
5. O VS gera o SHA256 da blind signature assinada – $SHA256(\{blind(SHA256([Voto]))\}_{vs})$ – e associa-o ao eleitor ‘user’ na eleição ‘ID eleição’. Desse modo, na etapa 4, o Filter Service (FS) utilizará este Hash para indicar que recebeu o voto cifrado do eleitor ‘user’, sem que necessite de ter conhecimento do ‘user’.
6. Na resposta ao pedido da etapa 1, é devolvida para a etapa 3 (*passo 6 da Figura 6*) a blind signature assinada pelo VS (ou código de erro apropriado).

Etapa 3

1. O Browser verifica a assinatura da blind signature assinada, verificando que foi assinada com a chave pública do CD VS recebido na etapa 0.
 2. O Browser gera o SHA256 da blind signature assinada – $SHA256(\{blind(SHA256([Voto]))\}_{vs})$ –, que será utilizada na etapa 4.
 3. É efetuado o unblind da blind signature assinada, obtendo-se neste passo o SHA256 do voto cifrado assinado pelo VS, i.e., $unblind(\{blind(SHA256([Voto]))\}_{vs}) = \{SHA256([Voto])\}_{vs}$.
 4. O Browser utiliza o $SHA256([Voto])$ calculado na etapa 1 e o certificado CD VS recebido na etapa 0, para verificar a assinatura de $\{SHA256([Voto])\}_{vs}$.
 5. É enviado pedido para o Filter Service (FS), com os seguintes dados (*passo 7 da Figura 6*):
 - $\{ID\}_{sv}$ – de modo ao FS ter a certeza que o BVoto pertence à eleição ‘ID eleição’;
 - $SHA256(\{blind(SHA256([Voto]))\}_{vs})$ – a ser utilizado pelo FS na comunicação com o VS;
 - $[Voto]$ – que FS irá reencaminhar para o AS;
 - $\{SHA256([Voto])\}_{vs}$ – que FS irá reencaminhar para o AS;
 - No único BVoto – que FS irá reencaminhar para o AS.
-

Etapas 4

1. O FS começa por efetuar várias verificações sintáticas e semânticas ao pedido que recebe do Browser:
 - Valida a correção sintática do pedido recebido do browser, em termos de estrutura e formato do pedido;
 - Verifica a assinatura de $\{ID\}_{sv}$, assim como se o certificado de assinatura SV é um certificado de Sistema de Votação emitido pela hierarquia eVotUM e se o certificado de assinatura SV e o certificado raiz da hierarquia eVotUM estão dentro da validade e não foram revogados;
 - Calcula a SHA256 do [Voto] e verifica se a mesma coincide com a SHA256 contida em $\{SHA256([Voto])\}_{vs}$;
 - Verifica a assinatura de $\{SHA256([Voto])\}_{vs}$, assim como se a assinatura VS é um certificado de Validator Service emitido pela hierarquia eVotUM e se o certificado de assinatura VS e o certificado raiz da hierarquia eVotUM estão dentro da validade e não foram revogados.
 2. O FS envia $\{ID\}_{sv}$ e $SHA256(\{blind(SHA256([Voto])\})_{vs})$ a VS (*passo 8 da Figura 6*). VS valida se na eleição 'ID eleição' existe um $SHA256(\{blind(SHA256([Voto])\})_{vs})$ que esteja no estado "Em votação" há menos de dois minutos. Caso tal ocorra, VS muda estado para "Votou" e responde ok a FS (caso contrário responde código de erro apropriado), conforme *passo 9 da Figura 6*. Esta comunicação entre FS e VS é necessária para ultrapassar eventuais problemas na quebra de acesso à Internet do dispositivo utilizado pelo eleitor para votar, depois da etapa 1 e antes da etapa 4. Caso isso ocorresse, e esta comunicação não existisse, o voto não seria contabilizado (não seria efetuado o *passo 7 da Figura 6*), mas o eleitor já não poderia voltar a tentar votar novamente (para o VS, o eleitor já teria votado). De modo a isso não acontecer, e para além desta comunicação entre o FS e VS, existem 3 estados de votação (no VS) por eleitor:
 - "Não votou";
 - "Em votação" – durante após o *passo 6 da Figura 6*. Se esta comunicação for efetuada passado o prazo estabelecido, VS responde com código de erro apropriado, de modo que FS a reencaminhe para o Browser do eleitor onde irá aparecer uma mensagem inteligível, i.e., "Excedeu o tempo máximo de votação. Volte a votar";
 - "Votou" – quando o VS recebeu esta comunicação, durante o tempo máximo de "Em votação".
 3. O FS reencaminha para Browser (*passo 10 da Figura 6*) a resposta do VS, e caso esta seja positiva, Browser apresenta ao eleitor (e envia-lhe por correio eletrónico) o número único que identifica o boletim de voto ('No único BVoto'), conforme *passo 11-B da Figura 6*. Caso a resposta de VS não seja positiva, o Browser apresenta a mensagem de erro adequado ao eleitor e o FS finaliza o processamento do pedido.
 4. É enviado pedido para o Anonymizer Service (AS), com os seguintes dados (*passo 11-VS da Figura 6*):
 - $\{ID\}_{sv}$;
 - [Voto];
-

-
- {SHA256([Voto]))_{VS};
 - No único BVoto.

Etapas 5

1. O Anonymizer Service (AS) guarda (e mistura aleatoriamente) o [Voto] e o {SHA256([Voto]))_{VS} numa tabela (da Urna eleitoral) para a eleição 'ID eleição' e, guarda (e mistura aleatoriamente) o 'Nº único BVoto' noutra tabela (da Urna eleitoral) para a eleição 'ID eleição'. A mistura aleatória é efetuada do seguinte modo:
 - Antes do início da eleição é criada tabela na Urna eleitoral (uma para o voto e outra para o número único do boletim de voto) com o triplo de entradas em relação aos votantes totais da eleição;
 - De cada vez que chega um "pacote" para lá colocar é gerado um número aleatório entre 1 e o número de entradas na tabela, que corresponde à linha onde colocar o "pacote";
 - Se nessa linha já tiver sido colocado um "pacote", volta-se ao passo anterior, até se encontrar uma linha que não tenha nenhum "pacote";
 - De referir que são gerados números aleatórios diferentes para cada tabela, de modo ao voto ser colocado na linha ditado por um número aleatório, e o número único ser colocado na linha ditada por outro número aleatório.

Etapas 6

1. **Extração:**
O CS verifica, neste passo, a assinatura e integridade dos votos cifrados e, para tal:
 - Calcula a SHA256 do [Voto] e verifica se a mesma coincide com a SHA256 contida em {SHA256([Voto]))_{VS};
 - Verifica a assinatura de {SHA256([Voto]))_{VS}, assim como se a assinatura VS é um certificado de Validator Service emitido pela hierarquia eVotUM e se o certificado de assinatura VS e o certificado raiz da hierarquia eVotUM estão dentro da validade e não foram revogados.
 2. **Decifragem de voto:**
São, neste segundo passo, decifrados todos os votos da eleição e, portanto:
 - É gerada a password de acesso à chave privada da eleição, a partir das várias partes guardadas pela Comissão eleitoral;
 - O voto é decifrado;
 - É validada a estrutura json do voto.
 3. **Contagem:**
No terceiro passo todos os votos são contabilizados, apurando-se o resultado.
 4. **Verificação final:**
É efetuada, neste passo, uma verificação da eleição, que será disponibilizada, no passo seguinte, à Comissão eleitoral, para análise. A verificação final consiste em:
 - Obter a quantidade de eleitores, desta eleição, nos vários estados ("Não votou", "Votou", "Em votação"). Para tal, o CS comunica com o VS, conforme *passos 12 e 13 da Figura 6*;
-

-
- Quantificar os dados obtidos no passo 1 (Extração) e passo 2 (Decifragem de voto), incluindo número de votos recebidos, com/sem assinatura do VS correta, com/sem SHA256 do [Voto] coincidente com a SHA256 contida em $\{SHA256([Voto])\}_{vs}$, decifrados (ou não) corretamente, com/sem estrutura json válida.

5. Publicação dos resultados:

No quinto passo são disponibilizados os dados do passo 4 para análise pela Comissão Eleitoral. Adicionalmente, é disponibilizado um Template da ATA à Comissão Eleitoral, com os dados do passo 3 pré-preenchidos, de forma a poder ser elaborada e assinada. No final da assinatura da ATA, a Comissão Eleitoral altera o estado da eleição para “Eleição fechada”.

6. Verificação de voto:

Após a eleição estar no estado “Eleição fechada”, o eleitor pode verificar se o seu voto foi contabilizado (através do número único que identifica o boletim de voto), conforme *passo 14 da Figura 6*.

CAPÍTULO 4

ESPECIFICAÇÃO DA PLATAFORMA FUTURA – eVotUM light

No decorrer do presente capítulo é efetuada a caracterização detalhada da arquitetura da futura plataforma de votação eletrônica, adaptada, portanto, ao novo contexto de votação em reuniões. Especificá-la passa, então, por descrever um variado conjunto de atributos que lhe são característicos e, nesse sentido, o capítulo começa por introduzir uma visão integral da plataforma e, posteriormente, subdivide-se em três lógicas distintas, designadamente, comportamento funcional, comportamento dinâmico e infraestrutura tecnológica inerentes à plataforma.

Numa primeira instância, é, ainda, vital recapitular a motivação e importância inerentes à especificação de uma nova plataforma, isto é, o móbil da dissertação. Como tal, é importante referir a necessidade de serem promovidas votações, em tempo real, em contexto de reuniões integralmente remotas, integralmente presenciais ou, essencialmente, híbridas, isto é, com ambas as modalidades em simultâneo, uma vez que a realidade atual é muito pouco ajustada para o efeito. A plataforma de votação eletrônica eVotUM, caracterizada no capítulo prévio, foi, como se pôde constatar, projetada para suportar votações que obedecem a um profuso e rigoroso conjunto de fases de um processo eleitoral, fases essas que são, no novo contexto de votação idealizado, desnecessárias. Identificou-se, então, a oportunidade de reimplementar a plataforma existente, com todas as alterações imprescindíveis à materialização da eVotUM *light*, reaproveitando algumas das componentes já desenvolvidas, simplificando as interfaces e ajustando todo o processo eleitoral.

4.1 Visão Integral da Plataforma

Nesta primeira fase, de caracterização da plataforma eVotUM *light*, é importante começar por apresentar uma visão integral do que será a plataforma e, como tal, é especificado quem serão os seus intervenientes, isto é, quem irá interatuar com a mesma. Posteriormente, são discriminadas matérias referentes ao processo de votação por parte do votante, à criação e

gestão da votação por parte do secretário da reunião, ao tipo de votações autorizadas, entre outras. É, portanto, descrito, de forma concisa, o propósito desta nova plataforma, quais as suas funcionalidades, e quem intercede em cada uma das mesmas.

4.1.1 Intervenientes

Os agentes que podem interatuar com o sistema eVotUM *light* desempenham funções diferenciadas e dispõem de restrições de acesso igualmente distintas, sendo importante clarificar quem são esses intervenientes e quais os papéis que desempenham na plataforma. Na tabela 10 são enumerados tais intervenientes e descrita a função que lhes compete desempenhar.

Tabela 10 - Intervenientes na Plataforma eVotUM light

Interveniente	Descrição
Secretário	Responsável por criar a votação, uma vez autenticado no Sistema de Gestão de Votações. A definição de parâmetros referentes à votação, tais como candidatos, lista de participantes, bem como a configuração do tipo de votação e boletim, são exemplos de atividades ao seu encargo. Este é, ainda, responsável pela gestão da votação, encarregue, portanto, de autorizar a sua abertura e respetivo fecho. Tem, nesse sentido, acesso a um painel de Gestão de Operações da Votação, onde é possível: • Adicionar e/ou remover elementos da lista de participantes na votação; • Autorizar abertura da votação; • Verificar, em período de votação, número de votos em urna; • Autorizar encerramento da votação; • Autorizar escrutínio dos votos e apresentação de resultados.
Votante	Utilizador que, uma vez autenticado no Sistema de Votação, está apto para: • Alterar informação referente a dados pessoais, nomeadamente, e-mail, telemóvel, e modo de envio de chave de segurança; • Participar nas votações das quais faz parte da lista de participantes, caso estejam dentro do período de votação; Verificar se o seu voto foi contabilizado na votação, através da introdução da referência de votação.

Administrador	O administrador é meramente responsável pelo carregamento inicial dos certificados digitais a utilizar pelo sistema. Não desempenha, portanto, um papel ativo no funcionamento da plataforma, isto é, não administra, efetivamente, a sua utilização.
----------------------	---

Contrariamente à eVotUM, esta nova plataforma irá interatuar com um número bastante reduzido de agentes, uma vez que os principais intervenientes são, apenas, o Secretário da reunião e o Votante. O Secretário é, neste caso, responsável pela criação e, ainda, gestão da votação. Sendo este um novo contexto de votação, mais intimista, o papel a desempenhar pelo Secretário da reunião é bastante mais abrangente do que aquele praticado na eVotUM tanto pelo Responsável Institucional como por qualquer elemento da Comissão Eleitoral. A sua função começa pela criação da votação, isto é, tipo de votação, lista de candidatos e, por fim, lista de participantes. A lista de participantes na votação representa a lista de presenças na reunião, existindo, portanto, a necessidade de a manter atualizada no decorrer da reunião. Finalmente, a função do Secretário deverá passar pela gestão da votação, isto é, autorização de abertura e fecho da mesma, análise de votos em urna durante o período de votação e, ainda, autorização de contagem dos votos e respetiva publicação de resultados. O participante na reunião será, por sua vez, convocado pelo Secretário do Conselho Geral a participar na votação enquanto votante. O votante poderá alterar os seus dados pessoais, participar na votação e, ainda, conferir a contabilização do seu voto através da referência de votação, sendo que terá de votar, necessariamente, num dos candidatos apresentados, uma vez que o voto em branco não é, neste novo contexto, autorizado. No caso de o votante não consentir nenhuma das alternativas, terá de comunicar com o Secretário do Conselho Geral que, previamente à votação, o removerá da lista.

4.1.2 Processo de Votação pelo Votante

Para participar numa votação através da plataforma de votação eletrónica eVotUM *light*, o votante necessita de satisfazer determinadas pré-condições. Para esclarecer, integralmente, o processo associado à votação, são descritos, na Tabela 11, todos os passos que o constituem.

Tabela 11 - Passos referentes ao Processo de Votação pelo Votante

Passo	Descrição
1. Autenticação	O votante autentica-se no sistema eVotUM <i>light</i> , através das credenciais que lhe foram atribuídas, sendo-lhe apresentadas todas as votações, às quais foi convocado, disponíveis;
2. Seleção de Votação	Se, da lista de votações disponíveis exibida ao votante, alguma estiver em período de votação, é-lhe exibido o botão “Votar”, a partir do qual terá acesso ao painel de votação;
3. Votação	A votação é constituída por cinco passos: • Seleção da lista/candidato em quem pretende votar; • Confirmação da lista/candidato selecionada/o; • Seleção do segundo método de autenticação na votação; • Apresentação da informação de submissão de voto, incluindo a referência de votação (enviada por correio eletrónico).
4. Verificação de Referência de Votação	À posteriori, após o encerramento das urnas, o votante poderá verificar se o seu voto foi contabilizado, verificando se a sua referência de votação se encontra nas referências de votação processadas. Esta é, portanto, uma etapa opcional, estando ao encargo do votante certificar-se de que a sua participação na eleição foi contabilizada.

Contrariamente ao que acontecia na eVotUM, na nova plataforma, não existem processos eleitorais, pelo que o votante não terá de selecionar, inicialmente, o processo em que insta participar. Neste caso, o votante avança uma etapa e seleciona, apenas, uma eleição, de entre as que tem ao seu dispor. Posto isto, em semelhança ao que já acontecia na plataforma atual, o votante seleciona a lista/candidato em quem intenta votar, confirma a sua escolha e, para concluir a votação, efetua uma segunda autenticação. Embora aparentemente irrisório, a verificação da Referência de Votação é passível de ser feita, na nova plataforma, pelo votante. No entanto, neste novo contexto não se vê grande utilidade no uso da funcionalidade de verificação, dado que, na prática, a votação só é concluída após a efetivação do voto por todos os seus participantes.

4.1.3 Processos de Criação e Gestão da Votação pelo Secretário

A criação de uma votação é efetuada pelo Secretário da Reunião, depois de autenticado na plataforma eVotUM *light*. A criação da votação passa, então, por definir uma sequência de parâmetros, designadamente:

- **Dados Gerais:** logótipo, identificador e respetiva descrição da votação;
- **Tipo de Votação:** por *default* é imposta a seleção de uma votação universal, isto é, a seleção, por parte do votante, de um, e apenas um, candidato entre os demais. As restantes configurações, passíveis de serem aplicadas a uma votação, poderão ser instituídas, apesar de não estarem pré-definidas. É ainda, neste passo, imposto, por *default*, o nível de segurança mínimo para as ações a desempenhar aquando da gestão da votação, uma vez que o único membro autorizado para desempenhar qualquer funcionalidade, no sistema, é o Secretário;
- **Participantes:** convocação dos membros do Conselho Geral, isto é, membros da reunião a efetuar, com permissão para participar na votação.

O processo de criação de uma votação tem ainda um **conjunto de considerações** a ter em conta, nomeadamente:

- Aquando da criação de uma votação, toda e qualquer data de fim, a definir, terá de ser, necessariamente, posterior à data de início do respetivo período;
- O Secretário da reunião é o responsável pela inserção da lista de participantes da votação;
- Os membros a nomear como parte integrante da lista de votantes têm de constar da lista de utilizadores do Serviço de Diretoria patente;
- O Secretário da reunião é configurado, automaticamente, pelo sistema eVotUM *light*, como responsável pela abertura e fecho da votação;
- Após a criação e submissão da votação, o Secretário tem de efetuar uma segunda autenticação através da Chave Móvel Digital;

- O sistema eVotUM *light* gera, automaticamente, chaves de cifra e de decifra para cada eleição. A password de acesso à chave de decifra é enviada ao Secretário através do correio eletrónico;

A gestão da votação, por outro lado, efetuada também ela pelo Secretário da reunião, é composta por uma série de passos, enumerados, de seguida, na Tabela 12.

Tabela 12 - Passos referentes ao Processo de Gestão da Votação

Passo	Descrição
1. Abertura da Votação	Autorizar o início da votação a todos os participantes.
2. Controlo de Votos em Urna	Verificar o número de total de votos, em urna, durante o período de votação.
3. Fecho da Votação	Autorizar o encerramento da votação, uma vez recolhidos os votos de todos os participantes na mesma.
4. Escrutínio de Votos	Autorizar o escrutínio de votos em urna, dada a votação por encerrada.
5. Apresentação de Resultados	Publicar, na plataforma, os resultados obtidos na votação, designadamente, o número de votos atribuídos a cada candidato e, naturalmente, qual o eleito.

Na eVotUM *light*, o processo de gestão começa com a permissão de abertura da votação, tendo sido previamente retificada a presença de todos os participantes na respetiva reunião. Iniciada a votação, o Secretário controla o número de votos em urna e aguarda até que todos os intervenientes tenham emitido o respetivo voto. Posto isto, reunidas todas as condições, o Secretário autoriza o fecho da votação e o escrutínio dos votos, respetivamente. O sistema determina, de imediato, a maioria absoluta, referente ao proponente com maior percentagem de votos, ou seja, o candidato que reúne, pelo menos, metade do número total de votos mais um. Dada a natureza da votação, do tipo universal, são apresentados os resultados, e eleito o candidato com maioria. Por fim, efetuados os passos previamente enumerados, a eleição é arquivada, tal como descrito no próximo ponto 4.1.5.

4.1.4 Tipos de Votação Autorizados

A plataforma de votação eletrônica eVotUM *light* deve estar preparada para consagrar alguma variedade de eleições. No entanto, dado o propósito da mesma, de suporte expedito de votações de pequenos grupos, o tipo de eleição definido, por default, aquando da criação da votação, é universal. Por universal entende-se uma votação com, apenas, dois candidatos, não sendo, ainda, exequível o exercício do voto em branco. Todas as outras configurações disponíveis na eVotUM são, neste contexto, dispensáveis, salvo exceções.

Posto isto, a eventual configuração de parâmetros está, pois, ao encargo do Secretário da reunião. Na Tabela 5, apresentada no capítulo anterior, são enumeradas as configurações passíveis de serem aplicadas numa eleição.

4.1.5 Arquivo da Votação

A votação é arquivada, de forma automática, finalizada a votação, ocorrendo o seguinte:

- A votação passa para o estado Arquivado;
- Todos os dados de votação são apagados do sistema. É apagado o estado da votação no *Validator Service*, os votos guardados e decifrados no *Counter Service* e a referência de votação guardada no *Anonymizer Service*.

Toda a informação remanescente à votação continua a poder ser acedida pelo Votante e pelo Secretário, na plataforma.

4.2 Comportamento Funcional da Plataforma

A plataforma de votação eletrônica futura, versão *light* da eVotUM, pode ser caracterizada através de uma especificação funcional do seu comportamento, que consiste, essencialmente, na enunciação dos requisitos funcionais e não funcionais a implementar no âmbito do projeto

e, ainda, dos casos de uso associados à interação com a plataforma, recorrendo, para tal, à ferramenta de especificação UML. A linguagem UML é utilizada para modelar e documentar as diversas fases do desenvolvimento do sistema e, nesse sentido, define uma série de elementos gráficos, utilizados em diferentes diagramas, para representar as componentes do sistema, as suas interações e potenciais mudanças de estado. Trata-se, portanto, de uma linguagem de modelação única, cujo papel é facilitar a visualização dos diversos aspetos da plataforma e, por conseguinte, a compreensão do seu funcionamento. Os diagramas vão, neste contexto, oferecer uma visão padronizada da plataforma e das suas especificações, auxiliar na visualização do funcionamento do software e servir a fase inicial de especificação dos requisitos do sistema.

4.2.1 Requisitos a Implementar

Como inicialmente referido, a eVotUM ainda não oferece uma solução devidamente adaptada a um contexto de votação em reuniões, quer em formato online, presencial ou, sobretudo, híbrido, crucial na realidade vivida, hoje, em qualquer organização ou instituição. Como tal, neste capítulo é especificada uma nova solução, dedicada a votações nesse novo contexto, através de uma adaptação da plataforma existente, preservando características como a rapidez, fácil utilização e alta segurança, que já detém.

Nesse sentido, é necessário realizar, nesta fase, um levantamento dos requisitos funcionais e não funcionais indispensáveis à plataforma, cingida ao novo contexto de votação. Deste levantamento deve resultar a especificação de uma nova plataforma, consequente de uma simplificação e apropriação das componentes atualmente existentes. O resultado é, então, a especificação de uma nova versão da eVotUM, a eVotUM *light*, para contextos de votação híbridos, em reuniões, por parte de pequenos grupos.

4.2.1.1 Requisitos Funcionais

Requisitos funcionais pormenorizam comportamentos específicos que o software tem de ser capaz de satisfazer, ou seja, são requisitos que especificam o que sistema deve fazer.

Os principais requisitos funcionais a implementar no âmbito do desenvolvimento da plataforma eVotUM *light*, são enunciados na Tabela 13, segundo as suas respetivas categoria e subcategoria, e aliados a uma descrição pormenorizada. No **anexo V**, passível de ser consultado no final do presente documento, são especificados todos os requisitos.

Tabela 13 - Requisitos Funcionais da eVotUM Light

Requisito	Categoria	Subcategoria	Descrição
REQ 3.1	Sistema de Votação	Passo 1: Selecionar Votação	O votante ao clicar no botão "votar" que surge na listagem das votações, é redirecionado para a área de votação. O sistema de votação é constituído por 5 passos [REQ 3.1 a REQ 3.6]. No passo 1 são apresentadas todas as votações, das quais o votante faz parte. Para cada votação é apresentada a seguinte informação: • Nome da votação; • Descrição da votação; • Botão "Votar": Está ativo quando o período de votação está em curso, enquanto o votante não votar. Antes de surgir a listagem é, ainda, apresentada uma mensagem informativa sobre o número total de votações e o número de votações disponíveis no momento.
REQ 3.2	Sistema de Votação	Passo 2: Selecionar Candidato	Neste passo, é apresentado o boletim de voto e o votante escolhe o candidato em que pretende votar.
REQ 3.3	Sistema de Votação	Passo 3: Confirmar Candidato	Neste passo o votante deve confirmar a escolha de candidato efetuada, existindo apenas para efeitos de validação.
REQ 3.4	Sistema de Votação	Passo 4.1: Segurança – Selecionar Método de Envio de Código PIN	Neste passo deve ser feita a seleção do mecanismo de envio do PIN de votação, sendo apresentado um formulário para esse efeito. Por defeito surge a opção que estiver inserida nos dados pessoais do votante. Após a seleção, o votante deve clicar no botão "Continuar" e é enviado, automaticamente, o PIN de votação.

REQ 3.5	Sistema de Votação	Passo 4.2: Segurança - Inserir Código PIN	Neste passo é apresentado o formulário onde deve ser inserido o PIN de votação recebido. Ao clicar em "Submeter Voto" o votante finaliza o processo de votação. Neste momento é enviado um email para o votante com a sua referência de votação.
REQ 3.6	Sistema de Votação	Passo 5: Recolher Referência de Votação	Neste passo é apresentada a referência de votação do votante. Ao clicar em "OK" a votação em questão deixa de estar ativa, ficando o botão "Votar" bloqueado e sendo atualizado o número de votações ativas.
REQ 4.1	Sistema de Gestão de Votações	<u>Criação</u> da Votação: Passo 1 – Inserir Dados Gerais	O Secretário, responsável pela criação da votação, é, no Passo 1, obrigado a preencher os Dados Gerais, que apresentam a seguinte estrutura: • Identificador da votação: dois campos de texto simples para inserir a informação em português e em inglês (limite de caracteres: 100); • Descrição da votação: dois campos de texto simples para inserir a informação em português e em inglês (limite de caracteres: 260);
REQ 4.2	Sistema de Gestão de Votações	<u>Criação</u> da Votação: Passo 2 – Selecionar Tipo de Votação	No passo 2 são efetuadas as configurações gerais da votação. Este passo é composto pelos seguintes campos: [Default] • Limite de escolhas assinaláveis: Por defeito o limite está definido para uma única opção; • Write in: Por defeito está preenchida com a opção "Não"; • Votação Ordenada: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção "Não"; • Peso dos votos: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção "Não"; • Método de Hondt: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção "Não".
REQ 4.3	Sistema de Gestão de Votações	<u>Criação</u> da Votação: Passo 3 – Inserir Lista de Participantes	No passo 3 é feita a inserção dos votantes que fazem parte da lista de presenças da reunião. Esta inserção é feita através da importação de um ficheiro, com formato CSV, que deve conter os seguintes dados: • Número de identificação; • Nome; • Email; • Telemóvel; O sistema valida, para cada votante, que:

			• O email está bem formado; • Não existem dois votantes com o mesmo email; • Os números de identificação (alfanumérico) são únicos;
REQ 4.4	Sistema de Gestão de Votações	<u>Criação</u> da Votação: Passo 4 – Inserir Candidatos	No passo 4 são inseridos os candidatos concorrentes à votação. Os dados associados são: • Nome; • Informação adicional; Este passo é composto por um formulário que apresenta por defeito uma linha com os seguintes campos vazios: • Designação; • Documentos: É possível adicionar mais do que um documento e para cada documento deve ser inserida a designação associada. Deve ser possível eliminar e trocar a ordem dos documentos, que será a ordem com a qual serão apresentados no sistema de consultas; • Botão para adicionar novos documentos; • Botão para eliminar o candidato. Ao clicar no botão "+" é adicionada uma nova linha com os campos referidos acima, para que sejam preenchidos os dados de um novo candidato.
REQ 4.5	Sistema de Gestão de Votações	<u>Criação</u> da Votação: Passo 5 – Configurar Boletim de Voto	No passo 5 é feita a configuração do boletim de voto. Os dados a configurar são os seguintes: • Instruções a constar no boletim de voto: dois campos de texto simples para preencher em português e em inglês; • Apresentação dos candidatos: Radio button com as opções Lista e Dropdown; • Ordenação dos candidatos: Apresentados todos os candidatos e o Secretário pode escolher a posição em que cada um é apresentado. Para além da gestão manual da ordem dos candidatos deve existir um botão para gerar aleatoriamente a ordem dos candidatos. Ao clicar no botão "Pré-visualizar boletim" é apresentada uma janela pop-up com a representação do boletim de voto que irá surgir no sistema de votação.
REQ 4.7	Sistema de Gestão de Votações	<u>Gestão</u> da Votação: Passo 1 – Autorizar Abertura de Votação	No Passo 1, através do Painel de Gestão da Votação, o Secretário tem permissão para dar começo à votação, através do botão "Iniciar Votação". Nestas circunstâncias, de votação em contexto de reuniões, não existem calendários eleitorais, isto é, períodos de votação pré-

			definidos, pelo que apenas o Secretário tem autoridade para decidir quando se dará início à votação.
REQ 4.8	Sistema de Gestão de Votações	<u>Gestão</u> da Votação: Passo 2 – Controlar Votos em Urna	No Passo 2, através do Painel de Gestão da Votação, o Secretário pode observar o número de votos já em urna, em tempo real. Nesta tab, o Secretário tem oportunidade de analisar o número de votos já efetuados e o número de votos por efetuar, o que lhe permite perceber quando avançar para o fecho da votação.
REQ 4.9	Sistema de Gestão de Votações	<u>Gestão</u> da Votação: Passo 3 – Autorizar Fecho de Votação	No Passo 3, através do Painel de Gestão da Votação, o Secretário tem permissão para dar fecho à votação, através do botão “Terminar Votação”. Nestas circunstâncias, de votação em contexto de reuniões, não existem calendários eleitorais, isto é, períodos de votação pré-definidos, pelo que apenas o Secretário tem autoridade para decidir quando se dará termo à votação. Através do controlo de votos em urna, no Passo 2, o Secretário tem perceção do número de votos já efetuados e, no caso desse número corresponder à totalidade de votantes, poder-se-á finalizar a votação.
REQ 4.10	Sistema de Gestão de Votações	<u>Gestão</u> da Votação: Passo 4 – Autorizar Escrutínio de Votos	No Passo 4, através do Painel de Gestão da Votação, o Secretário tem permissão para dar início ao escrutínio dos votos. Nesta tab, o Secretário terá, portanto, de clicar no botão “Iniciar Escrutínio de Votos” para que se dê o processo. Posto isto, o resultado da votação é apresentado, no painel, ao Secretário da Reunião.
REQ 4.11	Sistema de Gestão de Votações	<u>Gestão</u> da Votação: Passo 5 – Autorizar Publicação de Resultados	Por fim, no Passo 5, através do Painel de Gestão da Votação, o Secretário tem autorização para publicar o resultado da votação na plataforma. Nesta tab, o Secretário terá, portanto, de clicar no botão “Publicar Resultados” para que se dê o processo. Posto isto, o resultado da votação é apresentado, na plataforma, a todos os participantes.

4.2.1.2 Requisitos Não Funcionais

Requisitos não funcionais, como já referido no capítulo anterior, descrevem o modo de funcionamento do sistema, ou seja, estão centrados na forma como o sistema desempenha uma determinada função. Na eVotUM *light* devem ser asseguradas propriedades semelhantes às apontadas, na literatura, para sistemas de votação. Nesse sentido, e embora a realização

de votações neste novo contexto exija um nível de complexidade e segurança relativamente inferior, as propriedades mantêm-se as mesmas que já haviam sido apresentadas para a eVotUM, tal como podem ser observadas na tabela 7 do capítulo prévio.

4.2.2 Casos de Uso

O UML trata-se de uma ferramenta de documentação e modelação de sistemas e, nesse sentido, define elementos gráficos, por forma a representar as diversas componentes que os constituem, as suas respetivas interações e, ainda, eventuais mudanças de estado, com o objetivo de facilitar a compreensão do funcionamento de tais sistemas em especificação. Trata-se, portanto, de uma linguagem padrão, objetiva, eficiente e entendida por todos.

Diagramas desta natureza auxiliam na obtenção de uma visão clara e única do sistema em análise e são essenciais na prevenção de erros intrínsecos à fase de especificação do projeto, bem como de erros de comunicação estabelecidos entre as diversas partes envolvidas. Diagramas UML encontram-se subdivididos em duas categorias distintas, designadamente, estruturais e comportamentais, sendo a primeira responsável pela modelação de aspetos estáticos do sistema e a segunda, por sua vez, responsável pela especificação do seu comportamento face a determinadas interações.

O diagrama de Caso de Uso constitui, assim, um exemplo de diagrama comportamental, indispensável na medida em que, através do seu aproveitamento, os requisitos funcionais do projeto podem ser apresentados num novo formato, o que permite, em última análise, visualizar todo o sistema mais facilmente, através de diagramas padronizados, dotados de uma notação gráfica inteligível. Os casos de uso explicam o que irá acontecer aquando da interação do utilizador com o sistema, ou seja, expõem os requisitos do ponto de vista do utilizador final e representam as diferentes utilizações que esse mesmo pode exercer no sistema. Os atores são, por sua vez, utilizadores que interagem com o sistema. Um ator pode ser uma pessoa, um outro sistema, ou, até mesmo, tempo, que interage com a aplicação ou sistema, devendo ser, portanto, um objeto externo que produz ou consome dados. Deste modo, um caso de uso pode ser definido como uma sequência de eventos, e interações com o sistema, que produzem um resultado de valor para o ator.

De uma perspetiva funcional, são estabelecidos, essencialmente, dois tipos de interação com a eVotUM *light*, referentes à comunicação que se institui entre a mesma e os seus dois principais atores. Tais interações correspondem, pois, à comunicação entre o Secretário da Reunião e a plataforma e, ainda, entre o Votante e a plataforma.

De modo a melhor compreender tais interações, previamente especificadas na Tabela 13 referente aos requisitos funcionais do projeto, são agora ilustradas, através de diagramas de Caso de Uso, as relações que se estabelecem entre a eVotUM *light* e os seus intervenientes, o que permite, pois, visualizar todo o sistema mais facilmente.

4.2.2.1 Autenticação do Utilizador na eVotUM *light*

Inicialmente, é retratado, também recorrendo a um diagrama de Caso de Uso, o processo de autenticação que se sucede na plataforma por parte dos seus utilizadores [Figura 7]. Embora ambos obedeçam a um mesmo processo de autenticação, são, posteriormente, encaminhados para sistemas distintos.

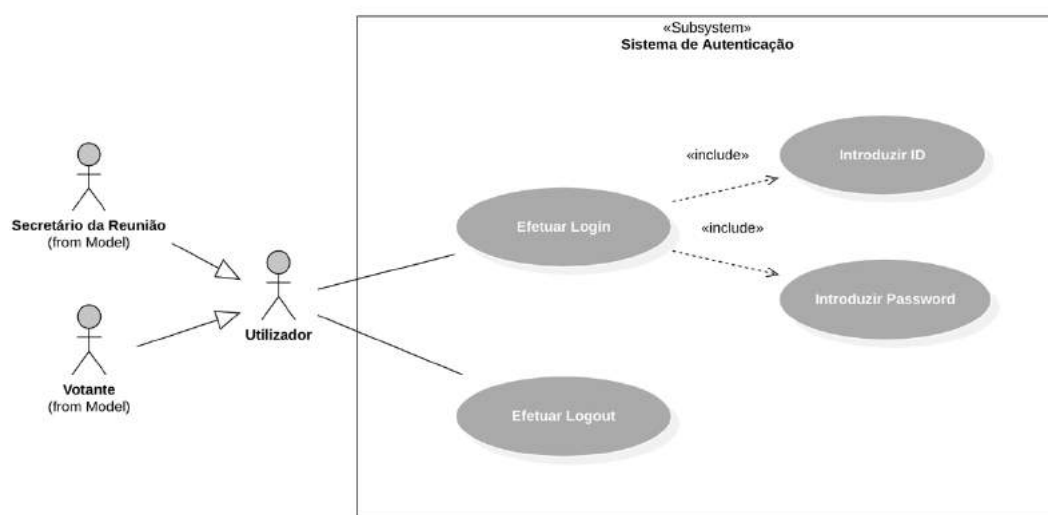


Figura 7 - Diagrama de Caso de Uso referente ao Processo de Autenticação do Utilizador na eVotUM *light*

4.2.2.2 Interação do Votante com a eVotUM *light*

O Votante interage com a plataforma eVotUM *light* através de dois sistemas distintos, designadamente, o Sistema de Consultas e o Sistema de Votação. Nas Figuras 8 e 9, são ilustradas tais interações, através dos respetivos Diagramas de Caso de Uso.

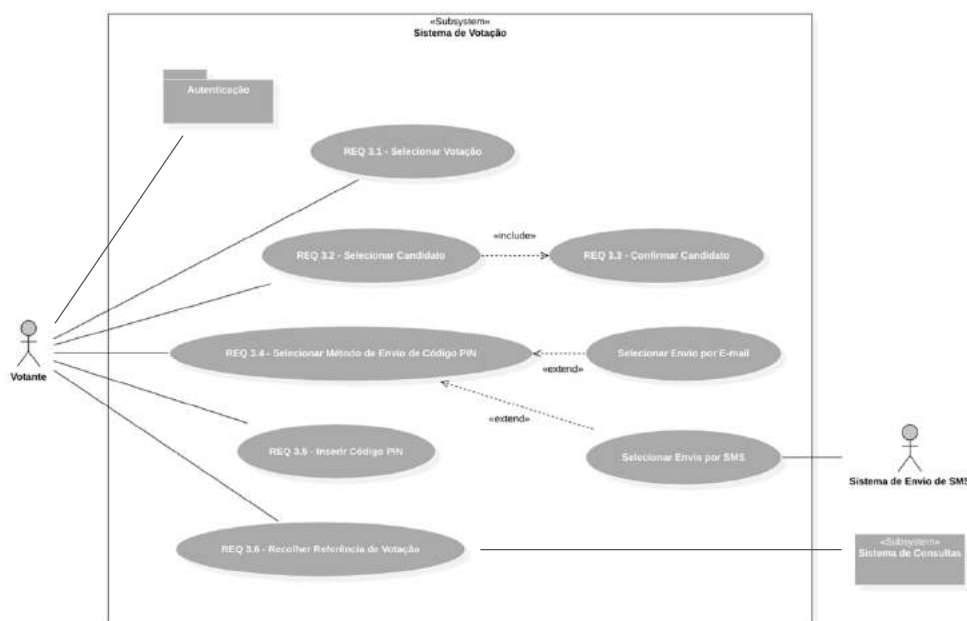


Figura 8 - Diagrama de Caso de Uso referente à interação do Votante com o Sistema de Votação da eVotUM *light*

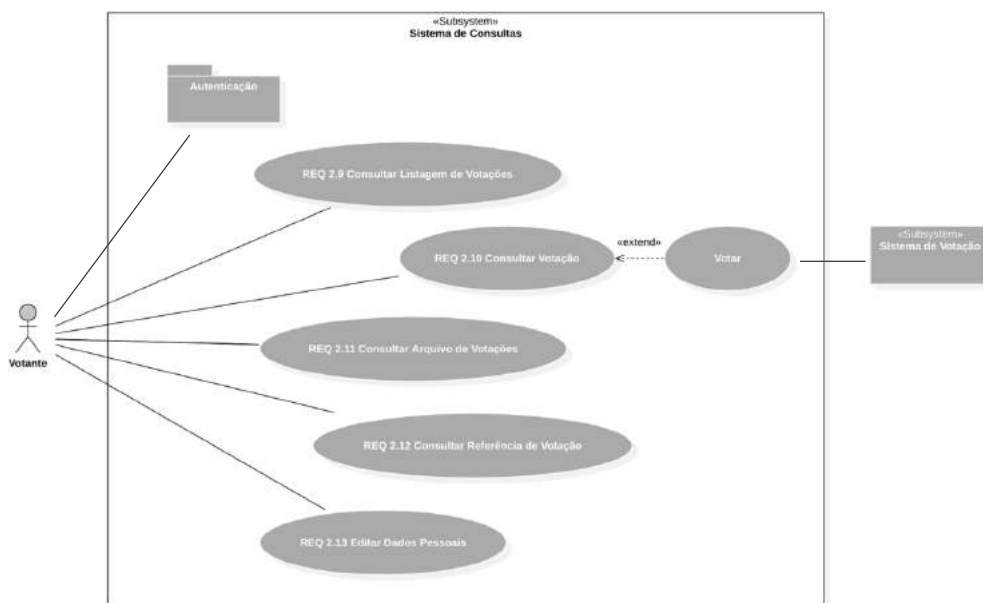


Figura 9 - Diagrama de Caso de Uso referente à interação do Votante com o Sistema de Consultas da eVotUM *light*

4.2.2.3 Interação do Secretário com a eVotUM *light*

O Secretário da Reunião, por outro lado, interage com a plataforma através do Sistema de Gestão de Votações. Na Figura 10 é ilustrada tal interação, através do respetivo Diagrama de Caso de Uso.

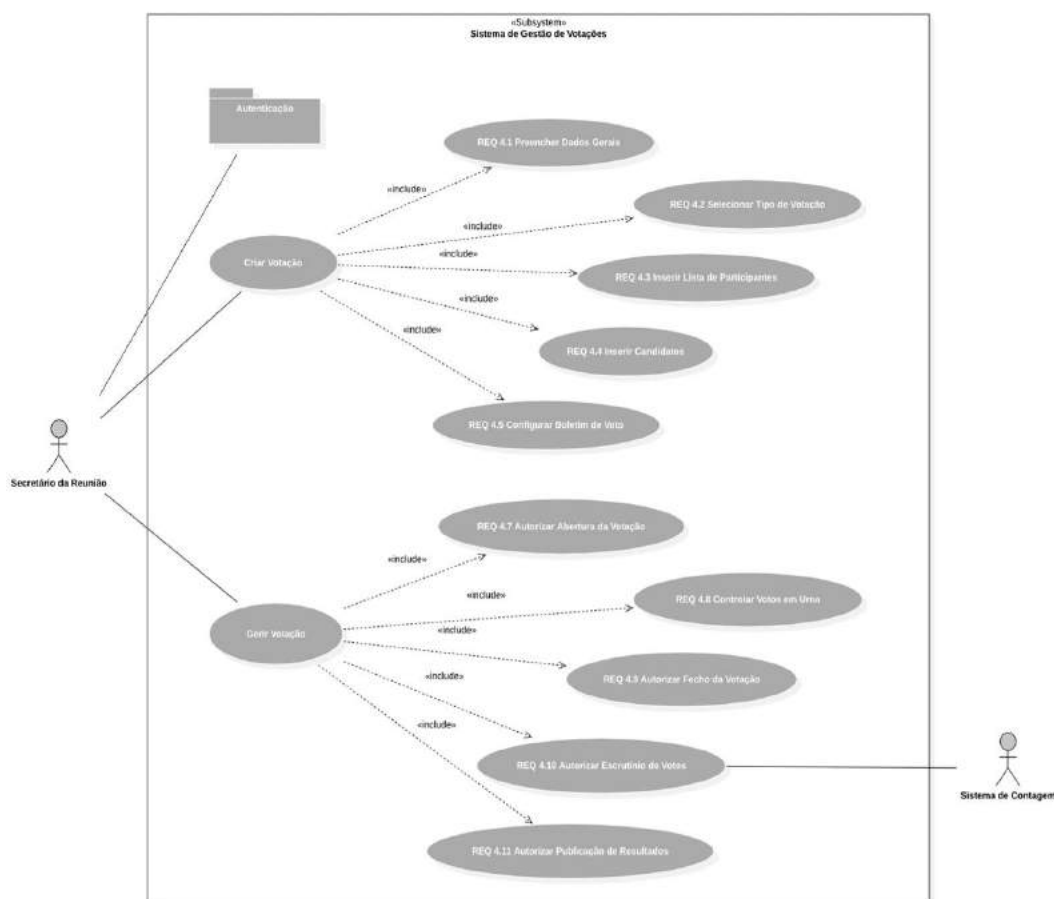


Figura 10 - Diagrama de Caso de Uso referente à interação do Secretário da Reunião com a eVotUM *light*

4.3 Comportamento Dinâmico da Plataforma

A plataforma de votação eletrónica eVotUM *light* pode ser caracterizada, ainda, através de uma especificação dinâmica do seu comportamento, que consiste, portanto, na discriminação pormenorizada daquelas que serão as suas interfaces. O resultado de tal especificação é, pois, o Manual de Utilização da eVotUM *light*, quer do ponto de vista do Votante quer do ponto de

vista do Secretário da Reunião. O Manual de Utilização da plataforma reflete, nesse caso, para cada interveniente, os seus respetivos Casos de Uso. Importa, ainda, referir que as interfaces aqui apresentadas servem, meramente, de orientação para o desenvolvimento daquela que será a plataforma futura. Grande parte irá resultar, inclusive, numa mera simplificação das interfaces já existentes.

4.3.1 Manual de Utilização do Votante

Para conceder uma ideia precisa daquela que será dinâmica de utilização da plataforma por parte do Votante, é apresentado, agora, o seu Manual de Utilização. Representados e especificados, nesta secção, estão os diversos ecrãs com os quais o Votante é confrontado. O Manual está, então, repartido pelos processos de Autenticação, Votação e Consultas.

4.3.1.1 Autenticação

Para se autenticar na plataforma, o Votante deverá clicar no botão "Autenticação", que surge no cabeçalho, através do qual é redirecionado para o formulário de Login, composto pelos campos "Username " e "Password" [Figura 11].



The image shows a login form titled "AUTENTICAÇÃO". It contains two input fields: "Username" with a person icon and "Palavra chave" (Password) with a lock icon. Below these fields is a blue button labeled "Autenticação".

Figura 11 - Formulário de Autenticação na eVotUM light

4.3.1.2 Votação

Passo 1: Para poder participar na votação, o Votante deverá clicar no botão "Votar", que surge na Listagem "As Minhas Votações" [Figura 12 e 13]. Para cada votação é apresentada a informação:

- Identificador;
- Estado;
- Botão "Votar".

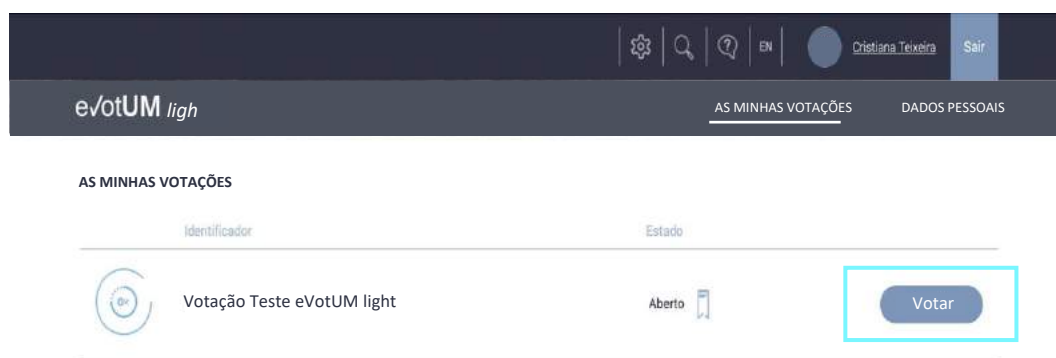


Figura 12 - Listagem de Votações do Votante na eVotUM light

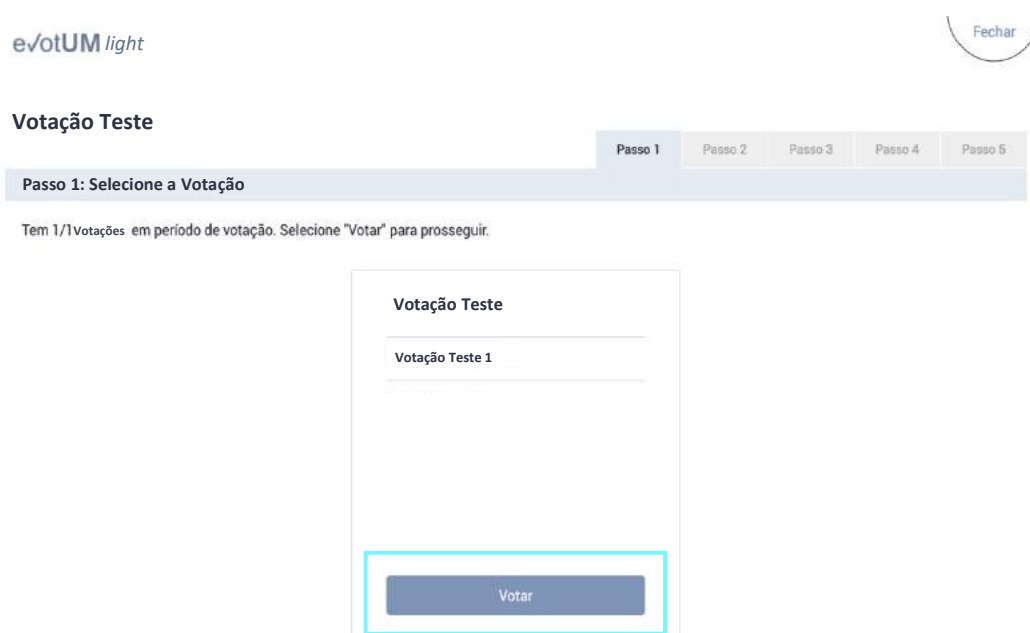


Figura 13 - Passo 1: Selecionar Votação

Passo 2: Apresentado o Boletim de Voto, através do qual o Votante deverá escolher o candidato em quem pretende votar [Figura 14]. Caso não pretenda prosseguir deverá clicar no botão "Anterior". Caso pretenda avançar deverá clicar no botão "Seguinte".

The screenshot shows the 'e/votUM light' interface for 'Votação Teste'. At the top right is a 'Fechar' button. Below the title, a progress bar shows five steps: 'Passo 1', 'Passo 2' (active), 'Passo 3', 'Passo 4', and 'Passo 5'. The main heading is 'Passo 2: Seleccione candidato', followed by the instruction 'Por favor, vote com consciência'. Two candidate options are listed: 'Candidato 1' with a light grey selection box, and 'Candidato 2' with a dark blue selection box and a red 'X' icon. At the bottom, there are 'retroceder' and 'seguinte' buttons.

Figura 14 - Passo 2: Selecionar Candidato

Passo 3: Confirmar a escolha de candidato previamente efetuada [Figura 15]. Caso o Votante não pretenda prosseguir deverá clicar no botão "Anterior". Caso pretenda avançar deverá clicar no botão "Votar".

The screenshot shows the 'e/votUM light' interface for 'Votação Teste'. At the top right is a 'Fechar' button. Below the title, a progress bar shows five steps: 'Passo 1', 'Passo 2', 'Passo 3' (active), 'Passo 4', and 'Passo 5'. The main heading is 'Passo 3: Confirmação da seleção de candidato', followed by the instruction 'Selecionou o seguinte candidato/lista de candidatos'. A single candidate option, 'Candidato 2', is shown with a dark blue selection box and a red 'X' icon. Below this, the instruction 'Click no botão "Votar" para confirmar o voto.' is displayed. A large 'VOTAR' button is highlighted with a red rectangle. At the bottom left, there is a 'retroceder' button.

Figura 15 - Passo 3: Confirmar Seleção de Candidato

Passo 4: Selecionar o mecanismo de envio do PIN de votação, sendo apresentado um formulário para o efeito [Figura 16]. Por norma surge a opção que estiver inserida nos dados pessoais do Votante. Após a seleção, o votante deve clicar no botão "Continuar" e é enviado, automaticamente, o PIN de votação. Posto isto, é apresentado o formulário onde deverá ser inserido o PIN de votação recebido. Ao clicar em "Votar", o Votante finaliza o processo de votação. Caso não pretenda prosseguir pode clicar no botão "Retroceder".

The figure consists of two screenshots of the e/votUM light interface, both showing the 'Votação Teste' section and the 'Passo 4: Submissão do voto' step.

Top Screenshot: The interface shows a progress bar with five steps: Passo 1, Passo 2, Passo 3, Passo 4 (active), and Passo 5. Below the progress bar, there is a text box stating: 'Para o autenticarmos pode escolher receber um código de votação via SMS/correio eletrónico ou utilizar a Chave Móvel Digital (CMD)'. Below this, there is a form with two options: 'E-mail' (selected) and 'Correio Eletrónico: cristiana@teixeira98@gmail.com'. A blue button labeled 'Continuar' is highlighted with a red box. Below the form, there is a link 'Alterar estes dados'. At the bottom, there is a section for 'Autenticar' with a logo and a button labeled 'Autenticar'.

Bottom Screenshot: The interface shows the same progress bar and step indicator. Below the progress bar, there is a text box stating: 'O seu voto só será submetido depois de introduzir o código de votação'. Below this, there is a form with a text input field labeled 'Introduzir o código de votação:'. A blue button labeled 'VOTAR' is highlighted with a red box. At the bottom, there is a button labeled 'retroceder'.

Figura 16 - Passo 4: Selecionar Mecanismo de Envio e Submeter Código PIN de Votação

Passo 5: Apresentada a referência de votação [Figura 17]. Ao clicar em "OK", a votação deixa de estar ativa, ficando o botão "Votar" bloqueado e sendo atualizado o número de votações ativas.

Votação Teste

Passo 1

Passo 2

Passo 3

Passo 4

Passo 5

Passo 5: Boletim de voto depositado na urna

O seu boletim de voto foi depositado na urna eletrônica. A seguinte referência de voto será-lhe enviada por correio eletrónico de modo a que no final do período de votação possa verificar se o seu voto foi contabilizado.

Referência de voto

a9f0466abe61abcce8a9d1020050510202cbcd30467a9c5a177072ea5b11a4bf

OK

Figura 17 - Passo 5: Finalizar Votação e Recolher Referência de Voto

4.3.1.3 Consultas

O votante, ao clicar no botão "Consulta", é redirecionado para a página onde pode consultar se a sua referência faz parte da lista de referências associadas à votação [Figura 18]. Esta página apresenta um formulário de pesquisa onde pode ser inserida a referência e, após a submissão, surge uma mensagem informativa a indicar se faz, ou não, parte da lista.

EN

Cristiana Teixeira

Sair

eVotUM lig

AS MINHAS VOTAÇÕES

DADOS PESSOAIS

AS MINHAS VOTAÇÕES

Identificador	Estado
Votação Teste eVotUM light	Aberto Consult Votar

CONSULTA DAS REFERÊNCIAS DE VOTO

Insira a sua referência de voto e valide se o seu voto foi contabilizado.

Insira aqui a referência de voto

VALIDAR

O voto foi contabilizado.

Lista de referências de voto

29b9637ba210b64d102a49ba8d9884124f375f1a7a6e9fcd2d44fadff72d

Figura 18 - Consultar Referência de Votação

77

4.3.2 Manual de Utilização do Secretário

De modo a conceder uma ideia concisa daquela que será a dinâmica de utilização da plataforma por parte do Secretário é, agora, apresentado o seu Manual de Utilização. Representados e especificados, nesta secção, estão os diversos ecrãs com os quais o Secretário é confrontado. O Manual está, então, repartido pelos processos de Criação da Votação e de Gestão da Votação. O processo de Autenticação não está, aqui, especificado, mas é equivalente ao do Votante [Figura 11].

4.3.2.1 Criação da Votação

Passo 1: Preencher os Dados Gerais [Figura 19], que apresentam a estrutura seguinte:

- Identificador: dois campos de texto simples para inserir a informação em português e em inglês;
- Descrição: dois campos de texto simples para inserir a informação em português e em inglês.

Figura 19 - Passo 1: Inserir Dados Gerais da Votação

Passo 2: Neste novo contexto, este passo é, na realidade, facultativo, sendo cada um dos campos configurado, por omissão, no sentido de respeitar as condições usuais de votação na eVotUM light. A possibilidade de configuração dos campos não é, contudo, eliminada, no sentido de salvaguardar uma necessidade inusitada [Figura 20]. As configurações são, então, compostas pelos seguintes campos:

- Limite de escolhas assinaláveis: Limite definido para uma única opção;
- Write in: Preenchida com a opção “Não”;
- Votação Ordenada: Preenchida com a opção “Não”;
- Peso dos votos: Preenchida com a opção “Não”;
- Método de Hondt: Preenchida com a opção “Não”.

Sistema de Gestão de Votações

Cristiana Teixeira Sair

eVotUM light VOTAÇÕES DADOS PESSOAIS

Criação da Votação

Por favor, insira a informação necessária à criação da votação

Configurações

1. Número máximo de candidatos a escolher no boletim
1

2. Boletim de voto com write-in?
☐ Sim ☒ Não

3. Boletim de voto permite ordenar candidatos?
☐ Sim ☒ Não

4. Os votos podem ter pesos diferentes?
☐ Sim ☒ Não

5. Utilizar método de Hondt?
☐ Sim ☒ Não

Guardar

Figura 20 - Passo 2: Definir Configurações da Votação

Passo 3: Inserir a lista dos votantes que fazem parte da reunião [Figura 21]. A inserção é feita através da importação de um ficheiro CSV, que deve conter os seguintes dados:

- Número de identificação;
- Nome;
- E-mail;
- Telemóvel.

Sistema de Gestão de Votações

Cristiana Teixeira Sair

eVotUM light VOTAÇÕES DADOS PESSOAIS

Criação da Votação

Por favor, insira a informação necessária à criação da votação

Lista de Votantes

Descrição	Documento
	Escolher ficheiro

Submeter

Nome Do Documento	Versão	Publicado Em	Carregado	Documento PDF
CSV file	202206021518	02-06-2022 16:18	✓	

Caderno eleitoral publicado

Figura 21 - Passo 3: Inserir Lista de Votantes na Votação

Passo 4: Inserir cada um dos candidatos concorrentes à votação [Figura 22]. Os dados associados são os seguintes:

- Nome;
- Documento com Informação adicional;

Sistema de Gestão de Votações

Cristiana Teixeira Sair

eVotUM light VOTAÇÕES DADOS PESSOAIS

Criação da Votação

Por favor, insira a informação necessária à criação da votação

Candidatos

Imagem	Nome do Candidato	Nome Do Documento	Ficheiro Do Documento
	Candidato 1	Candidato1	uploads/2022/06/0/ Escolher ficheiro
	Candidato 2	Candidato 2	uploads/2022/06/0/ Escolher ficheiro

Guardar

Figura 22 - Passo 4: Inserir Candidatos à Votação

Passo 5: Configurar o Boletim de Voto [Figura 23]. Os dados a configurar são os seguintes:

- Instruções: dois campos de texto simples para preencher em português e em inglês;
- Apresentação dos candidatos: Radio button com as opções Lista e Dropdown;
- Ordenação dos candidatos: Para além da gestão manual da ordem dos candidatos, existe um botão para gerar aleatoriamente a ordem dos candidatos.

Ao clicar no botão "Pré-Visualização do Boletim de Voto" é apresentada uma janela pop-up com a representação do boletim de voto que irá surgir no sistema de votação.

Sistema de Gestão de Votações

evotUM light

VOTAÇÕES

DADOS PESSOAIS

Cristiana Teixeira

Sair

Criação da Votação

Por favor, insira a informação necessária à criação da votação

Configuração do Boletim de Voto

Instruções a figurar no Boletim de Voto, antes dos Candidatos.

[PT] Por favor, vote com consciência

[EN] Por favor, vote com consciência

Selecione o modo de apresentação dos Candidatos no Boletim de

☒ Lista ☐ Caixa suspensa

Misturar Candidatos

Pré-Visualização Do Boletim De Voto

Logo	Designação
	Candidato 1
	Candidato 2

Guardar

Figura 23 - Passo 5: Configurar Boletim de Voto da Votação

4.3.2.2 Gestão da Votação

O Secretário, para poder acompanhar e gerir as suas votações, deve aceder ao Painel de Gestão de Votações [Figura 24]. Para cada votação são apresentadas as seguintes etapas:

- Iniciar Votação [Passo 1];
- Votos em Urna [Passo 2];
- Fechar Votação [Passo 3];
- Escrutinar Votos [Passo 4];
- Publicar Resultados [Passo 5].

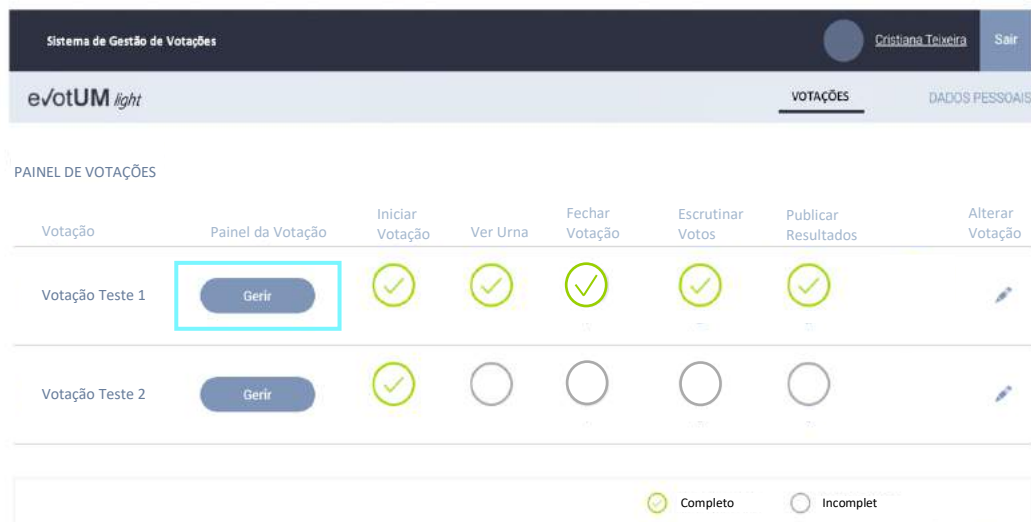


Figura 24 - Painel de Votações

Passo 1: Autorizar o começo da votação, através do botão “Autorizar Início da Votação” [Figura 25].

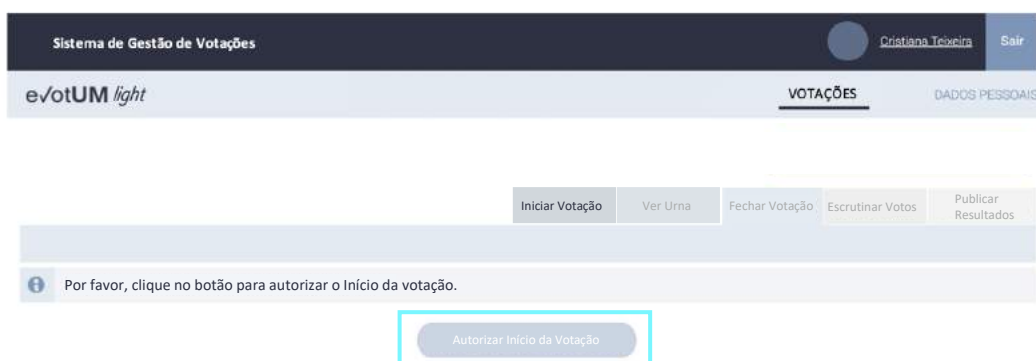


Figura 25 - Passo 1: Autorizar Início da Votação

Passo 2: Através do botão “Número Total de Boletins em Urna” [Figura 26], o Secretário consegue aceder à área referente à Urna eletrónica [Figura 27], o que lhe permite observar o

número de votos já efetuados, em tempo real, e perceber quando avançar para o fecho da votação.



Figura 26 - Passo 2: Aceder à Urna Eletrónica



Figura 27 - Passo 2: Visualizar Número Total de Boletins em Urna

Passo 3: Autorizar o fecho da votação, através do botão “Autorizar Fecho da Votação” [Figura 28]. Através do controlo de votos em urna, no Passo 2, o Secretário tem perceção do número de votos já efetuados e, no caso desse número corresponder à totalidade de votantes, poder-se-á finalizar a votação.

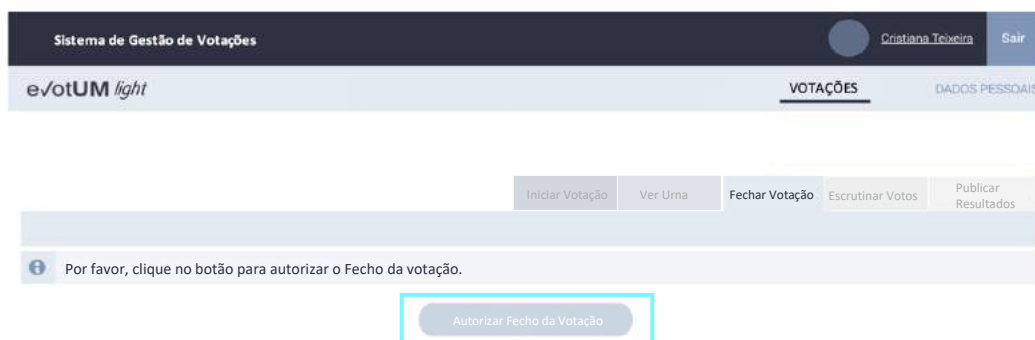


Figura 28 - Passo 3: Autorizar Fecho da Votação

Passo 4: Autorizar escrutínio dos votos [Figura 29]. Nesta área, o Secretário terá de clicar no botão “Autorizar Escrutínio de Votos” para que se dê o processo. Posto isto, o resultado da votação é apresentado no Painel [Figura 30].



Figura 29 - Passo 4: Autorizar Escrutínio dos Votos



Figura 30 - Passo 4: Apresentação de Resultados no Painel do Secretário

Passo 5: Autorizar publicação do resultado da votação na plataforma [Figura 31]. Nesta área, o Secretário terá de clicar no botão “Publicar Resultados” para que se dê o processo. Posto isto, o resultado da votação é apresentado, na plataforma, a todos os votantes.



Figura 31 - Passo 5: Autorizar Publicação de Resultados

4.4 Infraestrutura Tecnológica da Plataforma

A especificação da plataforma futura é concluída, neste segmento final, com a descrição daquela que será a sua infraestrutura tecnológica. Tal como aconteceu, no capítulo anterior, para a eVotUM, a descrição da infraestrutura da eVotUM *light* engloba a caracterização de todas as componentes de Software e Hardware, da arquitetura e do fluxo de comunicação que se estabelece em cada votação.

A eVotUM *light* é, essencialmente, uma adaptação da eVotUM, projetada no sentido de promover votações a uma escala substancialmente inferior à que é, atualmente, praticada. A adequação da plataforma ao novo contexto não altera, no entanto, de forma considerável, a sua infraestrutura tecnológica. A eVotUM *light* permanece, pois, uma plataforma de votação eletrónica via Web, sendo estabelecidas comunicações através de redes abertas, não seguras por definição. Os votantes podem interagir com a plataforma mediante a utilização de um browser, instalado num *desktop*, computador portátil, *tablet* ou *smartphone*. O sistema é, por conseguinte, capaz de adaptar as suas interfaces às condições de visualização e interação impostas.

A eVotUM *light*, tal como a eVotUM, está preparada para concretizar diversas votações em simultâneo, encontrando-se ao dispor de qualquer elemento da Universidade do Minho em matéria de votações em reuniões. Este sistema permite, ainda, a interação com os seus utilizadores tanto em língua portuguesa como inglesa.

4.4.1 Componentes de Software

Estruturalmente, a eVotUM *light* é idêntica à eVotUM, sendo, pois, suportada por quatro serviços, designadamente, o **Validator Service**, o **Filter Service**, o **Anonymizer Service** e o **Counter Service**. Existem, ainda, no sistema, quatro componentes de apoio, nomeadamente, o Sistema de Administração, o Sistema de Gestão de Votações, o Sistema de Consultas e o Sistema de Votação. Importa referir que tais componentes, embora aparentemente idênticas

às da eVotUM, podem estar sujeitas a algumas alterações. Na tabela 14 explana-se cada um dos componentes do sistema previamente enunciados.

Tabela 14 - Descrição detalhada dos componentes de Software da eVotUM light

Componente de Software	Descrição
Validator Service	Este serviço é responsável por validar os votos dos votantes, recolhidos através do sistema. Possui, tal como a votação, um certificado digital de chaves pública e privada. Através da chave privada, procede à assinatura do voto cifrado e cegado, que recebe do votante, validando-o. A assinatura, por sua vez, é guardada sem qualquer associação do voto ao respetivo votante. A ação do <i>Validator Service</i> termina com a devolução do voto, já assinado, ao votante.
Filter Service	Este serviço funciona como um filtro único para os votos dos votantes, antes de os mesmos serem enviados ao <i>Anonymizer Service</i> . A sua finalidade consiste em ocultar a origem do voto, pelo que, para o <i>Anonymizer Service</i> , os votos terão todos a mesma origem. O <i>Filter Service</i> aplica, ainda, verificações fortes aos pacotes que recebe e não guarda nenhum voto ou informação relativa ao mesmo. A ação do <i>Filter Service</i> acaba com o envio do pacote para o <i>Anonymizer Service</i> .
Anonymizer Service	O <i>Anonymizer Service</i> recebe um pacote constituído pelo voto cifrado, e respetiva assinatura, proveniente do <i>Validator Service</i>. Posto isto, procede à anonimização do mesmo. Este procedimento passa, então, por receber o pacote, guardá-lo de forma aleatória e misturá-lo, de imediato, com os votos previamente recolhidos. Os votos são guardados numa estrutura, tecnologicamente não ordenada, referenciados apenas por um número aleatório, gerado quando é recebido. Tem-se, assim, um tuplo constituído por <número, pacote>, guardado em posição desconhecida. Posteriormente, a estrutura é misturada. Etiquetas temporais são, no caso concreto da eVotUM light, desnecessárias, uma vez que a votação só é dada por encerrada após a reunião dos votos de todos os participantes em urna. Não existe, portanto, a necessidade de admitir votos que ainda estejam em transição no sistema, e já tenham passado a fase do <i>Validator Service</i>, no período válido de votação.
Counter Service	O <i>Counter Service</i> recebe os votos, misturados, do <i>Anonymizer Service</i> . Os votos podem ser enviados, para o serviço de contagem, em lotes, durante o período de votação, ou, então, de uma só vez,

	no final da votação. É, então, neste serviço que os votos são decifrados e contabilizados, no final da votação.
Sistema de Administração	O sistema de administração constitui o instrumento através do qual o administrador da plataforma tem permissão para efetuar, se necessário, o carregamento dos certificados digitais a utilizar pelo sistema. Os certificados são carregados, por norma, uma única vez, correspondente à fase de ativação da plataforma. O administrador não desempenha, assim, um papel ativo no funcionamento da plataforma, isto é, não administra, efetivamente, a sua utilização.
Sistema de Gestão de Votações	O sistema de gestão de votações concede apoio ao Secretário da Reunião. Para que a criação ou gestão de uma votação se torne mais intuitiva, o sistema de gestão de votações assenta o seu funcionamento num modelo de fluxo de trabalho, <i>workflow</i> , que guia o Secretário nas diversas tarefas conexas à votação.
Sistema de Consultas	O sistema de consultas permite, ao votante, verificar a listagem de votações das quais faz parte, o arquivo de votações, bem como as informações gerais referentes a uma dada votação. Através do sistema de consultas o votante poderá, ainda, aceder ao sistema de votação. Adicionalmente, concluído o período de votação, o votante poderá, neste local, verificar se o seu voto foi contabilizado na votação. A verificação é efetuada através de um número único atribuído ao voto no momento da votação.
Sistema de Votação	O sistema de votação é o meio através do qual o votante participa numa votação, podendo expressar a sua escolha através do voto. Para que tal seja possível, o sistema requer que o votante se autentique no sistema, recorrendo aos respetivos dados de autenticação. Uma vez efetuada a autenticação, o votante tem acesso à lista de votações nas quais poderá participar. O boletim será constituído por uma barra que exhibe a progressão da votação até à sua conclusão. No final da votação é apresentado, ao votante, o número único atribuído ao seu voto.

4.4.2 Arquitetura da Infraestrutura

A plataforma eVotUM *light* dispõe dos mesmos servidores da eVotUM, designadamente, o **WebServer**, o **DBServer** e os **Application Servers**. O WebServer, também referido como servidor *Front-end*, é o nível com o qual o navegador web do utilizador comunica e trata de pedidos HTTP. O *DBServer*, por outro lado, executa o processo da base de dados, utilizando a *Structured Query Language*, SQL, para armazenar e recuperar dados. Os *Application Servers*

suportam o objetivo de dotar a plataforma de uma arquitetura orientada a serviços *Web*. O diagrama lógico referente à arquitetura da infraestrutura é, portanto, em tudo semelhante ao que se pôde observar para a eVotUM, no capítulo anterior, através da Figura 4.

No que respeita à redundância da infraestrutura tecnológica, também a eVotUM *light* reaproveita toda a lógica da eVotUM e, nesse sentido, diversos dos seus componentes, como Firewalls e Web Servers, recorrem à replicação. Também a base de dados utiliza tecnologias como a replicação, no sentido de garantir uma alta disponibilidade do serviço. Neste modelo, tal como referido para a eVotUM, quando uma componente falha, a tarefa é enviada para componente complementar. Através do recurso a máquinas virtuais são, então, mantidas duas versões idênticas dos diversos servidores e Firewalls inerentes à plataforma. O objetivo é, portanto, garantir a utilização ininterrupta do sistema e evitar a perda de dados. Na Figura 5, do capítulo 3, é possível observar o diagrama referente à redundância aplicada ao sistema. Como também se poderá averiguar na figura, o sistema contempla, ainda, um servidor de gestão, responsável por efetuar as cópias de segurança, cumprir a monitorização e manter a centralização de *logs* da infraestrutura. A eVotUM *light* não deverá recorrer, à partida, a uma sala-cofre, em matéria de atualizações da plataforma, tal como a eVotUM, sendo que apenas o Secretário da Reunião é responsável pela sua modificação. A integridade da base de dados, por outro lado, segue os moldes da eVotUM e, nesse sentido, os dados são assinados com HMAC e é cumprida uma separação de privilégios, ou seja, o gestor do servidor da aplicação não pode ser gestor do servidor da base de dados.

4.4.3 Fluxo de Comunicação

Para cada votação existe um fluxo de comunicação. O diagrama que faz referência ao fluxo de comunicação que se estabelece na eVotUM *light*, aquando de uma votação, é em tudo semelhante ao da eVotUM, representado na Figura 6 do capítulo prévio, salvo pequenos ajustes na terminologia. O diagrama funciona, basicamente, como um meio de compreensão da correspondência que se estabelece entre os diversos serviços e sistemas da plataforma e o votante e, nesse sentido, o da eVotUM *light* é equivalente ao da eVotUM.

Na Figura 32 está, portanto, ilustrado o diagrama atualizado, representativo do fluxo de comunicação que se estabelece na eVotUM *light*.

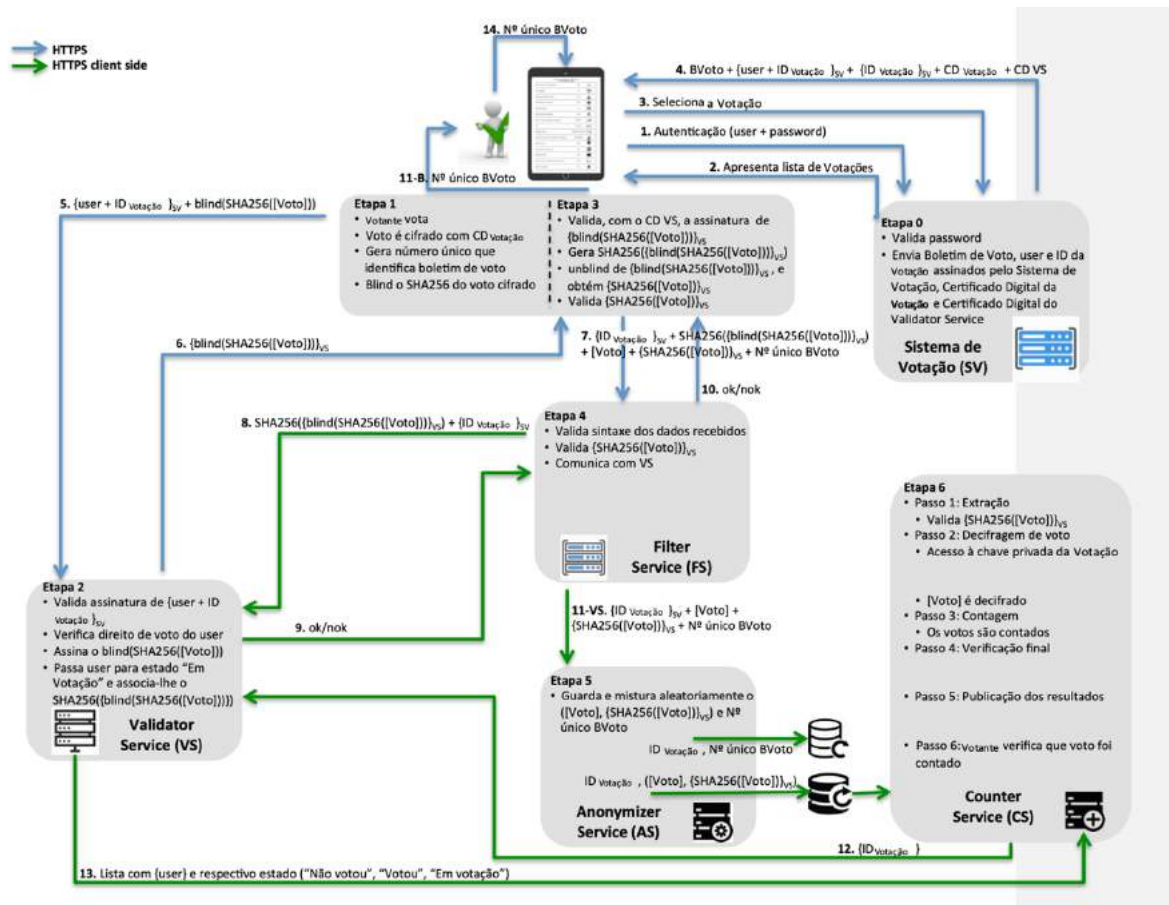


Figura 32 - Fluxo de Comunicação detalhado referente a uma Votação na eVotUM light (Fluxos de Comunicação, CCG, Eurotux & Devise Futures)

CAPÍTULO 5

CONCLUSÃO

No presente capítulo serão retiradas as principais conclusões associadas ao trabalho desenvolvido, anunciadas as dificuldades sentidas aquando da sua concretização e traçadas perspectivas futuras tendo por base a solução proposta.

Os objetivos inicialmente assinalados para a dissertação foram integralmente satisfeitos. A revisão de literatura, antes de mais, possibilitou um estudo minucioso no que concerne a arquiteturas projetadas para plataformas de votação eletrónica, o que resultou, por fim, numa melhor compreensão dos sistemas, dessa natureza, existentes. Para o efeito foram analisados inúmeros artigos e dissertações referentes à matéria em investigação.

A caracterização da eVotUM resultou, por sua vez, numa descrição detalhada de todas as componentes que a constituem e viabilizou, posteriormente, a especificação da eVotUM light, cujos componentes resultam, diretamente, da identificação e adaptação dos da eVotUM. Esta caracterização foi concebida, ainda, por meio de uma descrição do comportamento funcional e arquitetura tecnológica que lhe são inerentes, com vista à prossecução do objetivo seguinte, de especificação da nova plataforma. Uma vez concluído este segmento, e tendo por base os seus fundamentos, tornou-se exequível o objetivo seguinte, de levantamento e descrição dos requisitos funcionais e não funcionais imprescindíveis ao suporte da eVotUM *light*.

A concretização do último objetivo traçado para o projeto, de especificação de uma nova plataforma de votação, pensada para reuniões em formato híbrido, resultou, pois, do culminar do estudo efetuado e de uma continua reflexão. Só então foi possível efetuar uma descrição detalhada da eVotUM light, delinear os seus requisitos, funcionais e não funcionais, e esboçar, com base em todas as adaptações, as suas interfaces. A especificação derivou, então, de uma descrição integral da plataforma, designadamente, dos seus comportamentos funcional e dinâmico e da sua respetiva infraestrutura tecnológica.

A realização deste trabalho veio salientar a importância e urgência de desenvolver uma plataforma que promova votações em reuniões de uma forma segura, mas muito simples e intuitiva. O uso da eVotUM para esse efeito tem sido, até agora, um processo fastidioso, uma vez que a plataforma se encontra muito pouco ajustada para o efeito e exige o cumprimento de um alargado conjunto de etapas, intrínsecas àquele que é, por norma, o processo eleitoral. A especificação da eVotUM *light* procurou, assim, reaproveitar a atual arquitetura da eVotUM e adaptar, convenientemente, todas as suas implementações, ao novo contexto de votação. Nesse sentido, todas as garantias de segurança e credibilidade, inerentes à eVotUM, ficam salvaguardadas, e o propósito da nova plataforma é devidamente cumprido.

Todavia, foram sentidas algumas dificuldades aquando do desenvolvimento do trabalho, sobretudo em questões, de carácter técnico, concernentes à especificação da eVotUM *light*. As implicações, que a adaptação da eVotUM teve, na infraestrutura tecnológica da eVotUM *light*, originaram diversas dúvidas, designadamente em matéria de decifragem de votos e, ainda, de geração de credenciais para utilizadores da plataforma. A primeira grande questão que se colocou foi se a segurança da votação não seria comprometida, neste novo contexto, uma vez que o único detentor do segredo, de acesso à chave privada da votação, seria o Secretário da reunião, isto é, o responsável pela votação. Tal não foi possível aferir, por falta de conhecimento técnico na matéria, o que tem, naturalmente, repercussões nos resultados do trabalho. Ademais, a segunda questão que se colocou foi se a atribuição de credenciais aos utilizadores deveria ser efetuada pelo Secretário, através da submissão de uma lista com os respetivos dados dos participantes na votação, ou se deveria ser efetuada por um Serviço de Diretoria externo, tendo sido determinado que a segunda opção seria a mais viável e, portanto, de uso na eVotUM *light*.

Para desenvolvimento futuro aponto, antes de mais nada, a urgência em implementar a solução, neste documento, especificada. Uma vez implementada, a plataforma deverá, ainda, ser utilizada e avaliada em contexto real, para que, por último, possa ser convenientemente ajustada. Como resultado dos esforços enunciados, poderão, então, ser suportadas votações, em tempo real, em contexto de reuniões híbridas de pequenos grupos.

REFERÊNCIAS BIBLIOGRÁFICAS

- Benaloh, J. D. C. (1987). Verifiable secret-ballot elections. Yale University.
- Benaloh, J. D. C. (2006). Simple Verifiable Elections. *EVT*, 6, 5-5.
- Bernhard, D., & Warinschi, B. (2013). Cryptographic voting—a gentle introduction. In *Foundations of Security Analysis and Design VII* (pp. 167-211). Springer, Cham.
- Brioso, A. M. L. (2012). Votação Electrónica Resistente a Vírus. Retrieved from <https://fenix.tecnico.ulisboa.pt/downloadFile/395144233563/dissertacao.pdf>
- Burmester, M., & Magkos, E. (2003). Towards secure and practical e-elections in the new era. In *Secure electronic voting* (pp. 63-76). Springer, Boston, MA.
- Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2), 84-90.
- Cortier, V., Dreier, J., Gaudry, P., & Turuani, M. (2019). A simple alternative to Benaloh challenge for the cast-as-intended property in Helios/Belenios.
- Cranor, L. F., & Cytron, R. K. (1997, January). Sensus: A security-conscious electronic polling system for the internet. In *Proceedings of the Thirtieth Hawaii International Conference on system sciences* (Vol. 3, pp. 561-570). IEEE.
- Danezis, G., & Diaz, C. (2008). A survey of anonymous communication channels.
- de Sousa Grilo, P. F. V. (2015). Voto seguro pela Internet através de smartphones.
- Eliasson, C., & Zúquete, A. (2006). An electronic voting system supporting vote weights. *Internet Research*.
- Faria, P. V. C. L. (2013). Remote Electronic Voting: Studying and Improving Helios (Doctoral dissertation, Universidade do Minho (Portugal)).
- Haenni, R., Dubuis, E., & Ultes-Nitsche, U. (2008). Research on e-voting technologies. Bern University of Applied Sciences, Tech. Rep, 5.

- Joaquim, R. (2005). A fault tolerant voting system for the internet (Doctoral dissertation, Master's thesis, IST/UTL).
- Joaquim, R., Ribeiro, C., & Ferreira, P. (2011). Towards Trustworthy Internet Elections. Technical Report 6, INESC-ID.
- Nogueira, J. A. P. M. (2011). Confiança em votação electrónica (Doctoral dissertation).
- Wang, K. H., Mondal, S. K., Chan, K., & Xie, X. (2017). A review of contemporary e-voting: Requirements, technology, systems and usability. *Data Science and Pattern Recognition*, 1(1), 31-47.
- Zúquete, A., & Almeida, F. (2008, March). Verifiable anonymous vote submission. In *Proceedings of the 2008 ACM symposium on Applied computing* (pp. 2159-2166).
- Zúquete, A., Ferreira, A., Costa, C. J., Magalhães, D., Vieira, D., Simões, F., ... & Joaquim, R. (2008). Voto Electrónico-Discussão Técnica dos Seus Problemas e Oportunidades. Retrieved from <http://hdl.handle.net/10451/14891>

ANEXOS

ANEXO I – Guia do Eleitor;

ANEXO II – Guia da Comissão Eleitoral;

ANEXO III – Guia do Responsável Institucional;

ANEXO IV - Requisitos funcionais implementados no âmbito do projeto da eVotUM;

ANEXO V - Requisitos funcionais a implementar no âmbito do projeto da eVotUM *light*;

ANEXO I

GUIA DO ELEITOR

Neste primeiro anexo é apresentado o Guia do Eleitor, referente ao sistema de votação eletrónica eVotUM. O Guia encontra-se, portanto, repartido em sete questões fundamentais, de modo a esclarecer, objetivamente, as dúvidas dos utilizadores relativas à efetivação da votação. Abaixo são discriminadas cada uma das questões referidas, designadamente, as características, o modo de acesso à plataforma, o método de verificação do caderno eleitoral, o processo de votação, o método de verificação de votos contabilizados, o processo de envio de mensagens à comissão eleitoral e, ainda, o método de alteração de dados pessoais.

A. CARATERÍSTICAS



B. COMO ACEDER

Como aceder?

Sistema de votação eletrónica, Guia do eleitor

O acesso ao sistema eVotUM é feito através do site:

<https://evotum.uminho.pt/>



Como aceder?

Sistema de votação eletrónica, Guia do eleitor

PÚBLICO

Acede às páginas públicas do sistema de votação eletrónica, com:

- Informação genérica (Perguntas frequentes, Política de segurança de informação, Política de privacidade, Termos de utilização, Mapa do site, Contactos);
- Consulta de processos eleitorais (toda a informação disponibilizada pela Comissão eleitoral);
- Verifica se pertence ao caderno eleitoral, podendo apresentar reclamação caso haja incorreção no mesmo.



Como aceder?

Sistema de votação eletrónica, Guia do eleitor

ELEITOR

Após autenticação (credenciais de segurança utilizadas no acesso aos serviços da Universidade do Minho), acede a:

- Votação nas eleições que estejam dentro do período de votação;
- Informação genérica (Perguntas frequentes, Política de segurança de informação, Política de privacidade, Termos de utilização, Mapa do site, Contactos);
- Consulta dos processos eleitorais do eleitor (toda a informação disponibilizada pela Comissão eleitoral);
- Alteração de dados pessoais;
- Sistema de mensagens para comunicação com a Comissão Eleitoral.



C. COMO VERIFICAR O CADERNO ELEITORAL

Como verificar o caderno eleitoral?

Sistema de votação eletrônica, Guia do eleitor

1. Aceda a <https://evotum.uminho.pt/>
2. Selecione **“Verificar cadernos eleitorais”**





11

Como verificar o caderno eleitoral?

Sistema de votação eletrônica, Guia do eleitor

3. Selecione **“Consultar”** do processo eleitoral em causa.



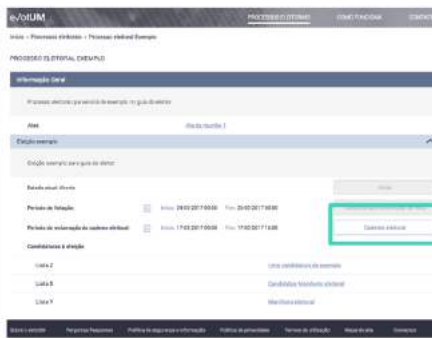


12

Como verificar o caderno eleitoral?

Sistema de votação eletrônica, Guia do eleitor

4. Selecione a aba da eleição em causa
5. Selecione **“Caderno eleitoral”** e verifique se faz parte do mesmo





13

Como verificar o caderno eleitoral?

Sistema de votação eletrônica, Guia do eleitor

6. Se houver alguma inconformidade, **“Apresente reclamação”**, e poderá escrever uma mensagem à comissão eleitoral, expondo o caso.



evotUM

14

D. COMO VOTAR

Como votar?

Sistema de votação eletrônica, Guia do eleitor

1. Aceda a <https://evotum.uminho.pt>
2. Selecione **“Autenticação”** ou **“Autentique-se para votar”**



evotUM

16

Como votar?

Sistema de votação eletrônica, Guia do eleitor

3. Insira as **credenciais** de segurança utilizadas no acesso aos serviços da Universidade do Minho

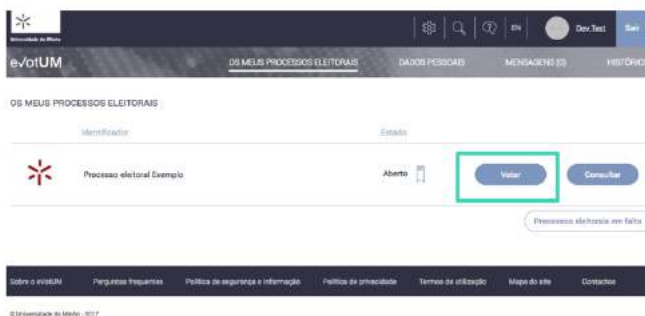


evotUM

Como votar?

Sistema de votação eletrônica . Guia do eleitor

4. Selecione
“Votar” no
processo eleitoral
em causa

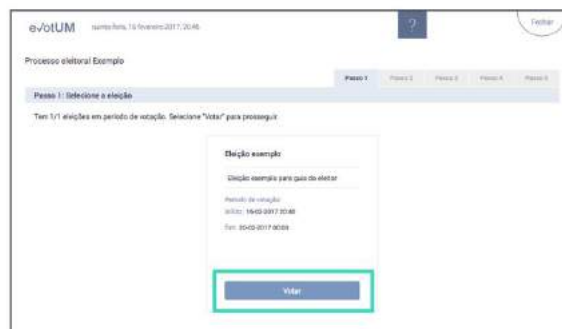


18

Como votar?

Sistema de votação eletrônica . Guia do eleitor

5. **Selecione a eleição**
onde pretende
exercer o seu direito
de voto.

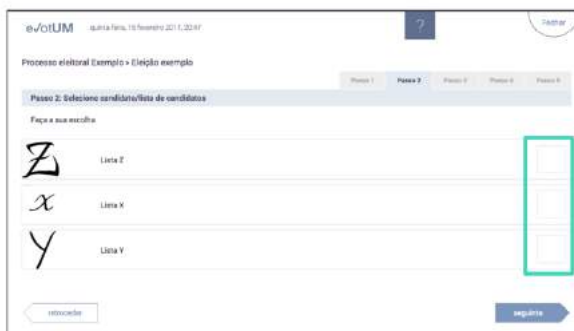


19

Como votar?

Sistema de votação eletrônica . Guia do eleitor

6. **Selecione candidato/lista** (pode
não escolher nenhum,
i.e., voto em branco).



20

Como votar?

Sistema de votação eletrónica - Guia do eleitor

7. **Confirme** a seleção do candidato/lista

The screenshot shows the eVotUM interface at Step 3: 'Confirmação de seleção de candidato'. It displays a list of candidates with 'Lista 1' selected. A red box highlights the 'VOTAR' button at the bottom right. The interface includes a progress bar at the top and a 'Finalizar' button in the top right corner.



21

Como votar?

Sistema de votação eletrónica - Guia do eleitor

8. Efetue uma **segunda autenticação** (A) recebendo um **código** por SMS ou e-mail, ou (B) por **Chave Móvel Digital** (serviço de autenticação do Governo Português).

The screenshot shows the eVotUM interface at Step 4: 'Submissão do voto'. It presents two authentication options: (A) receiving a code via SMS or email, and (B) using the Chave Móvel Digital. A red box highlights the 'Continuar' button next to the email selection. Another red box highlights the 'Autenticar' button under the Chave Móvel Digital section. The interface includes a progress bar at the top and a 'Finalizar' button in the top right corner.



22

Como votar?

Sistema de votação eletrónica - Guia do eleitor

8. A.1 – Ao selecionar **“Continuar”** recebe um código de votação no seu contacto de email ou de telemóvel.

This screenshot is identical to the one on page 22, showing the eVotUM interface at Step 4: 'Submissão do voto'. It highlights the 'Continuar' button for email authentication and the 'Autenticar' button for Chave Móvel Digital. The interface includes a progress bar at the top and a 'Finalizar' button in the top right corner.



23

Como votar?

Sistema de votação eletrônica . Guia do eleitor

8. A.2- **Introduza o código** de votação recebido. Ao selecionar **“Votar”** está a enviar o seu voto para a urna eletrônica.

The screenshot shows the eVotUM interface at Step 4, 'Submissão do voto'. The header indicates 'Processo eleitoral Exemplo - Eleição exemplo' and 'Passo 4' is selected in a sequence of five steps. The instruction reads: 'O seu voto só será submetido depois de introduzir o código de votação'. There is a text input field for the code, which is highlighted with a red rectangle. Below it is a blue button labeled 'VOTAR', also highlighted with a red rectangle. A 'Retornar' button is at the bottom left.

 eVotUM

24

Como votar?

Sistema de votação eletrônica . Guia do eleitor

8 B.1 – Ao selecionar **“Autenticar”** é direcionado para Autenticação.Gov onde se pode autenticar por Chave Móvel Digital ou com o Cartão de Cidadão.

The screenshot shows the eVotUM interface at Step 4, 'Submissão do voto'. The instruction reads: 'Para o autenticar pode escolher receber um código de verificação via SMS/correo eletrónico ou utilizar a Chave Móvel Digital (CMD)'. There is a dropdown menu for 'Enviar o código de verificação para:' with 'Email' selected. Below this, it says 'Pode também escolher validar através da Chave Móvel Digital para Autenticação gov.'. There is a button for 'Autenticar' with the Autenticação.gov logo, which is highlighted with a red rectangle. A 'Retornar' button is at the bottom left.

 eVotUM

25

Como votar?

Sistema de votação eletrônica . Guia do eleitor

8 B.2 – **Autorize** o fornecimento dos vários dados indicados ao sistema eVotUM, de modo a este o poder autenticar.

The screenshot shows the Autenticação.gov interface for authorization. The header says 'Faça a sua autenticação com:'. There are two tabs: 'Cartão de Cidadão' and 'Chave Móvel Digital'. The 'Chave Móvel Digital' tab is active. The instruction reads: 'Efetua validação do Móvel: associa alguns dos seus dados para realizar a autenticação'. Under 'Dados opcionais', there are checkboxes for 'Nome Completo', 'Identificação no Sís. Social', 'Identificação Postal', and 'Identificação Civil'. Under 'Método de autenticação', there are radio buttons for 'Interativo' (selected) and 'Não Interativo'. At the bottom, there are 'Recusar' and 'Autorizar' buttons, with 'Autorizar' highlighted with a red rectangle.

 eVotUM

26

Como votar?

Sistema de votação eletrônica . Guia do eleitor

8 B.3 – Introduza o número de telemóvel e PIN associado à sua Chave Móvel Digital, e selecione “Autenticar”.

aqui os seus dados. Se ainda não tem, registre-se [aqui](#).'"/>

Como votar?

Sistema de votação eletrônica . Guia do eleitor

8 B.4 – Insira o **código** de segurança recebido por SMS e clique em “Confirmar”. O Autenticação.Gov enviará os dados autorizados para o sistema eVotUM e, o seu voto será depositado na urna eletrônica.

Como votar?

Sistema de votação eletrônica . Guia do eleitor

9. O seu boletim de voto foi depositado na urna eletrônica e é-lhe fornecida a sua referência de voto (que também é enviada para o seu e-mail).

E. COMO VERIFICAR SE O VOTO FOI CONTABILIZADO

Como verificar se o seu voto foi contabilizado?

Sistema de votação eletrônica - Guia do eleitor

1. Aceda a
<https://evotum.uminho.pt/>

2. Selecione
“Autenticação”



**eVotUM**
Sistema de Votação Eletrónica da Universidade do Minho

31

Como verificar se o seu voto foi contabilizado?

Sistema de votação eletrônica - Guia do eleitor

3. Insira as
credenciais de
segurança
utilizadas no
acesso aos
serviços da
Universidade do
Minho



**eVotUM**
Sistema de Votação Eletrónica da Universidade do Minho

32

Como verificar se o seu voto foi contabilizado?

Sistema de votação eletrônica - Guia do eleitor

4. Selecione
“Consultar” do
processo eleitoral
em causa



**eVotUM**
Sistema de Votação Eletrónica da Universidade do Minho

33

Como verificar se o seu voto foi contabilizado?

Sistema de votação eletrônica - Guia do eleitor

5. Selecione a aba da eleição em causa
6. Selecione “Consulta das referências de voto”

 eVotUM

34

Como verificar se o seu voto foi contabilizado?

Sistema de votação eletrônica - Guia do eleitor

7. Pesquise a sua referência de voto (recebida por e-mail) e verifique se a mesma se encontra na “Lista de referências de voto”

 eVotUM

35

F. COMO ENVIAR MENSAGENS À COMISSÃO ELEITORAL

Como enviar mensagens à comissão eleitoral?

Sistema de votação eletrônica - Guia do eleitor

É disponibilizado um sistema de mensagens que permite que dentro do sistema eVotUM:

- Público e eleitor possam comunicar diretamente com a Comissão Eleitoral de uma determinada eleição;
- Comissão Eleitoral possa comunicar diretamente com um eleitor ou com um conjunto de eleitores (agrupado por processo eleitoral, eleição e/ou peso do voto).
- A mensagem será enviada para a caixa de mensagens no sistema eVotUM, assim como uma cópia será enviada para o email de comunicação identificado pelo eleitor ou pelos membros da Comissão Eleitoral (embora não seja possível responder ou enviar mensagens para o sistema eVotUM, a partir dos emails externos ao sistema);
- O sistema de mensagens mantém um histórico/arquivo das mensagens enviadas e recebidas.

 eVotUM

37

Como enviar mensagens à comissão eleitoral?

Sistema de votação eletrônica . Guia do eleitor

1. Aceda a <https://evotum.uminho.pt/>
2. Selecione “Autenticação”



eVotUM

38

Como enviar mensagens à comissão eleitoral?

Sistema de votação eletrônica . Guia do eleitor

3. Insira as **credenciais** de segurança utilizadas no acesso aos serviços da Universidade do Minho

eVotUM

39

Como enviar mensagens à comissão eleitoral?

Sistema de votação eletrônica . Guia do eleitor

5. Selecione “Nova”, insira destinatário, assunto e texto da mensagem, e de seguida clique em “Enviar” – uma cópia da mensagem será enviada para o seu e-mail de contacto.

eVotUM

40

G. COMO ALTERAR OS DADOS PESSOAIS

Como alterar os meus dados?

Sistema de votação eletrónica - Guia do eleitor

Dados do eleitor na plataforma eVotUM:

- Dados pré-definido – nome, foto, telefone e endereço de correio eletrónico (fornecidos à Universidade do Minho, aquando da obtenção de credenciais de segurança);
- Dados de contacto – pode alterar endereço de correio eletrónico e telefone, passando esses a ser os dados de contacto utilizados pelo sistema eVotUM;
- Modo de envio de chave de segurança – No modo de envio de chave de segurança, deve indicar como pretende receber o código secreto gerado automaticamente, que é enviado ao eleitor na parte terminal da votação, com o objetivo de confirmar a sua identidade.

Pode alterar os dados de contacto e o modo de envio de chave de segurança.



eVotUM

42

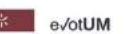
Como alterar os meus dados?

Sistema de votação eletrónica - Guia do eleitor

1. Aceda a <https://evotum.uminho.pt/>

2. Selecione “Autenticação”





eVotUM

43

Como alterar os meus dados?

Sistema de votação eletrónica - Guia do eleitor

3. Insira as **credenciais** de segurança utilizadas no acesso aos serviços da Universidade do Minho



AUTENTICAÇÃO

Escreva o seu login e password

Login

Password

☐ Lembrar o meu acesso

INICIAR SESSÃO



CARTÃO DE CIDADÃO

Alternativamente pode aceder utilizando o seu cartão de cidadão.



Insira o seu cartão no leitor SmartCard.

INICIAR SESSÃO



eVotUM

Como alterar os meus dados?

Sistema de votação eletrônica . Guia do eleitor

4. Selecione “Dados pessoais”



Como alterar os meus dados?

Sistema de votação eletrônica . Guia do eleitor

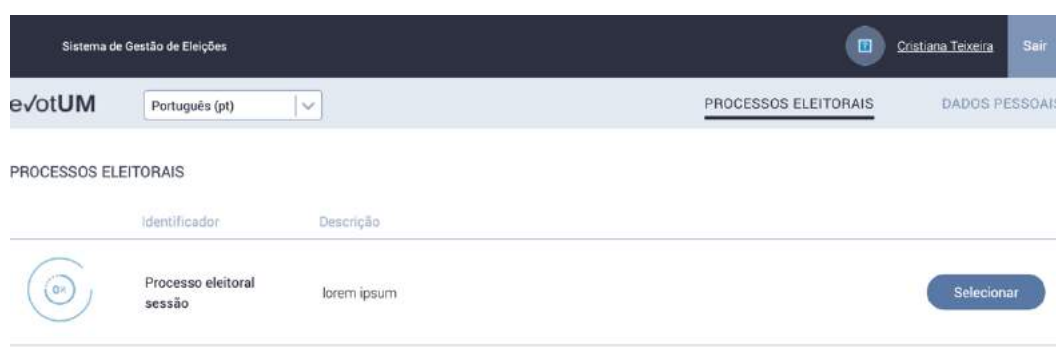
5. Pode alterar os dados de contacto e o modo de envio de chave de segurança. De seguida clique em “Guardar”

ANEXO II

GUIA DA COMISSÃO ELEITORAL

Neste segundo anexo é apresentado o Guia da Comissão Eleitoral, referente à gestão do processo eleitoral. Esta gestão é efetuada por um Membro da Comissão Eleitoral, autenticado na respetiva Área do Sistema eVotUM. O Guia apresenta quatro passos a serem cumpridos, necessariamente, pelo membro da comissão eleitoral, de modo a efetuar a devida gestão do processo eleitoral. São apresentadas, ainda, funcionalidades adicionais ao sistema de gestão de eleições, nos passos 5 e 6.

1. SELECIONAR PROCESSO ELEITORAL A CONFIGURAR



2. CONFIGURAR NÍVEL DE SEGURANÇA



- a. Configurar o Nível de Segurança das diferentes ações que podem ser efetuadas pela Comissão Eleitoral [Radio Button]:
 - i. Simples: Necessária apenas uma das componentes do segredo para executar a ação, ou seja, apenas um elemento da Comissão Eleitoral (1);
 - ii. Forte: Necessárias $(M/2)+1$ componentes distintas do segredo para executar a ação, ou seja, metade mais um elementos da Comissão Eleitoral (M = Número total de membros da Comissão Eleitoral);
 - iii. Crítico: Necessárias M componentes distintas do segredo para executar a ação, ou seja, todos os membros da Comissão Eleitoral.

Ações	Simple (1)	Força (M/2+1)	Crítico (M)
Alterar o membro da comissão eleitoral que pode responder às mensagens eletrônicas.	☐	☐	☐
Configuração inicial do processo eleitoral	☐	☐	☐
Publicar documentos na página pública do processo eleitoral	☐	☐	☐
Iniciar contagem dos votos	☐	☐	☐
Encerrar o período de votação da eleição.	☐	☐	☐
Iniciar o período de votação da eleição	☐	☐	☐
Outras ações	☐	☐	☐

[Guardar](#)

b. Guardar Configurações do Nível de Segurança [Botão Guardar]

- i. Autorizar Ação de Guardar [Botão Autorizar]: Ação definida como tendo um nível de segurança crítico, sendo necessárias M componentes distintas do segredo para executar a ação.

1. Carregar Ficheiros das componentes do segredo de todos os membros da Comissão Eleitoral [Botão Escolher Ficheiro].

evotUM

Fechar

Autorização de ação

Esta ação foi definida como tendo um nível de segurança crítico - São necessárias M componentes distintas do segredo, enviado aos membros da comissão eleitoral, para executar a ação.
(M = número total de membros da comissão eleitoral)
Por favor carregue os ficheiros com as componentes.

Key 1: [Escolher ficheiro](#)

Key 2: [Escolher ficheiro](#)

Key 3: [Escolher ficheiro](#)

[Autorizar](#)

3. EDITAR PROCESSO ELEITORAL

0%

Processo eleitoral sessão

lorem ipsum

[Editar](#)

a. Editar Informação Geral [Tab Dados Gerais]

- i. Inserir Data de Publicação do Processo Eleitoral [Date Picker]
- ii. Rever/Alterar/Adicionar Informação Geral:

1. Logótipo [Botão Escolher Ficheiro];
2. Identificador do Processo Eleitoral [PT/EN] [Write In];
3. Descrição do Processo Eleitoral [PT/EN] [Write In];
4. Documentos referentes ao Processo Eleitoral [Botão Escolher Ficheiro].

iii. Guardar Edição [Botão Guardar]

Edição do processo eleitoral

Dados gerais | Comissão eleitoral | Responsável pela comunicação

Por favor insira a informação geral necessária à criação do processo eleitoral.

Data de publicação: 09-06-2022 15:23

Logo (tamanho mínimo 135px x 100px):

uploads/2022/06/images/icon-sem-juros-1 Escolher ficheiro

Identificador do processo eleitoral [pt]: Processo eleitoral sessão

Identificador do processo eleitoral [en]: Processo eleitoral sessão 'EN'

Descrição do processo eleitoral [pt]: lorem ipsum

Descrição do processo eleitoral [en]: lorem ipsum

Nome da Categoria Do Documento: Documento

Nome Do Documento: Ata

Ficheiro Do Documento: uploads/2022/06/docum Escolher ficheiro

2ª Ata

uploads/2022/06/docum Escolher ficheiro

Guardar

b. Visualizar membros da Comissão Eleitoral [Tab Comissão Eleitoral]

Edição do processo eleitoral

Dados gerais | Comissão eleitoral | Responsável pela comunicação

Processo eleitoral Processo eleitoral sessão

#	Nome	Role	Designação	Endereço De Correio Eletrónico Pré-Definido	Contact Phone Number
1	Sara Coelho	Presidente	Sara	sfc@eurotux.com	+351912233441
2	Cristiana Teixeira	Membro	Cristiana	cristianateixeira98@gmail.com	+351915219445
3	Andreia Félix	Membro	Andreia	adf@eurotux.com	+351912233441
4	Sandro Rodrigues	Membro	Sandro	sfr@eurotux.com	+351912233441

c. Editar Responsável pela Comunicação [Tab Responsável pela Comunicação]

- ii. Selecionar Membro da Comissão Eleitoral [Dropdown List];
- iii. Guardar Edição [Botão Guardar].

Edição do processo eleitoral

Dados gerais Comissão eleitoral Responsável pela comunicação

Processo eleitoral Processo eleitoral sessão

Por favor selecione o membro da comissão eleitoral que irá responder às mensagens eletrónicas.

Responsável pela comunicação

Sara Coelho (Presidente)

Guardar

4. GERIR PAINEL DE ELEIÇÕES

Processo eleitoral sessão lorem ipsum

Editar

02-06-2022 15:21

Painel de eleições

a. Editar Eleição [Icon Button]:

i. Editar Configurações [Tab Configuração]

1. Identificador da Eleição [PT/EN] [Write In];
2. Descrição da Eleição [PT/EN] [Write In];
3. Número máximo de candidatos a escolher no boletim [Dropdown List];
4. Opção Write In no Boletim de voto [Radio Button];
5. Opção Ordenação de Candidatos no Boletim de voto [Radio Button];
6. Opção Pesos de Voto distintos no Boletim de voto [Radio Button];
7. Opção Método de Hondt no Boletim de voto [Radio Button];
8. Guardar Edição [Botão Guardar].

Identificador da eleição [pt]

Eleição teste sessão 1

Identificador da eleição [en]

Eleição sessão 1 en

Descrição da eleição [pt]

Eleição teste sessão 1

Descrição da eleição [en]

Eleição teste sessão 1

1. Número máximo de candidatos a escolher no boletim

1

2. Boletim de voto com write in?

☐ Sim ☒ Não

3. Boletim de voto permite ordenar candidatos?

☐ Sim ☒ Não

4. Os votos podem ter pesos diferentes?

☐ Sim ☒ Não

5. Utilizar método de Hondt?

☐ Sim ☒ Não

Guardar

ii. Editar Calendário Eleitoral [Tab Calendário Eleitoral]

1. Definir Período de Publicação de Listas Candidatas:
 - a. Início do Período [Date/Hour Picker];
 - b. Fim do Período [Date/Hour Picker];
2. Definir Período de Publicação do Caderno Eleitoral:
 - a. Data de Publicação do Caderno Eleitoral Provisório [Date/Hour Picker];
 - b. Data de Publicação do Caderno Eleitoral Definitivo [Date/Hour Picker];
 - c. Início do Período de Reclamação [Date/Hour Picker];
 - d. Fim do Período de Reclamação [Date/Hour Picker];
3. Definir Período de Votação:
 - a. Início do Período de Votação [Date/Hour Picker];
 - b. Fim do Período de Votação [Date/Hour Picker];
4. Definir Período de Publicação de Resultados:
 - a. Data de Publicação [Date/Hour Picker];
 - b. Início do Período de Homologação [Date/Hour Picker];
 - c. Fim do Período de Homologação [Date/Hour Picker];
5. Guardar Edição [Botão Guardar].

2.1 Período de apresentação de listas candidatas	
Início: 02-06-2022 14:45	Fim: 03-06-2022 13:00
2.2 Caderno eleitoral	
Publicação do caderno eleitoral provisório: 03-06-2022 14:15	Publicação do caderno eleitoral definitivo: 03-06-2022 15:15
Período de reclamação - início: 03-06-2022 14:30	Período de reclamação - fim: 03-06-2022 15:00
2.3 Período de votação	
Início: 03-06-2022 15:00	Fim: 03-06-2022 18:00
2.4 Resultados	
Data de publicação: 03-06-2022 18:30	Período de homologação - fim: 03-06-2022 21:00
Período de homologação - início: 03-06-2022 20:00	
<button>Guardar</button>	

iii. Editar Peso do Voto [Tab Peso do Voto]

1. Introduzir Pesos de Voto permitidos na Eleição

Eleição A

Configuração | Calendário eleitoral | **Peso do voto** | Caderno eleitoral | Candidatos | Boletim de voto

Por favor associe o identificador (Id) com o peso do voto

Id	Descrição [PT]	Descrição [EN]	Peso
um	Um	One	1

+

iv. Editar Caderno Eleitoral [Tab Caderno Eleitoral]

1. Carregar Caderno Eleitoral [Botão Escolher Ficheiro]: Ficheiro CSV UTF-8, delimitado pelo caracter ponto e vírgula, constituído pelos campos `personnel_number`, `name`, `email`, `category` (pesos de voto, se aplicável);
2. Submeter Edição [Botão Submeter].

Descrição | Documento

Escolher ficheiro Submeter

Nome Do Documento	Versão	Publicado Em	Carregado	Documento PDF
CSV file	202206021518	02-06-2022 16:18	✓	

Caderno eleitoral publicado

tv - refresque a página para actualizar o estado

v. Editar Candidatos [Tab Candidatos]

1. Editar/Inserir Nome do Candidato/Lista [Write In];
2. Editar/Inserir Nome do Documento [Write In];
3. Carregar Documento [Botão Escolher Ficheiro];
4. Adicionar Documento [Icon Button];
5. Apagar Candidato [Icon Button];
6. Adicionar Candidato [Icon Button];
7. Guardar Edição [Botão Guardar].

The screenshot shows a web interface for managing election candidates and documents. It features a table with columns for 'Imagem/Logotipo', 'Nome Do Candidato/Lista De Candidatos', 'Nome Do Documento', and 'Ficheiro Do Documento'. Two rows are visible, each with a candidate (A and B) and a document named 'Candidato1' and 'Candidato2'. Each row has a file upload button labeled 'Escolher ficheiro' and a date 'uploads/2022/06/0/'. Below the table is a '+ ' button and a 'Guardar' button.

vi. Editar Boletim de Voto [Tab Boletim de Voto]

1. Inserir Instruções a Figurar no Boletim de Voto [Write In];
2. Selecionar Modo de Apresentação [Radio Button];
3. Misturar Candidatos [Botão Misturar Candidatos];
4. Pré-visualizar Boletim de Voto [Botão Pré-Visualização Do Boletim de Voto];
5. Guardar Edição [Botão Guardar].

The left screenshot shows the 'Boletim de Voto' tab with instructions for writing in candidates and a list of candidates (A and B). The right screenshot shows the 'Pré-Visualização' button, which is used to preview the ballot paper.

b. Gerir Painel do Dia da Eleição [Botão Gerir]

i. Iniciar Votação [Tab Iniciar Votação]

1. Rever/Editar Início do Período de Votação [Date/Hour Picker];
2. Aprovar Início do Período de Votação [Botão Aprovar Início do Período de Votação].

Início do período de votação:

03-06-2022 15:05  Fuso horário GMT

Junho 2022

Seg	Ter	Qua	Qui	Sex	Sab	Dom
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Aprovar início do período de votação

Horas

Minutos

Agora Fechar

ii. Fechar Votação [Tab Fechar Votação]

1. Rever/Editar Fim do Período de Votação [Date/Hour Picker];
2. Aprovar Fim do Período de Votação [Botão Aprovar Fim do Período de Votação]

Fim do período de votação:

03-06-2022 16:00  Fuso horário GMT

Junho 2022

Seg	Ter	Qua	Qui	Sex	Sab	Dom
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Aprovar fim do período de votação

Horas

Minutos

Agora Fechar

iii. Escrutinar Votos [Tab Escrutinar Votos]

1. Iniciar Contagem de Votos [Botão Iniciar Contagem de Votos]

Iniciar votação

Fechar votação

Escrutinar votos

Por favor dê início à contagem de votos

Iniciar contagem de votos

Resultados da eleição		
Número de votos totais na urna eleitoral:		
1		
Candidato/Lista De Candidatos	Votos	Porcentagem
Candidato 2	1	100.00%
Candidato 1	0	0.00%
Voto em branco	0	0.00%
Informação adicional		
Boletins De Voto Inválidos	Boletins De Voto Submetidos	Boletins De Voto Que Não Finalizaram A Submissão
0	1	0
Boletins Que Não Foram		
1		

- iv. Visualizar Número de Boletins na Urna em Período de Votação [Botão Número Total de Boletins na Urna Eleitoral]

Número total de boletins na urna eleitoral		
Número total de boletins na urna eleitoral:		
1		
Pedido Por	Data	# Boletins
Cristiana Teixeira	03-06-2022 15:19	1
Cristiana Teixeira	03-06-2022 14:28	0
Cristiana Teixeira	02-06-2022 17:58	0
Sara Coelho	02-06-2022 15:32	0

5. VISUALIZAR MENSAGENS

PROCESSO ELEITORAL SESSÃO

Configuração do nível de segurança

Mensagens (0)

- Visualizar Mensagens Recebidas [Botão Recebidas];
 - Ler Mensagem [Click Link];
 - Arquivar Mensagem [Icon Button].
- Visualizar Mensagens Enviadas [Botão Enviadas];
- Visualizar Mensagens Arquivadas [Botão Arquivadas].

MENSAGENS

Recebidas (1)

Enviadas

Arquivadas

Cristiana Teixeira (cristiana Teixeira98@gmail.com)

03-06-2022 14:31

Reclamação - Eleição: Eleição teste sessão 1

Reclamação

RECLAMAÇÃO - ELEIÇÃO: ELEIÇÃO TESTE SESSÃO 1

Recebidas

Enviadas

Arquivadas

De: Cristiana Teixeira (cristiana Teixeira98@gmail.com)

Para: Cristiana Teixeira (cristiana Teixeira98@gmail.com)

Assunto: Reclamação - Eleição: Eleição teste sessão 1

03-06-2022 14:31

Reclamação

Voltar

6. VISUALIZAR HISTÓRICO DE AÇÕES

Sistema de Gestão de Eleições

Cristiana Teixeira

Sair

evotUM

Português (pt)

PROCESSOS ELEITORAIS

DADOS PESSOAIS

Processos eleitorais > Processo eleitoral sessão

PROCESSO ELEITORAL SESSÃO

Configuração do nível de segurança

Mensagens (0)

Identificador	Descrição	Data De Publicação
01 Processo eleitoral sessão	lorem ipsum	Editar 02-06-2022 15:21 Panel de eleições

Data de publicação: Publicação de documentos na página pública do processo eleitoral

HISTÓRICO DE AÇÕES

03-06-2022 14:28

Cristiana Teixeira

O utilizador Cristiana Teixeira criou o/a Query de contagem

Eleição teste sessão 1 (Cristiana Teixeira (cristiana Teixeira98@gmail.com)) - 0

03-06-2022 12:07

Cristiana Teixeira

O utilizador Cristiana Teixeira atualizou o/a candidato

Candidato 1

03-06-2022 12:07

Cristiana Teixeira

O utilizador Cristiana Teixeira atualizou o/a candidato

Candidato 2

02-06-2022 11:26

Cristiana Teixeira

O utilizador Cristiana Teixeira atualizou o/a eleição

Eleição teste sessão 1

02-06-2022 11:26

Cristiana Teixeira

O utilizador Cristiana Teixeira atualizou o/a eleição

Eleição teste sessão 1

ANEXO III

GUIA DO RESPONSÁVEL INSTITUCIONAL

Neste terceiro anexo é apresentado o Guia do Responsável Institucional, referente à criação de um processo eleitoral. Este processo é efetuado pelo Responsável Institucional, autenticado na respetiva Área do Sistema eVotUM. Importa ainda referir que o processo inclui duas etapas, sendo a segunda efetuada, automaticamente, pelo sistema. O Guia apresenta cinco passos a serem cumpridos, necessariamente, na Etapa 1, pelo Responsável Institucional, de modo a efetuar a devida criação do processo eleitoral. Posteriormente, para efeitos de uma boa compreensão, é esclarecido o processo à luz da Etapa 2. Finalmente, são esclarecidos os processos de cifra e decifra dos votos.

A. ETAPA 1

1. FORNECER DADOS GERAIS REFERENTES AO PROCESSO ELEITORAL

- a. Carregar Ficheiro referente ao Logótipo do Processo Eleitoral [Botão Escolher Ficheiro];
- b. Inserir Identificador do Processo Eleitoral [PT] [Write In];
- c. Inserir Descrição do Processo Eleitoral [PT] [Write In];
- d. Inserir Identificador do Processo Eleitoral [EN] [Write In];
- e. Inserir Descrição do Processo Eleitoral [EN] [Write In];
- f. Selecionar Tipo de Processo Eleitoral [Radio Button];
- g. Avançar para o Próximo Passo [Botão Seguinte].

The screenshot shows the 'eVotUM' web application interface. At the top, there's a header with the logo, a language dropdown set to 'Português (pt)', and navigation tabs for 'PROCESSOS ELEITORAIS' (selected) and 'DADOS PESSOAIS'. Below the header, a breadcrumb trail reads 'Processos eleitorais > Novo'. The main section is titled 'Criação do processo eleitoral' and contains three sub-tabs: 'Dados gerais' (active), 'Eleições', and 'Geração eleitoral'. A message box states: 'Por favor insira a informação geral necessária à criação do processo eleitoral.' Below this, there's a 'Logo' upload section with a text input showing 'processo-eleitoral.png' and a button 'Escolher ficheiro'. The form then has four text input fields arranged in a 2x2 grid: 'Identificador do processo eleitoral [pt]:' with the value 'Processo Eleitoral [Teste]', 'Identificador do processo eleitoral [en]:' with 'Electoral Process [Teste]', 'Descrição do processo eleitoral [pt]:' with 'Processo Eleitoral', and 'Descrição do processo eleitoral [en]:' with 'Electoral Process'. At the bottom, there's a question 'É um processo eleitoral de teste?' with radio buttons for 'Sim' (selected) and 'Não'. A 'Seguinte' button is located at the bottom right.

2. FORNECER DADOS CONCRETOS REFERENTES ÀS ELEIÇÕES

a. Criação de Eleição

i. Identificar Eleição

- 1. Inserir Identificador da Eleição [PT] [Write In];**
- 2. Inserir Descrição da Eleição [PT] [Write In];**
- 3. Inserir Identificador da Eleição [EN] [Write In];**
- 4. Inserir Descrição da Eleição [EN] [Write In].**

ii. Definir Período de Apresentação de Listas Candidatas

- 1. Definir Início do Período [Date/Hour Picker];**
- 2. Definir Fim do Período [Date/Hour Picker].**

iii. Definir Caderno Eleitoral

- 1. Definir Horário de Publicação do Caderno Eleitoral Provisório [Date/Hour Picker];**
- 2. Definir Início do Período de Reclamação [Date/Hour Picker];**
- 3. Definir Fim do Período de Reclamação [Date/Hour Picker];**
- 4. Definir Horário de Publicação do Caderno Eleitoral Definitivo [Date/Hour Picker].**

iv. Definir Período de Votação

- 1. Definir Início do Período de Votação [Date/Hour Picker];**
- 2. Definir Fim do Período de Votação [Date/Hour Picker].**

v. Definir Resultados

- 1. Definir Data de Publicação de Resultados [Date/Hour Picker];**
- 2. Definir Início do Período de Homologação [Date/Hour Picker];**
- 3. Definir Fim do Período de Homologação [Date/Hour Picker].**

b. Avançar para o Próximo Passo [Botão Seguinte]

Sistema de Gestão de Eleições

evotUM

PROCESSOS ELEITORAIS

Processos eleitorais - Nova

Criação do processo eleitoral

Por favor insira a informação necessária à criação da(s) eleição(ões)

1.1 Eleições

Identificador da eleição (pt)

Identificador da eleição (en)

Descrição da eleição (pt)

Descrição da eleição (en)

1.1.1 Período de apresentação de listas candidatas

Início

Fim

1.1.2 Calendar eleitoral

Publicação do sistema eleitoral provisório

Publicação do sistema eleitoral definitivo

Período de candidatura - Início

Período de candidatura - Fim

1.1.3 Período de votação

Início

Fim

1.1.4 Resultados

Data de publicação

Período de homologação - Início

Período de homologação - Fim

Anterior

Seguinte

3. FORNECER DADOS REFERENTES À COMISSÃO ELEITORAL

- a. Inserir Membros da Comissão Eleitoral
 - i. Inserir Username do Membro da Comissão Eleitoral [Write In];
 - ii. Verificar Validez do Username Inserido [Botão Verificar];
 - iii. Inserir Designação do Membro da Comissão Eleitoral [Write In];
 - iv. Selecionar Função do Membro da Comissão Eleitoral [Dropdown List].
- b. Avançar para o Próximo Passo [Botão Seguinte].

Sistema de Gestão de Eleições

evotUM

PROCESSOS ELEITORAIS

Processos eleitorais - Nova

Criação do processo eleitoral

Processo eleitoral Processo Eleitoral [Teste]

Por favor insira os membros da comissão eleitoral

Username	Endereço De Correio Eletrónico	Nome	Designação	Função	Número De Telefone De Contacto
crisiana.teixeira	crisanteixeira98@gmail.com	Cristiana Teixeira	Cristiana	Presid. 1	+351915219445
sic	efc@evotum.com	Sara Cordeiro	Sara	Memb. 2	+351912233441
atf	atf@evotum.com	Andreia Félix	Andreia	Memb. 3	+351912233441

Anterior

Seguinte

4. AUTENTICAR COM CHAVE MÓVEL DIGITAL

a. Visualizar Sumário do Processo Eleitoral;

Processos eleitorais - Novo

criação do processo eleitoral Imprimir

Sumário

1. Dados gerais

Identificador do processo eleitoral	Designação
Processo Eleitoral (Teste)	Processo Eleitoral Teste

1.1 Dados gerais (Eleição Teste 1)

Identificação da eleição	Designação
Eleição Teste 1	Eleição Teste 1

Calendário eleitoral

Período de apresentação de listas candidatas

Data de início	Fuso horário GMT	Data de fim	Fuso horário GMT
01-07-2022 09:00		01-07-2022 09:15	

Cadernos Eleitorais

Publicação do caderno eleitoral provisório	Fuso horário GMT	Publicação do caderno eleitoral definitivo	Fuso horário GMT
01-07-2022 09:30		01-07-2022 10:00	

Período de reclamação - início	Fuso horário GMT	Período de reclamação - fim	Fuso horário GMT
01-07-2022 09:40		01-07-2022 09:50	

Período de votação

Data de início	Fuso horário GMT	Data de fim	Fuso horário GMT
01-07-2022 10:15		01-07-2022 10:30	

Resultado

Data de publicação	Fuso horário GMT	Período de homologação - fim	Fuso horário GMT
01-07-2022 10:45		01-07-2022 11:15	

2. Comissão eleitoral

#	Nome	Função	Designação	Endereço De Correio Eletrónico (Pai, Confirmado)	Contacto Móvel Number
1	Cristiano Teixeira	Presidente	Cristiana	cristianoteixeira9@gmail.com	+351915219485
2	Sara Cordeiro	Membro	Sara	sfc@eurotum.com	+351912233441
3	Andréia Félix	Membro	Andréia	ad@eurotum.com	+351912233441

Anterior Criar

b. Criar Processo Eleitoral [Botão Criar];

i. Finalizar Processo de Autenticação com Chave Móvel Digital [Botão Autenticar];

evotUM Fechar

Autenticação com 'Chave Móvel Digital'

Ao clicar em 'Autenticar' será redirecionado para o site da AUTENTICAÇÃO.GOV.PT do Estado Português, onde finalizará este processo de autenticação.

AUTENTICAÇÃO.GOV.PTAutenticar

Saltar autenticação

- ii. Finalizar Processo de Autenticação com a Palavra-Chave da Entidade de Certificação raiz da Hierarquia de Confiança eVotUM [Write In];
- c. Gerar Certificado Digital, Chave Privada de Cifra de Votação e respetivo Segredo Dividido [Botão Gerar].

B. ETAPA 2

1. Após a segunda autenticação do Responsável Institucional, através da Chave Móvel Digital, a Plataforma eVotUM:
 - a. Gera segredo, **ks**, de acesso às chaves privadas de cada uma das eleições, com 64 caracteres [Crypto 4.4.0];
 - b. Gera par de chaves assimétricas, chave privada cifrada com **ks**, [Crypto 9.1.0 e Crypto 9.4.0] e *certificate requests* para todos os certificados das eleições [Crypto 9.2.0].
 - i. Os dados, para a geração do *certificate request* são: *commonName* (<composição do nome da eleição com o processo eleitoral>), *countryName* (PT), *stateOrProvinceName* (Portugal), *localityName* (Braga), *organizationName* (Universidade do Minho), *organizationalUnitName* (eVotUM Poll);
 - c. Divide **ks** em **n** (número de elementos da comissão eleitoral) componentes, sendo necessários $(n/2 + 1)$ elementos para reconstruir **ks** [Crypto 4.1.0];
 - d. Envia *certificate requests* e chave privada de assinatura da EC, em javascript, para o browser do Responsável Institucional [Crypto 9.3.2].
2. O Responsável Institucional insere o segredo de acesso à chave privada de assinatura da EC, em javascript, e acede à chave privada e aos *certificate requests*, gerando certificados de eleição [Crypto 9.3.2 e Crypto 9.3.1];
 - a. Os dados para a geração do certificado da eleição são: *serialNumber* (<número inteiro único. Se for utilizado um ID de eleição único inteiro, pode ser utilizado esse ID>), *notBefore* (0 – i.e., período de validade começa com a emissão do certificado), *notAfter* (data da eleição + 9 meses – nota que

se tem de transformar para os segundos a partir da hora/data de geração/emissão do certificado).

3. Certificados de eleição são devolvidos à plataforma eVotUM, que os guarda;
4. A plataforma eVotUM envia uma das n componentes do segredo ks , a um dos elementos da Comissão Eleitoral. Cada elemento da Comissão recebe uma componente diferente.

C. CIFRA DO VOTO

1. Cada voto é cifrado com o certificado da respetiva eleição [Crypto 5.2.0];
2. Para verificar, se necessário, se o certificado é bem formado: [Crypto 5.5.0];
3. Para verificar, se necessário, se o certificado se encontra na hierarquia de confiança: [Crypto 5.3.0].

D. DECIFRA DO VOTO

1. Cada voto é decifrado com a chave privada ‘associada’ ao certificado da eleição;
2. Para obter a password de acesso à chave privada: [Crypto 4.2.0];
3. Para decifrar o voto: [Crypto 5.4.0];
 - a. A password só pode ser gerada em memória e deve ser descartada/apagada imediatamente após a sua utilização.

ANEXO IV

REQUISITOS FUNCIONAIS IMPLEMENTADOS NO ÂMBITO DO PROJETO DA EVOTUM

Neste quarto anexo é apresentada, de forma integral, a descrição detalhada de todos os requisitos funcionais implementados no âmbito do projeto de conceção da plataforma eVotUM, conforme se pode observar na tabela seguinte.

Esta informação, demasiado extensa para ser apresentada no corpo da dissertação, pode ser resumidamente encontrada no capítulo 3, secção referente aos requisitos funcionais.

Requisito	Categoria	Subcategoria	Descrição
REQ 1.1	Geral	Design	O tema genérico deve estar adaptado aos browsers Internet Explorer 11, Firefox 34, Chrome 40, Safari, e versões superiores.
REQ 1.2	Geral	Perfis	Devem existir os seguintes perfis de utilizadores: • Anónimo: Acesso ao sistema de consultas; • Comissão eleitoral: Acesso às eleições disponíveis no sistema de gestão de eleições; • Responsável Institucional: Acesso ao formulário de pedido de criação do processo eleitoral, disponível no sistema de gestão de eleições; • Eleitor: Acesso ao sistema de consultas e ao sistema de votação; • Administrador: Acesso ao Sistema de Administração.
REQ 2.1	Sistema de Consultas	Página Inicial	A Homepage deve apresentar a informação seguinte: • Logótipo eVotUM e frase estática “Sistema de Votação Eletrónica da Universidade do Minho”: Redireciona para a Homepage ao clicar; • Menu Estático: Processos Eleitorais [REQ 2.8], Como Funciona [REQ 2.11], Contactos [REQ 2.12]; • Texto estático sobre a plataforma; • Botão "Verificar cadernos eleitorais": Redirecionada para a listagem de processos eleitorais [REQ 2.8]; • Botão "Autentique-se para votar": Redireciona para a página de autenticação [REQ 2.6].
REQ 2.2	Sistema de Consultas	Cabeçalho e Rodapé	O cabeçalho deve ser constituído pelos seguintes itens: • Logótipo da universidade do Minho; • Preferências [REQ 2.3]; • Pesquisa [REQ 2.4]; • FAQs: Redireciona para a página geral de perguntas frequentes; • Idioma: PT ou EN. Se o idioma selecionado for PT, apresenta o link para selecionar EN, e vice-versa; • Botão de Autenticação [REQ 2.6]: Visível apenas caso o utilizador seja anónimo;

			• Foto do eleitor: Visível apenas caso o utilizador esteja autenticado; • Nome do eleitor com link para a edição de dados pessoais: Visível apenas caso o utilizador esteja autenticado; • Botão de log out, denominado "sair": Visível apenas caso o utilizador esteja autenticado; • Logótipo do eVotUM: Link redirecionada para a página inicial do portal; • Menu [REQ 2.5].
REQ 2.3	Sistema de Consultas	Configurações	Ao clicar no botão “Configurações” surge uma janela onde o utilizador pode adaptar as suas preferências: • Tamanho da fonte: Por defeito está selecionado o tamanho normal e pode ser alterado para o tamanho Grande. As preferências selecionadas ficam gravadas apenas durante a sessão; • Cor: Por defeito está selecionada a cor azul e pode ser alterada para vermelho. As preferências selecionadas ficam gravadas apenas durante a sessão.
REQ 2.4	Sistema de Consultas	Pesquisa	Ao clicar na lupa do cabeçalho surge a área de pesquisa por texto livre. A página de resultados apresenta o número de resultados encontrados para determinado termo de pesquisa, e a lista de resultados, em que para cada item é apresentada a seguinte informação: • Título; • Descrição.
REQ 2.5	Sistema de Consultas	Menu	Os itens de menu variam conforme o utilizador é anónimo ou autenticado: Utilizador anónimo: • Processos Eleitorais [REQ 2-8]; • Como Funciona [REQ 2.11]; • Contactos [REQ 2.12]. Utilizador autenticado: • Os meus processos eleitorais [REQ 2.13]; • Dados pessoais [REQ 2.14]; • Mensagens [REQ 2.15]; • Histórico [REQ 2.16].
REQ 2.6	Sistema de Consultas	Autenticação	O utilizador anónimo ao clicar no botão "Autenticação", que surge no cabeçalho, ou no botão "Autentique-se para votar" é redirecionado para a página de login. Nesta página surge o formulário composto pelos campos "Email" e "Senha de acesso". A autenticação deve estar integrada com a autenticação da DTSI. Deve ser possível memorizar os dados de acesso no browser, selecionando a checkbox "memorizar".

REQ 2.7	Sistema de Consultas	Páginas Institucionais	O portal deve apresentar, em rodapé, as seguintes páginas institucionais: • Sobre o eVotUM; • Perguntas frequentes; • Política de segurança e informação; • Política de privacidade; • Termos de utilização; • Mapa do Site; • Contactos.
REQ 2.8	Sistema de Consultas	Processos Eleitorais: Listagem	A listagem apresenta os últimos três processos eleitorais publicados, ordenados do mais recente para o mais antigo. Para cada processo eleitoral é apresentada a seguinte informação: • Logótipo; • Nome do processo eleitoral; • Estado do processo eleitoral; • Botão "Consultar": redireciona para a página de consulta do processo eleitoral [REQ 2.9]. No topo da listagem surge o botão "Arquivo" que redirecionada para a página de arquivo dos processos eleitorais [REQ 2.9]. No final da listagem surge o botão "Ver todos" que redireciona para uma página que apresenta a lista de todos os processos eleitorais abertos. Este botão só é apresentado no caso de existirem mais processos eleitorais no estado aberto.
REQ 2.9	Sistema de Consultas	Processos Eleitorais: Página de Consulta	O eleitor autenticado, bem como o utilizador anónimo, ao clicar no botão "Consultar" disponível na listagem de processos eleitorais, é redirecionado para a página de consulta de um processo eleitoral. A página de consulta de um processo eleitoral apresenta a seguinte estrutura: [Informações gerais do processo eleitoral] • Texto descritivo do processo eleitoral; • Documentos associados ao processo eleitoral, em que para documento é apresentado o nome associado ao documento, seguido dos links para visualização dos ficheiros. [Eleições] A lista de eleições apresenta todas as eleições associadas ao processo eleitoral, independentemente do seu estado. Por defeito é apenas apresentado o nome da eleição e uma seta, em que ao clicar abre a respetiva informação

			detalhada. Ao clicar numa eleição diferente é escondida a informação da anterior. A informação detalhada a apresentar é a seguinte: • Estado atual; • Período de verificação; • Texto descritivo da eleição; • Período de votação; • Calendário eleitoral; • Caderno eleitoral; • Lista de candidatos e respetivos ficheiros associados; • Botão "Apresentar reclamação": Ao clicar abre o formulário de envio de mensagens. Se a Página de Consulta for acedida por um eleitor que faz parte do caderno eleitoral, é apresentada ainda a seguinte informação: • Botão "Votar" no canto superior direito da listagem. Ao clicar no botão, o eleitor é redirecionado para a página de votação [REQ 3.1]; • Botão "Consulta de referência de votos". Ao clicar no botão, o eleitor é redirecionado para a página de consulta de referência de votos [REQ 2.17].
REQ 2.10	Sistema de Consultas	Processos Eleitorais: Arquivo	Ao clicar no botão "Arquivo" que surge na listagem de processos eleitorais, o utilizador é redirecionado para a página de arquivo de processos eleitorais que apresenta a seguinte estrutura: [Filtros de pesquisa] Os processos eleitorais podem ser filtrados pelos seguintes critérios: • Paginação: Corresponde ao número de itens visíveis por página e deve ter as opções 5 ou 10. Por defeito deve existir uma paginação de 5 em 5 itens; • Ano: Devolver todos os anos que tiveram, pelo menos, uma eleição, desde a primeira eleição existente na plataforma, até ao momento atual. [Listagem de processos eleitorais] Apresenta todos os processos eleitorais que se encontram no estado fechado, ordenados por data de publicação do mais recente para o mais antigo. Para cada processo deve ser apresentada a seguinte informação: • Logótipo; • Nome do processo eleitoral; • Lista de eleições do processo eleitoral: Ao clicar redireciona para a página de consulta do processo eleitoral [REQ 2.9]. • Estado do processo eleitoral;

			• Botão "Consultar": Ao clicar redireciona para a página de consulta do processo eleitoral [REQ 2.9]. Não é possível visualizar mais informação sobre os processos eleitorais já fechados, apenas a que surge nesta listagem.
REQ 2.11	Sistema de Consultas	Como funciona	Página estática que apresenta informação relativa à plataforma. O botão "Guia do Eleitor" redireciona o utilizador para uma página que contém o guia de utilização da eVotUM.
REQ 2.12	Sistema de Consultas	Contactos	O utilizador anónimo, bem como o eleitor autenticado, ao clicar no link "Contactos" que surge no cabeçalho ou rodapé é redirecionado para a página de contactos. A página de contactos deve ser composta pela seguinte estrutura: [Formulário de contacto] • Nome; • Email; • Assunto; • Mensagem; • Campo reCAPTCHA. Após submetida, a mensagem é enviada para o responsável institucional. Caso a submissão seja efetuada com sucesso surge uma mensagem informativa com o texto "O seu pedido foi submetido com sucesso". Caso algum dos campos tenha um erro, é apresentada a respetiva mensagem de erro. [Informação de contacto] • Nome; • Email; • Telefone; • Morada; • Mapa de localização.
REQ 2.13	Sistema de Consultas	Os meus processos eleitorais	O eleitor autenticado ao clicar no link "Os meus processos eleitorais", que surge no cabeçalho, é redirecionado para a página que apresenta a listagem de processos eleitorais das quais o eleitor faz parte. Esta listagem apresenta os processos ordenados do mais recente para o mais antigo. Para cada processo eleitoral é apresentada a seguinte informação: • Logótipo; • Nome do processo eleitoral; • Estado do processo eleitoral;

			• Botão "Consultar": redireciona para a página de consulta do processo eleitoral [REQ 2.9]; • Botão "Votar": redireciona para a página de votação das eleições do respetivo processo eleitoral [REQ 3.1]. No final da listagem surge um botão "Processos Eleitorais em falta" e ao clicar surge uma janela pop-up a informar o eleitor que para fazer uma reclamação associada a uma eleição da qual não faz parte no momento, deve fazer logout e aceder à consulta pública (para utilizadores anónimos) do respetivo processo eleitoral.
REQ 2.14	Sistema de Consultas	Dados pessoais	O eleitor autenticado ao clicar no link "Dados pessoais", que surge no cabeçalho, é redirecionado para a página que apresenta os seus dados pessoais. Esta página apresenta a seguinte estrutura: • Imagem de perfil: Fornecida pela DTSI e não pode ser editada; • Nome: Fornecido pela DTSI e não pode ser editado; • Email: Fornecido pela DTSI e não pode ser editado; • Telemóvel: Fornecido pela DTSI; • Telemóvel para comunicação: por defeito aparece o mesmo da DTSI, mas pode ser editado pelo eleitor; • Email para comunicação: por defeito aparece o mesmo da DTSI e pode ser editado pelo eleitor nesta área; • Forma de envio de PIN de votação: Apresenta as opções SMS e Email e por defeito tem a opção SMS selecionada. Caso o utilizador não tenha número de telemóvel associado tem por defeito a opção Email selecionada; No final deve existir um botão "Guardar" para preservar a edição dos campos editáveis.
REQ 2.15	Sistema de Consultas	Mensagens	O eleitor autenticado ao clicar no link "Mensagens", que surge no cabeçalho, é redirecionado para a página que apresenta as suas mensagens.
REQ 2.16	Sistema de Consultas	Histórico	O eleitor autenticado ao clicar no link "Histórico", que surge no cabeçalho, é redirecionado para a página que apresenta o histórico das eleições das quais o eleitor fez parte. Esta página apresenta a seguinte estrutura: [Filtros de pesquisa] As eleições podem ser filtradas pelos seguintes critérios: • Paginação: Corresponde ao número de itens visíveis por página e deve ter as opções 5 ou 10. Por defeito deve existir uma paginação de 5 em 5 itens; • Ano: Corresponde ao ano em que a eleição se realizou.

			[Listagem de eleições] Apresenta todas as eleições cujo eleitor autenticado fez parte, ordenadas por data de publicação, da mais recente para a mais antiga. Para cada eleição deve ser apresentada a seguinte informação: • Logótipo do processo eleitoral da respetiva eleição; • Nome do processo eleitoral; • Nome da eleição; • Data de início da eleição; • Data de fim da eleição.
REQ 2.17	Sistema de Consultas	Consulta de referência de voto	O eleitor autenticado ao consultar a página de detalhe de um processo eleitoral pode clicar no botão "Consulta de referência de voto", e ser redirecionado para a página onde pode consultar se a sua referência de votação faz parte da lista de referências associadas à eleição. Esta página apresenta um formulário de pesquisa onde pode ser inserida a referência do voto e após a submissão da pesquisa surge uma mensagem informativa a indicar se a referência faz ou não parte da lista associada à eleição em questão.
REQ 3.1	Sistema de Votação	Passo 1: Selecionar Eleição	O eleitor autenticado ao clicar no botão "votar" que surge no detalhe do processo eleitoral ou na listagem dos meus processos eleitorais, é redirecionado para a área de votação. O sistema de votação é constituído por 5 passos [REQ 3.1 a REQ 3.6]. No passo 1 são apresentadas todas as eleições associadas ao respetivo processo eleitoral, das quais o eleitor faz parte do caderno eleitoral. Para cada eleição é apresentada a seguinte informação: • Nome da eleição; • Descrição da eleição; • Período de Votação (Data de início de Data de fim); • Botão "Votar": Está ativo quando o período de votação está em curso, enquanto o eleitor não votar. Ao clicar no botão o eleitor é redirecionado para o "Passo 2". Antes da listagem de eleições é apresentada uma mensagem informativa sobre o número total de eleições e o número de eleições que estão ainda disponíveis para votação.
REQ 3.2	Sistema de Votação	Passo 2: Selecionar Lista	Neste passo, é apresentado o boletim de voto e o eleitor escolhe a lista ou o candidato em que pretende votar. Caso não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 1 [REQ 3.1], onde deve escolher novamente em que eleição pretende

			votar. Caso pretenda avançar deve clicar no botão "Seguinte" e é redirecionado para o passo 3 [REQ 3.3].
REQ 3.3	Sistema de Votação	Passo 3: Confirmar Lista	Neste passo o eleitor deve confirmar a escolha de lista ou candidato efetuada, existindo apenas para efeitos de validação. Caso este não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 2 [REQ 3.2], onde pode escolher outra lista ou candidato em que pretende votar. Caso pretenda avançar deve clicar no botão "Votar" e é redirecionado para o passo 4 [REQ 3.4].
REQ 3.4	Sistema de Votação	Passo 4: Segurança - Envio de código PIN	Neste passo deve ser feita a seleção do mecanismo de envio do PIN de votação, sendo apresentado um formulário para esse efeito. Por defeito surge a opção que estiver inserida nos dados pessoais do eleitor. Após a seleção, o eleitor deve clicar no botão "Continuar" e é enviado, automaticamente, o PIN de votação e o utilizador é encaminhado para o passo 5 [REQ 3.5]. Caso não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 3 [REQ 3.3].
REQ 3.5	Sistema de Votação	Passo 5: Segurança - Inserção de código PIN	Neste passo é apresentado o formulário onde deve ser inserido o PIN de votação recebido. Ao clicar em "Submeter Voto" o eleitor finaliza o processo de votação na respetiva eleição e é redirecionado para o passo 6 [REQ 3.6], onde é apresentada a sua referência de votação. Neste momento é enviado um email para o eleitor com a referência da sua votação. Caso o eleitor não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 4 [REQ 3.4]. O PIN de votação deve ficar visível.
REQ 3.6	Sistema de Votação	Passo 6: Informação de submissão de voto	Neste passo é apresentada a referência de votação do eleitor. Ao clicar em "OK" o utilizador é encaminhado novamente para o passo 1 [REQ 3.1] e a eleição em questão deixa de estar ativa, ficando o botão "Votar" bloqueado e sendo atualizado o número de eleições ativas.
REQ 4.1	Sistema de Gestão de Eleições	Pedido de criação do processo eleitoral: Dados Gerais	O responsável institucional acede ao formulário para pedido de criação do processo eleitoral através do endereço. O formulário é composto pelos passos de inserção de dados gerais e de membros. O passo dos Dados Gerais apresenta a seguinte estrutura: [Processo Eleitoral] Informação básica do processo eleitoral: • Logótipo: Dimensão mínima de 135x100px; • Identificador do processo eleitoral; • Descrição do processo eleitoral;

			[Eleições] Devem ser inseridas as várias eleições associadas ao processo eleitoral. Por defeito é apresentado o formulário de inserção de uma eleição com a seguinte estrutura: • Calendário eleitoral: Formulário de inserção dos dados do caderno eleitoral [REQ 4.2]; • Identificador da eleição (limite de caracteres: 100); • Descrição da eleição (limite de caracteres: 260); • Botão "+": Ao clicar é adicionado um novo bloco com os campos referidos acima, para que seja criada uma nova eleição. Ao clicar no botão "Seguinte", são submetidos os dados inseridos até ao momento e o responsável institucional passa para a criação de membros [REQ 4.3].
REQ 4.2	Sistema de Gestão de Eleições	Pedido de criação do processo eleitoral: Calendário Eleitoral	Quando o responsável institucional clica no botão "Calendário eleitoral" que surge nos dados gerais do formulário de pedido de criação do processo eleitoral, abre uma janela pop-up com o formulário de gestão de caderno eleitoral que apresenta a seguinte estrutura: [Datas de proposituras] • Data de início; • Data de fim. [Cadernos eleitorais] • Data de publicação antes de verificação; • Data de publicação após verificação e correção. [Votação] • Período de votação: Apresenta dois campos para a data de início e fim. [Consulta das referências de votos] • Data da consulta: Apenas um dia. [Ata eleitoral] • Data de publicação; • Período de verificação: Apresenta dois campos para a data de início e fim. Após preencher esta informação, o responsável institucional clica no botão "Inserir", os dados ficam associados à respetiva eleição e a janela pop-up fecha, voltando para a página de dados gerais. Caso clique no botão "Fechar" a janela pop-up fecha, voltando para a página de dados gerais e os dados inseridos não são guardados.

REQ 4.3	Sistema de Gestão de Eleições	Pedido de criação do processo eleitoral: Membros	Nesta área, caso já existam membros, é apresentada uma listagem com a seguinte informação para cada membro: • ID; • Nome; • Qualidade; • Designação; • Email; • Telemóvel; • Endereço Postal; • Opção de envio de Credenciais; • Botão "Editar": Ao clicar acede ao formulário de edição de dados do membro, que é igual ao formulário de criação de membros; • Botão "Eliminar": Ao clicar elimina o respetivo membro da lista de membros. Após a listagem surge o botão "+", em que ao clicar abre uma janela pop-up com o formulário de criação de membro. Este formulário apresenta os seguintes campos: • Nome: caixa de texto simples; • Qualidade: caixa de seleção com as opções "Presidente" ou "Outro"; • Designação: caixa de texto simples; • Email: caixa de texto livre com validação para formato de email; • Telemóvel: caixa de texto com o formato XXXX-XXXXXXX; • Endereço Postal: caixa de texto livre; • Opção de envio de credenciais: caixa de seleção com as opções "SMS" ou "Email". Por defeito está preenchido com a opção SMS; Após preencher esta informação o responsável institucional clica no botão "Inserir", é criado um novo membro associado à respetiva eleição e a janela pop-up fecha, voltando para a página de membros. Caso clique no botão "Fechar" a janela pop-up fecha, voltando para a página de membros e os dados inseridos não são guardados. No final da listagem, para além do botão para adicionar novos membros, existe o botão "Anterior", em que ao clicar redireciona para o passo de gestão de dados gerais, e o botão "Seguinte" em que ao clicar redireciona para a página de resumo que apresenta todos os dados submetidos relativos ao processo eleitoral [REQ 4.4].
----------------	-------------------------------	--	---

REQ 4.4	Sistema de Gestão de Eleições	Pedido de criação do processo eleitoral: Resumo	Esta página apresenta toda a informação preenchida nos passos "Dados gerais" e "Membros", exatamente com a mesma representação que nos respetivos passos, mas sem botões de inserção. Surge ainda um botão "Imprimir" que gera um PDF com os dados. No final surge o botão reCAPCHA, de preenchimento obrigatório, para prosseguir com a submissão. Caso responsável institucional clique no botão "Anterior" é redirecionado para o passo de gestão de membros. Caso clique no botão "Seguinte" a submissão é efetuada e surge uma janela pop-up com uma mensagem informativa de que o seu pedido foi submetido com sucesso. Nesta janela ao clicar em "Ok" o responsável institucional é encaminhado para o passo de dados gerais vazio, podendo fazer uma nova submissão e recomeçar todo o processo.
REQ 4.5	Sistema de Gestão de Eleições	Processos eleitorais: Listagem	O membro da comissão eleitoral ao autenticar-se no sistema de gestão de eleições é redirecionado para a listagem de processos eleitorais. Esta apresenta todos os processos eleitorais no estado aberto cujo membro faz parte. Para cada processo eleitoral é apresentada a seguinte informação: • Logótipo do processo eleitoral; • Identificador do processo eleitoral; • Descrição do processo eleitoral; • Botão "Selecionar" que redireciona para a área de detalhe do respetivo processo eleitoral [REQ 4.6].
REQ 4.6	Sistema de Gestão de Eleições	Processos eleitorais: Detalhe	Esta página apresenta a seguinte estrutura: • Botão "Configuração de operações" que redireciona para [REQ 4.7]; • Logótipo do processo eleitoral; • Identificador do processo eleitoral; • Descrição do processo eleitoral; • Data de publicação do processo eleitoral; • Documentos: Apresenta o número de documentos do processo. Ao clicar no ícone de edição é redirecionado para a página de edição do processo eleitoral [REQ 4.8]; • Eleições: Apresenta o número de eleições associadas ao processo. Ao clicar no botão "Eleições" redireciona para o painel de eleições [REQ 4.9];
REQ 4.7	Sistema de Gestão de Eleições	Processos eleitorais: Configuração de operações	Área onde é definido o nível de segurança que deve ser associado a cada ação crítica. Para as ações que se seguem deve ser definido qual o respetivo nível de segurança, Simples, Forte ou Crítico: • Abrir eleição com verificação de que a urna está vazia • Encerramento de eleição/urna

			• Contagem de votos • Publicação do processo eleitoral • Alterar quem responde às mensagens • Configuração inicial do processo eleitoral • Outros Ao clicar no botão "Gravar", surge um formulário onde devem ser inseridas as chaves de todos os membros da comissão eleitoral. Apenas após a inserção das chaves e validação pela aplicação, as configurações ficam guardadas.
REQ 4.8	Sistema de Gestão de Eleições	Processos eleitorais: Edição	O membro da comissão eleitoral ao clicar no botão de edição que surge no detalhe dos processos eleitorais acede à área de edição do processo, que é composta por Informações Gerais e Comissão Eleitoral. Em Informações Gerais estão pré-preenchidos os dados que foram inseridos pelo responsável institucional, e é possível editar os seguintes dados: • Logótipo; • Identificador do processo eleitoral; • Descrição do processo eleitoral; • Data de publicação; • Documentos: É apresentado o nome do documento, o ficheiro e o botão para eliminação do ficheiro. Ao clicar no botão "Gravar" são guardadas as alterações efetuadas. Em Comissão Eleitoral são apresentados os dados dos membros da comissão eleitoral. Estes dados são apenas informativos e não podem ser editados pela comissão eleitoral.
REQ 4.9	Sistema de Gestão de Eleições	Painel de Eleições: Ecrã inicial	O membro da comissão eleitoral ao clicar no botão "Eleições" que surge no detalhe dos processos eleitorais acede ao painel de gestão de eleições. O Painel de eleições apresenta a informação geral das eleições associadas ao processo eleitoral, permitindo o acompanhamento e gestão dos dados da eleição. Para cada eleição é apresentada a seguinte informação: • Identificador da Eleição; • Painel de Operações: O botão "Gerir" fica ativo XX dias antes do início do período de votação. Ao clicar no botão "Gerir" o membro da comissão vai para a página onde é feita a gestão de operações críticas perto do período de votação da eleição; • Configurações: Apresenta o ícone representativo do estado da gestão deste passo;

-
- Calendário: Apresenta o ícone representativo do estado da gestão deste passo;
 - Categorias: Apresenta o ícone representativo do estado da gestão deste passo e o número de categorias preenchidas até ao momento;
 - Cadernos: Apresenta o ícone representativo do estado da gestão deste passo e o número de eleitores inseridos até ao momento;
 - Candidatos: Apresenta o ícone representativo do estado da gestão deste passo e o número de candidatos inseridos até ao momento;
 - Boletim: Apresenta o ícone representativo do estado da gestão deste passo;
 - Botão de edição: Ao clicar redireciona para a edição do passo 1 do painel de eleições.

Os ícones representativos do estado da gestão dos passos são os seguintes:

- Com informação: Basta que tenha sido preenchido um campo;
- Sem informação: Não foi preenchida nenhuma informação;
- Bloqueado: Não é possível editar os dados relativos a este passo. Na fase inicial, em que ainda não foi feita a configuração de operações [REQ 4.7], todos os passos se encontram no estado bloqueado.

REQ 4.10	Sistema de Gestão de Eleições	Painel de Eleições: Passo 1 - Configurações	No passo 1 são efetuadas as configurações gerais da eleição. Este passo é composto pelos seguintes campos: • Identificador da eleição: dois campos de texto simples para inserir a informação em português e em inglês; • Descrição: dois campos de texto simples para inserir a informação em português e em inglês; • Limite de escolhas assinaláveis: Caixa de seleção única com as opções de 0 a 10; • Write in: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção “Sim”; • Votação Ordenada: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção “Sim”; • Peso dos votos: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção “Sim”; • Método de Hondt: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção “Sim”. Caso seja selecionada a opção “Sim”, deve ser apresentado o campo "Número de mandatos totais", que é uma caixa de seleção única com as opções de 0 a 10.
-----------------	-------------------------------	---	---

			Ao clicar no botão "Voltar" o membro da comissão eleitoral é redirecionado para o Painel de eleições. Ao clicar no botão "Seguinte", é redirecionado para o passo 2 [REQ 4.11].
REQ 4.11	Sistema de Gestão de Eleições	Painel de Eleições: Passo 2 - Calendários Eleitorais	No passo 2 são efetuadas as configurações da eleição relativas ao caderno eleitoral. Os dados já estão pré-preenchidos com a informação inserida pelo responsável institucional e podem ser editados pelos membros da comissão. Este passo é composto pelos seguintes campos: [Datas de proposituras] • Data de início; • Data de fim. [Cadernos eleitorais] • Data de publicação antes de verificação; • Data de publicação após verificação e correção. [Votação] • Período de votação: Apresenta dois campos para a data de início e fim. [Consulta das referências de votos] • Data da consulta: Apenas um dia. [Ata eleitoral] • Data de publicação; • Período de verificação: Apresenta dois campos para a data de início e fim. Ao clicar no botão "Anterior" o membro da comissão eleitoral é redirecionado para o passo 1 [REQ 4.10]. Ao clicar no botão "Seguinte", é redirecionado para o passo 3 [REQ 4.12].
REQ 4.12	Sistema de Gestão de Eleições	Painel de Eleições: Passo 3 - Categorias	No passo 3 são efetuadas as configurações da eleição relativas às categorias dos eleitores. Os eleitores têm diferentes pesos, o que se traduz em votos com pesos distintos, designando-se esta característica por categoria. Este passo é composto por um formulário que apresenta por defeito uma linha com os seguintes campos: • Designação da categoria: campo alfanumérico devendo ser estabelecida a relação entre eleitor e o seu peso; • Peso; • Botão para eliminar: Ao clicar a respetiva categoria é eliminada. Ao clicar no botão "+" é adicionada uma nova linha à lista de categorias, para que sejam preenchidos os dados da respetiva categoria. A categoria apresentada por defeito deve ter a designação "um" e peso "1". Caso não sejam

			preenchidas mais categorias todos os membros ficam associados à categoria por defeito. Ao clicar no botão "Anterior" o membro da comissão eleitoral é redirecionado para o passo 2 [REQ 4.11]. Ao clicar no botão "Seguinte", é redirecionado para o passo 4 [REQ 4.13].
REQ 4.13	Sistema de Gestão de Eleições	Painel de Eleições: Passo 4 - Cadernos Eleitorais	No passo 4 é feita a inserção dos eleitores que fazem parte do caderno eleitoral da eleição. Esta inserção é feita através da importação de um ficheiro, com formato CSV, que deve conter os seguintes dados: • Número de identificação; • Nome; • Email; • Telemóvel; • Designação da categoria: Esta opção tem de ser obrigatoriamente uma das opções inseridas no passo 3 [REQ 4.12]; O sistema valida, para cada eleitor, que: • O email está bem formado; • Não existem dois eleitores com o mesmo email; • Os números de identificação (alfanumérico) são únicos; • A categoria indicada para cada uma das eleições, existe nessa eleição (note-se que se a categoria for vazia, significa que é para utilizar a categoria por defeito para essa eleição). Para além da inserção dos eleitores que correspondem ao caderno eleitoral, neste passo existe o botão "Publicitar caderno eleitoral", que gera um documento PDF e torna pública a página de apresentação do caderno eleitoral. Este, para além dos membros, deve apresentar a versão e a data. Deve existir um histórico dos vários documentos PDF gerados relativos ao caderno eleitoral. No momento em que o caderno eleitoral passa a público, os eleitores que fazem parte, passam a visualizar, no sistema de consultas, a respetiva eleição na área "os meus processos eleitorais". Após a data de verificação do caderno eleitoral, o botão "Publicitar caderno eleitoral" fica inativo. Ao clicar no botão "Anterior" o membro da comissão eleitoral é redirecionado para o passo 3 [REQ 4.12]. Ao clicar no botão "Seguinte", é redirecionado para o passo 5 [REQ 4.14].
REQ 4.14	Sistema de Gestão de Eleições	Painel de Eleições: Passo 5 - Listas	No passo 5 são inseridas as listas ou candidatos concorrentes à eleição. Neste passo são criadas as listas ou

			os candidatos concorrentes à eleição. Os dados associados são: • Logótipo; • Nome; • Informação adicional; • Programa eleitoral (link e/ou um ficheiro PDF). Este passo é composto por um formulário que apresenta por defeito uma linha com os seguintes campos vazios: • Foto; • Designação; • Documentos: É possível adicionar mais do que um documento e para cada documento deve ser inserida a designação associada. Deve ser possível eliminar e trocar a ordem dos documentos, que será a ordem com a qual serão apresentados no sistema de consultas; • Botão para adicionar novos documentos; • Botão para eliminar o candidato. Ao clicar no botão "+" é adicionada uma nova linha com os campos referidos acima, para que sejam preenchidos os dados de um novo candidato. Ao clicar no botão "Anterior" o membro da comissão eleitoral é redirecionado para o passo 4 [REQ 4.13]. Ao clicar no botão "Seguinte", é redirecionado para o passo 5 [REQ 4.14].
REQ 4.15	Sistema de Gestão de Eleições	Painel de Eleições: Passo 6 - Boletim de voto	No passo 6 é feita a configuração do boletim de voto. Os dados a configurar são os seguintes: • Instruções a constar no boletim de voto: dois campos de texto simples para preencher em português e em inglês; • Apresentação dos candidatos/listas: Radio button com as opções Lista e Dropdown; • Ordenação dos candidatos: Apresentados todos os candidatos inseridos no passo 5 [REQ 4.14], e a comissão eleitoral pode escolher a posição em que cada um é apresentado. Para além da gestão manual da ordem dos candidatos deve existir um botão para gerar aleatoriamente a ordem dos candidatos. Ao clicar no botão "Pré-visualizar boletim" é apresentada uma janela pop-up com a representação do boletim de voto que irá surgir no sistema de votação. Ao clicar no botão "Anterior" o membro da comissão eleitoral é redirecionado para o passo 5 [REQ 4.12]. Ao clicar no botão "Seguinte", é redirecionado para o painel de eleições.

REQ 4.16	Sistema de Gestão de Eleições	Eleições: Gestão de Operações Críticas	Ao clicar no botão "Gerir", que surge no painel de eleições, o membro da comissão eleitoral é redirecionado para a área de gestão de operações críticas. Esta área é composta pela "Abertura de urna", "Encerramento de Urna" e "Escrutínio de Votos": [Abertura de urna]: É definida a data e hora em que o período de votação vai iniciar. Para confirmar esta configuração devem ser inseridas as chaves de alguns membros da comissão eleitoral, de acordo com o definido nas configurações gerais [REQ 4.07]. [Encerramento de urna]: É definida a data e hora em que o período de votação vai terminar. Para confirmar esta configuração devem ser inseridas as chaves de alguns membros da comissão eleitoral, de acordo com o definido nas configurações gerais [REQ 4.07]. [Escrutínio de votos]: É feita a contagem dos votos após finalização do período de votação. Para confirmar esta configuração devem ser inseridas as chaves de alguns membros da comissão eleitoral, de acordo com o definido nas configurações gerais [REQ 4.07]. Para além das opções acima referidas existe o botão "Total de votos em urna", em que ao clicar surge uma janela pop-up que apresenta o número de votos contabilizados em urna até ao momento. Sempre que um membro da comissão eleitoral clica nesta opção, essa informação é guardada em histórico. O histórico apresenta o nome do membro da comissão que acedeu à contagem, a data, a hora e o número de votos no respetivo momento. Ao clicar em "Fechar" volta para a página de gestão de operações críticas. Todos os membros da comissão eleitoral podem aceder a este botão sem necessidade de inserção de chave. Este botão fica ativo apenas durante o período de votação.
REQ 4.17	Sistema de Gestão de Eleições	Histórico de Ações	Sempre que é efetuada uma inserção, edição ou eliminação nos dados do sistema de gestão de eleições, por parte de qualquer um dos membros do sistema de gestão de eleições, essa ação é guardada num histórico de ações. No ecrã do painel de eleições surge no canto direito do browser um botão denominado "Histórico de ações". Ao clicar nesse botão abre uma caixa que apresenta todo o

			histórico de ações do respetivo processo eleitoral. Esta área é visível a todos os membros da comissão eleitoral.
REQ 4.18	Sistema de Gestão de Eleições	Gestão de textos informativos	Os textos informativos dos passos do sistema de gestão de eleições devem estar agregados num ficheiro que possa ser editável.
REQ 5.1	Integrações	Autenticação	O mecanismo de autenticação deve ser integrado com o mecanismo utilizado pela DTSl, que corresponde ao ADFS da Microsoft. No momento de login são transferidos, como parâmetros para o endpoint a fornecer pela DTSl, os seguintes dados: • Email; • Password. São recebidos os seguintes dados como resposta: • Sucesso ou Insucesso do login; • Nome do utilizador; • Número de telefone; • Forma de envio de PIN: SMS ou Email; • Foto. Apesar de o design apresentar o botão "recuperar senha", essa funcionalidade não estará disponível na plataforma. Para recuperar senha o utilizador deve comunicar diretamente com a DTSl. Os testes relativos a esta integração só podem ser efetuados na Intranet da Universidade do Minho.
REQ 5.2	Integrações	SMS	O mecanismo de envio de SMS deve ser integrado com o mecanismo utilizado pela DTSl. Será implementado um webservice por parte da DTSl, que terá dois endpoints. O endpoint para envio de SMS irá receber os seguintes parâmetros: • Número de telemóvel; • Mensagem. Este irá devolver, como resposta, se a SMS foi ou não submetida com sucesso e o respetivo ID. O endpoint para atualização do estado irá receber, como parâmetro, o ID da mensagem, e devolver, como resposta, o respetivo estado. A resposta relativa ao estado da mensagem será guardada na base de dados, mas não será apresentada ao eleitor.

REQ 6.1	Notificações	Sistema de Consultas	No sistema de consultas existem as seguintes notificações: • Envio de email com a referência de voto após uma votação; • Envio de email quando o utilizador altera o email de comunicação. É enviada uma notificação para o email antigo a informar que foi inserido um novo email de comunicação e é enviada uma notificação também para o novo email.
REQ 6.2	Notificações	Sistema de Gestão de Eleições	No sistema de gestão de eleições são enviadas as seguintes notificações para todos os membros da comissão eleitoral: • Indicação de que vai terminar o período de proposituras, com X dias de antecedência; • Indicação de que se está a aproximar a data de publicação definitiva, após verificação, dos cadernos eleitorais, com X dias de antecedência; • Indicação de que vai iniciar o período de votação, com X dias de antecedência; • Indicação de que o período de verificação da ata eleitoral vai terminar, com X dias de antecedência.
REQ 7.1	Mensagens	Listagem	Ao aceder à área de mensagens é apresentada, por defeito, a listagem de mensagens recebidas. Esta área a contém as tabs "Recebidas" e "Enviadas", apresentando o total de mensagens existentes em cada listagem. [Recebidas]: Apresenta a lista de todas as mensagens recebidas pelo utilizador autenticado; [Enviadas]: Apresenta a lista de todas as mensagens enviadas pelo utilizador autenticado. Nas listagens de mensagens, para cada mensagem é apresentada a seguinte informação: • Remetente da mensagem; • Data de envio da mensagem; • Assunto da mensagem; • Texto da mensagem: São apresentados X caracteres (Definir de forma a preencher uma linha) • Botão para responder à mensagem; • Botão para eliminar a mensagem. Ao clicar no botão para responder à mensagem, abre o formulário de submissão de mensagens [REQ 7.2] com os seguintes campos pré-preenchidos (Não editáveis): • Nome utilizador autenticado; • Email do utilizador autenticado; • Destinatário da mensagem de origem;

			- Assunto: Texto "Re:" seguido do assunto da mensagem de origem. Ao clicar no botão “eliminar mensagem”, a mesma passa para o estado "Lixo", e deixa de aparecer na listagem visível para o utilizador. Ao clicar no assunto da mensagem o utilizador é encaminhado para uma página que apresenta a seguinte informação: - Assunto da mensagem; - Texto da mensagem completo; - Botão "Voltar": Ao clicar redireciona novamente para a lista de mensagens. No topo da listagem surge o botão "Nova", que abre uma página com o formulário de submissão de mensagens [REQ 7.2].
REQ 7.2	Mensagens	Formulário de submissão	O formulário de submissão de mensagens é composto pelos seguintes campos: - Nome; - Email; - Destinatário; - Assunto; - Mensagem; - ReCAPTCHA. O preenchimento dos campos acima definidos depende dos utilizadores que acedem ao formulário e da respetiva forma de acesso, de acordo com o definido nos [REQ 7.3] a [REQ 7.6].
REQ 7.3	Mensagens	Anónimos	Os utilizadores anónimos podem aceder ao formulário de submissão de mensagens, através do botão "Apresentar reclamação", que surge na página de consulta dos processos eleitorais [REQ 2.9]. O comportamento do formulário para estes utilizadores é o seguinte: - Nome: Preenchido pelo utilizador; - Email: Preenchido pelo utilizador; - Destinatário: Preenchido automaticamente com o grupo dos membros da comissão eleitoral da respetiva eleição. Este campo não fica visível para o utilizador; - Assunto: Preenchido automaticamente com o texto "Reclamação - Eleição X"; - Mensagem: Preenchido pelo utilizador; - ReCAPTCHA: Preenchido pelo utilizador.

			Ao clicar no botão "Enviar" são efetuadas as seguintes ações: • Envio de email para o remetente; • Envio de email para o destinatário; • Mensagem guardada nas mensagens recebidas do destinatário;
REQ 7.4	Mensagens	Eleitores	Os eleitores autenticados podem aceder ao formulário de submissão de mensagens, através do botão "Apresentar reclamação", que surge no sistema de consultas, na página de consulta dos processos eleitorais [REQ 2.9]. O comportamento do formulário para esta situação é o seguinte: • Nome: Preenchido automaticamente com o nome do eleitor autenticado; • Email: Preenchido automaticamente com o email do eleitor autenticado. Caso o eleitor tenha preenchido o email alternativo de comunicação, é esse email que deve ser usado; • Destinatário: Preenchido automaticamente com os membros da comissão eleitoral da respetiva eleição. Este campo não fica visível para o utilizador; • Assunto: Preenchido automaticamente com o texto "Reclamação - Eleição X"; • Mensagem: Preenchido pelo eleitor; • ReCAPTCHA: Preenchido pelo eleitor. Os eleitores autenticados também podem aceder ao formulário de submissão de mensagens, através do botão "Nova mensagem", que surge na área de mensagens. O comportamento do formulário para esta situação é o seguinte: • Nome: Preenchido automaticamente com o nome do eleitor autenticado; • Email: Preenchido automaticamente com o email do eleitor autenticado. Caso o eleitor tenha preenchido o email alternativo de comunicação, é esse email que deve ser usado; • Destinatário: Campo de seleção com a lista de membros das comissões eleitorais, de eleições em que o eleitor faz parte do caderno eleitoral. Este campo permite a escolha de mais do que uma opção; • Assunto: Preenchido pelo eleitor; • Mensagem: Preenchido pelo eleitor; • ReCAPTCHA: Preenchido pelo eleitor. Para ambos os casos, ao clicar no botão "Enviar" são efetuadas as seguintes ações: • Envio de email para o destinatário;

			• Mensagem guardada nas mensagens enviadas do remetente; • Mensagem guardada nas mensagens recebidas do destinatário.
REQ 7.5	Mensagens	Comissão Eleitoral	Os membros da comissão eleitoral podem aceder ao formulário de submissão de mensagens, através do botão "Nova mensagem", que surge na área de mensagens. O comportamento do formulário para estes utilizadores é o seguinte • Nome: Preenchido automaticamente com o nome do membro autenticado; • Email: Preenchido automaticamente com o email do membro autenticado. Caso o membro tenha preenchido o email alternativo de comunicação, é esse email que deve ser usado; • Destinatário: Este campo permite a escolha de mais do que uma opção. Deve ser possível enviar mensagens para: ◦ Grupo de todos os membros da comissão; ◦ Um membro da comissão (Pesquisa por nome ou email); ◦ Um eleitor dos cadernos eleitorais das eleições da comissão; ◦ Todos os eleitores dos cadernos eleitorais das eleições da comissão eleitoral; ◦ Grupo de eleitores de determinada eleição; ◦ Grupo de eleitores de determinada categoria de uma eleição; ◦ Grupo de administradores do sistema de administração; • Assunto: Preenchido pelo membro; • Mensagem: Preenchido pelo membro; • ReCAPTCHA: Preenchido pelo membro. Ao clicar no botão "Enviar" são efetuadas as seguintes ações: - Envio de email para o destinatário • Mensagem guardada nas mensagens enviadas do remetente; • Mensagem guardada nas mensagens recebidas do destinatário.
REQ 7.6	Mensagens	Administrador	Os administradores podem aceder ao formulário de submissão de mensagens, através do botão "Nova mensagem", que surge na área de mensagens. O comportamento do formulário para estes utilizadores é o seguinte: • Nome: Preenchido automaticamente com o nome do utilizador autenticado;

			• Email: Preenchido automaticamente com o email do utilizador autenticado; • Destinatário: Este campo permite a escolha de mais do que uma opção. Deve ser possível enviar mensagens para: ◦ Grupo de todos os membros de uma comissão eleitoral; ◦ Um membro de uma comissão eleitoral (pesquisa por nome ou email); • Assunto: Preenchido pelo utilizador; • Mensagem: Preenchido pelo utilizador; • ReCAPTCHA: Preenchido pelo utilizador. Ao clicar no botão "Enviar" são efetuadas as seguintes ações: • Envio de email para o destinatário; • Mensagem guardada nas mensagens enviadas do remetente; • Mensagem guardada nas mensagens recebidas do destinatário.
REQ 8.1	Sistema de Administração	Autenticação	A página de autenticação é composta por um formulário igual ao da autenticação do sistema de consultas [REQ 2.5], composto pelos seguintes campos: • Email; • Password. O mecanismo de autenticação deve estar integrado com a autenticação da DTSl [REQ 5.1].
REQ 8.2	Sistema de Administração	Estrutura	O sistema de administração é composto pela seguinte estrutura: [Cabeçalho] • Caixa de seleção do idioma com as opções "Português" e "Inglês", em que por defeito se encontra selecionado com "Português"; • Data atual; • Data do último login; • Nome do Utilizador autenticado; • Botão "Sair", em que ao clicar o utilizador deixa de estar autenticado. [Menu Lateral] • Gestão de Processos eleitorais [REQ 8.3]: Aponta para a área de gestão de processos eleitorais. Esta página é apresentada por defeito quando se entra no sistema de administração;

			• Gestão de Páginas [REQ 8.4]: Aponta para a área de gestão de páginas institucionais; • Pedidos de Emissão de certificados [REQ 8.5]: Aponta para a área de emissão de certificados; • Painel de Monitorização: Aponta para uma página externa de monitorização; • Mensagens: Aponta para a área de Mensagens [REQ 7.1]; • Rodapé; • Texto estático "Universidade do Minho 2016 ©".
REQ 8.3	Sistema de Administração	Gestão de processos eleitorais	A área de gestão de processos eleitorais apresenta a seguinte estrutura: [Pesquisa por texto livre]: Permite pesquisar sobre os seguintes campos dos processos eleitorais: • Identificador; • Descrição. [Filtro de processos eleitorais]: Permite filtrar pelos seguintes critérios: • Data: Apresenta o ano de submissão dos processos; • Estado: Apresenta os estados dos processos eleitorais. [Paginação]: Permite configurar se são listados 5 ou 10 processos eleitorais por página. [Listagem de processos eleitorais]: Para cada item é apresentada a seguinte informação: • Logótipo; • Identificador; • Data de submissão; • Proponente (Nome do responsável institucional); • Estado; • Botão "Aprovar". Ao clicar no identificador do processo eleitoral surge uma página igual à de resumo do processo eleitoral [REQ 4.4], onde apenas podem ser consultados os dados recebidos. O administrador não pode editar os dados. O botão "Adicionar" deve ser ignorado, uma vez que o administrador não irá adicionar processos eleitorais, apenas aprovar. A opção "Ações" deve ser ignorada, pois a única ação que pode ser efetuada é a alteração do estado e ficará associada a cada processo eleitoral. O botão "Aprovar" não existe no design, mas deve surgir associado a cada processo eleitoral e ter o design do botão

			"Consultar", que surge na listagem de processos eleitorais [REQ 2.8].
REQ 8.4	Sistema de Administração	Gestão de Páginas	A área de gestão de páginas apresenta a seguinte estrutura: [Pesquisa por texto livre]: Permite pesquisar sobre o título da página institucional. [Paginação]: Permite configurar se são listados 5 ou 10 páginas institucionais por página. [Listagem de páginas]: Apresenta as páginas institucionais da plataforma [REQ 2.7], em que para cada item apresenta a seguinte informação: • Título da Página; • Opção de tradução para inglês; • Autor. Ao clicar no título da página é apresentada a respetiva página com o corpo de texto que ficará visível na área de consultas. Ao passar o rato sobre o título de página, são apresentadas as seguintes opções: • Editar: Abre um formulário que apresenta o título da página e o editor de texto; • Ver: Abre a respetiva página com o corpo de texto que ficará visível na área de consultas; • Lixo: Elimina a respetiva página. O botão "Adicionar" deve ser ignorado. A opção "Ações" deve ser ignorada. Os campos "Data de Publicitação" e "Estado" devem ser ignorados. O filtro de páginas deve ignorado.
REQ 8.5	Sistema de Administração	Pedidos de Emissão de Certificados	O administrador tem permissão para aceder ao sistema de administração, onde são geridas as páginas de conteúdo informativo e onde são carregados os certificados usados pela plataforma, designadamente: • Root self-signed Certificate; • Root Private key; • Validator Service Certificate; • Validator Service Private key; • Counter Service Certificate; • Counter Service Private key; • Voting System Certificate; • Voting System Private key.

ANEXO V

REQUISITOS FUNCIONAIS A IMPLEMENTAR NO ÂMBITO DO PROJETO DA EVOTUM *LIGHT*

Neste quinto anexo é apresentada, de forma integral, a descrição detalhada de todos os requisitos funcionais a implementar no âmbito do projeto de conceção da plataforma eVotUM *light*, conforme se pode observar na tabela seguinte.

Esta informação pode ser resumidamente encontrada no capítulo 4, secção referente aos requisitos funcionais.

Requisito	Categoria	Subcategoria	Descrição
REQ 1.1	Geral	Design	O tema genérico deve estar adaptado aos browsers Internet Explorer 11, Firefox 34, Chrome 40, Safari, e versões superiores.
REQ 1.2	Geral	Perfis	Devem existir os seguintes perfis de utilizadores: • Secretário: Responsável pela criação e gestão de eleições através do sistema de gestão de votações; • Votante: Acesso ao sistema de consultas e ao sistema de votação; • Administrador: Responsável pelo carregamento inicial dos certificados digitais a utilizar pelo sistema. Não administra, efetivamente, a utilização do sistema.
REQ 2.1	Sistema de Consultas	Página Inicial	A Homepage deve apresentar a informação seguinte: • Logótipo eVotUM light e frase estática “Sistema de Votação Eletrónica em Reuniões”: Redireciona para a Homepage ao clicar; • Como Funciona [REQ 2.8]; • Texto estático sobre a plataforma; • Botão "Autenticação": Redireciona para a página de autenticação [REQ 2.6].
REQ 2.2	Sistema de Consultas	Cabeçalho e Rodapé	O cabeçalho deve ser constituído pelos seguintes itens: • Logótipo da universidade do Minho; • Configurações [REQ 2.3]; • Pesquisa [REQ 2.4]; • FAQs: Redireciona para a página geral de perguntas frequentes; • Idioma: PT ou EN. Se o idioma selecionado for PT, apresenta o link para selecionar EN, e vice-versa; • Nome do votante com link para a edição de dados pessoais; • Botão de log out, denominado "sair"; • Logótipo do eVotUM: Link redirecionada para a página inicial do portal; • Menu [REQ 2.5].

REQ 2.3	Sistema de Consultas	Configurações	Ao clicar no botão “Configurações” surge uma janela onde o utilizador pode adaptar as suas preferências: • Tamanho da fonte: Por defeito está selecionado o tamanho normal e pode ser alterado para o tamanho Grande. As preferências selecionadas ficam gravadas apenas durante a sessão; • Cor: Por defeito está selecionada a cor azul e pode ser alterada para vermelho. As preferências selecionadas ficam gravadas apenas durante a sessão.
REQ 2.4	Sistema de Consultas	Pesquisa	Ao clicar na lupa do cabeçalho surge a área de pesquisa por texto livre. A página de resultados apresenta o número de resultados encontrados para determinado termo de pesquisa, e a lista de resultados, em que para cada item é apresentada a seguinte informação: • Título; • Descrição.
REQ 2.5	Sistema de Consultas	Menu	Os itens de menu: • As minhas votações [REQ 2.9]; • Dados pessoais [REQ 2.13];
REQ 2.6	Sistema de Consultas	Autenticação	Ao clicar no botão "Autenticação", que surge no cabeçalho, o utilizador é redirecionado para a página de login. Nesta página surge o formulário composto pelos campos "E-mail" e "Senha de acesso". O sistema de acreditação da eVotUM recorre a um Serviço de Diretoria, <i>Active Directory</i>. Deve ser possível memorizar os dados de acesso no browser, selecionando a Checkbox "memorizar".
REQ 2.7	Sistema de Consultas	Páginas Institucionais	O portal deve apresentar, em rodapé, as seguintes páginas institucionais: • Sobre o eVotUM; • Perguntas frequentes; • Política de segurança e informação; • Política de privacidade; • Termos de utilização; • Mapa do Site;
REQ 2.8	Sistema de Consultas	Como funciona	Página estática que apresenta informação relativa à plataforma. O botão “Guia do Utilizador” redireciona para uma página que contém o guia de utilização da eVotUM.
REQ 2.9	Sistema de Consultas	Votações – Consultar Listagem	O votante autenticado ao clicar em "As minhas votações", que surge no cabeçalho, é redirecionado para a página que apresenta a listagem de votações das quais o votante faz parte. Esta listagem apresenta as votações ordenadas da

			mais recente para a mais antiga. Para cada votação é apresentada a seguinte informação: • Logótipo; • Nome da votação; • Estado da votação; • Botão "Consultar": redireciona para a página de consulta da votação [REQ 2.10]; • Botão "Votar": redireciona para a página de votação [REQ 3.1]. No topo da listagem surge o botão "Arquivo" que redirecionada para a página de arquivo das votações [REQ 2.11].
REQ 2.10	Sistema de Consultas	Votações: Consultar Votação	O votante ao clicar no botão "Consultar" disponível na listagem de votações, é redirecionado para a página de consulta de uma votação. A página de consulta de uma votação apresenta a seguinte estrutura: [Informações gerais da votação] • Texto descritivo da votação; • Documentos associados à votação, em que para documento é apresentado o nome associado ao documento, seguido dos links para visualização dos ficheiros. [Votações] Por defeito é apenas apresentado o nome da votação e uma seta, em que ao clicar abre a respetiva informação detalhada. Ao clicar numa votação diferente é escondida a informação da anterior. A informação detalhada a apresentar é a seguinte: • Estado atual; • Texto descritivo da votação; • Candidatos; • Botão "Votar" no canto superior direito da listagem. Ao clicar no botão, o votante é redirecionado para a página de votação [REQ 3.1]; • Botão "Consulta de referência de votos". Ao clicar no botão, o votante é redirecionado para a página de consulta de referência de votos [REQ 2.12].
REQ 2.11	Sistema de Consultas	Votações: Consultar Arquivo	Ao clicar no botão "Arquivo" que surge na listagem de votações, o utilizador é redirecionado para a página de arquivo de votações que apresenta a seguinte estrutura: [Filtros de pesquisa] As votações podem ser filtradas pelos seguintes critérios:

			• Paginação: Corresponde ao número de itens visíveis por página e deve ter as opções 5 ou 10. Por defeito deve existir uma paginação de 5 em 5 itens; • Ano: Devolver todos os anos que tiveram, pelo menos, uma votação, desde a primeira votação existente na plataforma, até ao momento atual. [Listagem de votações] Apresenta todos as votações que se encontram no estado fechado, ordenadas por data de publicação, da mais recente para a mais antiga. Para cada votação deve ser apresentada a seguinte informação: • Logótipo; • Nome da votação; • Estado da votação; • Botão "Consultar": Ao clicar redireciona para a página de consulta da votação [REQ 2.10].
REQ 2.12	Sistema de Consultas	Consultar Referência de Votação	O votante autenticado ao consultar a página de detalhe de uma votação pode clicar no botão "Consulta de referência de votos", e ser redirecionado para a página onde pode consultar se a sua referência de votação faz parte da lista de referências associadas à votação. Esta página apresenta um formulário de pesquisa onde pode ser inserida a referência do voto e após a submissão da pesquisa surge uma mensagem informativa a indicar se a referência faz ou não parte da lista associada à votação em questão.
REQ 2.13	Sistema de Consultas	Editar Dados pessoais	O votante autenticado ao clicar no link "Dados pessoais", que surge no cabeçalho, é redirecionado para a página que apresenta os seus dados pessoais. Esta página apresenta a seguinte estrutura: • Imagem de perfil: não pode ser editada; • Nome: não pode ser editado; • Email: não pode ser editado; • Telemóvel; • Forma de envio de PIN de votação: Apresenta as opções SMS e Email e por defeito tem a opção SMS selecionada. Caso o utilizador não tenha número de telemóvel associado tem, por defeito, a opção Email selecionada; No final deve existir um botão "Guardar" para preservar a edição dos campos editáveis.
REQ 3.1	Sistema de Votação	Passo 1: Selecionar Votação	O votante ao clicar no botão "votar" que surge na listagem das votações, é redirecionado para a área de votação. O sistema de votação é constituído por 5 passos [REQ 3.1 a REQ 3.6]. No passo 1 são apresentadas todas as votações,

			das quais o votante faz parte. Para cada votação é apresentada a seguinte informação: • Nome da votação; • Descrição da votação; • Botão "Votar": Está ativo quando o período de votação está em curso, enquanto o votante não votar. Ao clicar no botão o votante é redirecionado para o "Passo 2".
REQ 3.2	Sistema de Votação	Passo 2: Selecionar Candidato	Antes de surgir a listagem é, ainda, apresentada uma mensagem informativa sobre o número total de votações e o número de votações disponíveis no momento. Neste passo, é apresentado o boletim de voto e o votante escolhe o candidato em que pretende votar. Caso não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 1 [REQ 3.1], onde deve escolher novamente em que votação pretende votar. Caso pretenda avançar deve clicar no botão "Seguinte" e é redirecionado para o passo 3 [REQ 3.3].
REQ 3.3	Sistema de Votação	Passo 3: Confirmar Candidato	Neste passo o votante deve confirmar a escolha de candidato efetuada, existindo apenas para efeitos de validação. Caso este não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 2 [REQ 3.2], onde pode escolher outro candidato em que pretende votar. Caso pretenda avançar deve clicar no botão "Votar" e é redirecionado para o passo 4.1 [REQ 3.4].
REQ 3.4	Sistema de Votação	Passo 4.1: Segurança – Selecionar Método de Envio de Código PIN	Neste passo deve ser feita a seleção do mecanismo de envio do PIN de votação, sendo apresentado um formulário para esse efeito. Por defeito surge a opção que estiver inserida nos dados pessoais do votante. Após a seleção, o votante deve clicar no botão "Continuar" e é enviado, automaticamente, o PIN de votação e o utilizador é encaminhado para o passo 4.2 [REQ 3.5]. Caso não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 3 [REQ 3.3].
REQ 3.5	Sistema de Votação	Passo 4.2: Segurança - Inserir Código PIN	Neste passo é apresentado o formulário onde deve ser inserido o PIN de votação recebido. Ao clicar em "Submeter Voto" o votante finaliza o processo de votação na respetiva votação e é redirecionado para o passo 5 [REQ 3.6], onde é apresentada a sua referência de votação. Neste momento é enviado um email para o votante com a referência da sua votação. Caso o votante não pretenda prosseguir pode clicar no botão "Anterior" e é redirecionado para o passo 4.1 [REQ 3.4]. O PIN de votação deve ficar visível.

REQ 3.6	Sistema de Votação	Passo 5: Recolher Referência de Votação	Neste passo é apresentada a referência de votação do votante. Ao clicar em "OK" o utilizador é encaminhado novamente para o passo 1 [REQ 3.1] e a votação em questão deixa de estar ativa, ficando o botão "Votar" bloqueado e sendo atualizado o número de votações ativas.
REQ 4.1	Sistema de Gestão de Votações	Criação da Votação: Passo 1 – Inserir Dados Gerais	O passo dos Dados Gerais apresenta a seguinte estrutura: • Identificador da votação: dois campos de texto simples para inserir a informação em português e em inglês (limite de caracteres: 100); • Descrição da votação: dois campos de texto simples para inserir a informação em português e em inglês (limite de caracteres: 260); • Botão "+": Ao clicar é adicionado um novo bloco com os campos referidos acima, para que seja criada uma votação. Ao clicar no botão "Seguinte", são submetidos os dados inseridos até ao momento e o Secretário passa para o Passo 2 [REQ 4.2].
REQ 4.2	Sistema de Gestão de Votações	Criação da Votação: Passo 2 – Selecionar Tipo de Votação	No passo 2 são efetuadas as configurações gerais da votação. Este passo é composto pelos seguintes campos: [Default] • Limite de escolhas assinaláveis: Por defeito o limite está definido para uma única opção; • Write in: Por defeito está preenchida com a opção "Não"; • Votação Ordenada: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção "Não"; • Peso dos votos: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção "Não"; • Método de Hondt: Radio buttons com as opções Sim ou Não. Por defeito está preenchida com a opção "Não". Ao clicar no botão "Anterior" o Secretário é redirecionado para o passo 1. Ao clicar no botão "Seguinte", é redirecionado para o passo 3.
REQ 4.3	Sistema de Gestão de Votações	Criação da Votação: Passo 3 – Inserir Lista de Participantes	No passo 3 é feita a inserção dos votantes que fazem parte da lista de presenças da reunião. Esta inserção é feita através da importação de um ficheiro, com formato CSV, que deve conter os seguintes dados: • Número de identificação; • Nome; • Email;

			• Telemóvel; O sistema valida, para cada votante, que: • O email está bem formado; • Não existem dois votantes com o mesmo email; • Os números de identificação (alfanumérico) são únicos; Ao clicar no botão "Anterior" o Secretário é redirecionado para o passo 2. Ao clicar no botão "Seguinte", é redirecionado para o passo 4.
REQ 4.4	Sistema de Gestão de Votações	Criação da Votação: Passo 4 – Inserir Candidatos	No passo 4 são inseridos os candidatos concorrentes à votação. Os dados associados são: • Nome; • Informação adicional; Este passo é composto por um formulário que apresenta por defeito uma linha com os seguintes campos vazios: • Designação; • Documentos: É possível adicionar mais do que um documento e para cada documento deve ser inserida a designação associada. Deve ser possível eliminar e trocar a ordem dos documentos, que será a ordem com a qual serão apresentados no sistema de consultas; • Botão para adicionar novos documentos; • Botão para eliminar o candidato. Ao clicar no botão "+" é adicionada uma nova linha com os campos referidos acima, para que sejam preenchidos os dados de um novo candidato. Ao clicar no botão "Anterior" o membro da comissão eleitoral é redirecionado para o passo 3. Ao clicar no botão "Seguinte", é redirecionado para o passo 5.
REQ 4.5	Sistema de Gestão de Votações	Criação da Votação: Passo 5 – Configurar Boletim de Voto	No passo 5 é feita a configuração do boletim de voto. Os dados a configurar são os seguintes: • Instruções a constar no boletim de voto: dois campos de texto simples para preencher em português e em inglês; • Apresentação dos candidatos: Radio button com as opções Lista e Dropdown; • Ordenação dos candidatos: Apresentados todos os candidatos e o Secretário pode escolher a posição em que cada um é apresentado. Para além da gestão manual da ordem dos candidatos deve existir um botão para gerar aleatoriamente a ordem dos candidatos.

			Ao clicar no botão "Pré-visualizar boletim" é apresentada uma janela pop-up com a representação do boletim de voto que irá surgir no sistema de votação. Ao clicar no botão "Anterior" o Secretário é redirecionado para o passo 4. Ao clicar no botão "Seguinte", é redirecionado para o Painel de Gestão da Votação.
REQ 4.6	Sistema de Gestão de Votações	Gestão da Votação: Ecrã inicial	O Secretário ao clicar no botão "Votações" acede ao painel de gestão de votações, que permite o acompanhamento e gestão dos dados da votação. Para cada votação são apresentadas as seguintes tabs: • Iniciar Votação; • Votos em Urna; • Fechar Votação; • Escrutinar Votos; • Publicar Resultados;
REQ 4.7	Sistema de Gestão de Votações	Gestão da Votação: Passo 1 - Autorizar Abertura de Votação	No Passo 1, através do Painel de Gestão da Votação, o Secretário tem permissão para dar começo à votação, através do botão "Iniciar Votação". Nestas circunstâncias, de votação em contexto de reuniões, não existem calendários eleitorais, isto é, períodos de votação pré-definidos, pelo que apenas o Secretário tem autoridade para decidir quando se dará início à votação. Ao clicar no botão "Anterior" o Secretário é redirecionado para o Ecrã Inicial. Ao clicar no botão "Seguinte", é redirecionado para o Passo 2.
REQ 4.8	Sistema de Gestão de Votações	Gestão da Votação: Passo 2 – Controlar Votos em Urna	No Passo 2, através do Painel de Gestão da Votação, o Secretário pode observar o número de votos já em urna, em tempo real. Nesta tab, o Secretário tem oportunidade de analisar o número de votos já efetuados e o número de votos por efetuar, o que lhe permite perceber quando avançar para o fecho da votação. Ao clicar no botão "Anterior" o Secretário é redirecionado para o Passo 1. Ao clicar no botão "Seguinte", é redirecionado para o Passo 3.
REQ 4.9	Sistema de Gestão de Votações	Gestão da Votação: Passo 3 – Autorizar Fecho de Votação	No Passo 3, através do Painel de Gestão da Votação, o Secretário tem permissão para dar fecho à votação, através do botão "Terminar Votação". Nestas circunstâncias, de votação em contexto de reuniões, não existem calendários eleitorais, isto é, períodos de votação pré-definidos, pelo que apenas o Secretário tem autoridade para decidir quando se dará termo à votação. Através do controlo de votos em urna, no Passo 2, o

			Secretário tem percepção do número de votos já efetuados e, no caso desse número corresponder à totalidade de votantes, poder-se-á finalizar a votação.
REQ 4.10	Sistema de Gestão de Votações	Gestão da Votação: Passo 4 - Autorizar Escrutínio de Votos	Ao clicar no botão "Anterior" o Secretário é redirecionado para o Passo 2. Ao clicar no botão "Seguinte", é redirecionado para o Passo 4. No Passo 4, através do Painel de Gestão da Votação, o Secretário tem permissão para dar início ao escrutínio dos votos. Nesta tab, o Secretário terá, portanto, de clicar no botão "Iniciar Escrutínio de Votos" para que se dê o processo. Posto isto, o resultado da votação é apresentado, no painel, ao Secretário da Reunião.
REQ 4.11	Sistema de Gestão de Votações	Gestão da Votação: Passo 5 – Autorizar Publicação de Resultados	Ao clicar no botão "Anterior" o Secretário é redirecionado para o Passo 3. Ao clicar no botão "Seguinte", é redirecionado para o Passo 5. Por fim, no Passo 5, através do Painel de Gestão da Votação, o Secretário tem autorização para publicar o resultado da votação na plataforma. Nesta tab, o Secretário terá, portanto, de clicar no botão "Publicar Resultados" para que se dê o processo. Posto isto, o resultado da votação é apresentado, na plataforma, a todos os participantes.
REQ 5.1	Integrações	Autenticação	Ao clicar no botão "Anterior" o Secretário é redirecionado para o Passo 4. Ao clicar no botão "Seguinte" é redirecionado, novamente, para o Ecrã Inicial. O mecanismo de autenticação recorre a um Serviço de Diretoria, <i>Active Directory</i>, que corresponde ao ADFS da Microsoft. No momento de login são transferidos, como parâmetros para o endpoint, os seguintes dados: • Email; • Password. São recebidos os seguintes dados como resposta: • Sucesso ou Insucesso do login; • Nome do utilizador; • Número de telefone; • Forma de envio de PIN: SMS ou Email; Apesar de o design apresentar o botão "recuperar senha", essa funcionalidade não estará disponível na plataforma.

REQ 5.2	Integrações	SMS	O mecanismo de envio de SMS integra um webservice que terá dois endpoints. O endpoint para envio de SMS irá receber os seguintes parâmetros: • Número de telemóvel; • Mensagem. Este irá devolver, como resposta, se a SMS foi ou não submetida com sucesso e o respetivo ID. O endpoint para atualização do estado irá receber, como parâmetro, o ID da mensagem, e devolver, como resposta, o respetivo estado. A resposta relativa ao estado da mensagem será guardada na base de dados, mas não será apresentada ao votante.
REQ 6.1	Notificações	Sistema de Consultas	No sistema de consultas existem as seguintes notificações: • Envio de email com a referência de voto após uma votação; • Envio de email quando o utilizador altera o email de comunicação. É enviada uma notificação para o email antigo a informar que foi inserido um novo email de comunicação e é enviada uma notificação também para o novo email.
REQ 7.1	Sistema de Administração	Autenticação	A página de autenticação é composta por um formulário igual ao da autenticação do sistema de consultas [REQ 2.5], composto pelos seguintes campos: • Email; • Password. O mecanismo de autenticação deve estar integrado com a autenticação [REQ 5.1].
REQ 7.2	Sistema de Administração	Emissão de Certificados	O Administrador é meramente responsável pelo carregamento inicial dos certificados digitais a utilizar pelo sistema. Não desempenha, portanto, um papel ativo no funcionamento da plataforma, isto é, não administra, efetivamente, a sua utilização. Em caso de necessidade de atualização dos certificados, o administrador terá de se autenticar no Sistema em causa e adicionar e/ou remover os certificados necessários. Os certificados utilizados pela Plataforma serão, à partida, os mesmos utilizados na eVotUM, designadamente: • Root self-signed Certificate; • Root Private key; • Validator Service Certificate; • Validator Service Private key; • Counter Service Certificate;

-
- Counter Service Private key;
 - Voting System Certificate;
 - Voting System Private key.
-