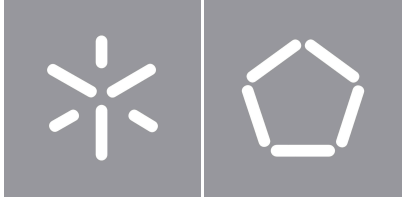
Universidade do Minho
Escola de Engenharia

Carolina da Torre Vila Chã

Definição técnica da solução eVoto num modelo Software-as-a-Service

outubro 2024



Universidade do Minho
Escola de Engenharia

Carolina da Torre Vila Chã

Definição técnica da solução eVoto num modelo Software-as-a-Service

Dissertação de Mestrado
Mestrado em Engenharia Informática

Trabalho efetuado sob a orientação de
João Alexandre Baptista Vieira Saraiva

outubro 2024

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:

CC BY-NC-SA

https://creativecommons.org/licenses/by-nc-sa/4.0/

Agradecimentos

Agradeço ao meu orientador, o Professor João Alexandre Baptista Vieira Saraiva, pelo apoio e supervisão contínua e crucial durante todo o processo de investigação e escrita desta dissertação.

Agradeço também à empresa Eurotux e à empresa Dipcode por me acolherem e facultarem os meios necessários para a realização desta dissertação, assim como também fornecerem o acesso a toda a informação sobre a plataforma eVoto necessária para a minha investigação. Gostaria de agradecer especificamente a António José Pinheiro Coutinho, Diretor Executivo (CEO) da Eurotux, pela sua liderança e visão na Eurotux. Apesar de não ter apoiado diretamente a realização desta dissertação, a sua influência foi instrumental na criação de um ambiente colaborativo. Também gostaria de agradecer a António Luis Pinto Ferreira de Sousa, Diretor de Curso de Engenharia Informática da Universidade do Minho e também Diretor de Informações (CIO) da Eurotux, pelo apoio não só enquanto aluna do curso mas também enquanto colaboradora na Dipcode.

Agradeço à equipa da Dipcode pelo apoio, entreajuda, e bom ambiente sentido durante todo o meu percurso como *developer* na empresa. Agradeço especialmente à Chief Operating Officer da Dipcode, Daniela Costa, pela sugestão e criação do tema de tese, pelo apoio e supervisão durante a realização da presente dissertação, e por motivar sempre ao trabalho e progresso na investigação. Agradeço também por promover sempre uma relação casa-trabalho equilibrada e por evidenciar a importância da saúde mental para o bem-estar pessoal.

Por fim, agradeço a todas as pessoas que, direta ou indiretamente, permitiram e facilitaram a escrita desta dissertação, nomeadamente: a minha família, pelo suporte durante o meu percurso educativo, e os meus colegas de curso, pela sugestão da empresa Eurotux para realizar a minha dissertação.

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.

Universidade do Minho, Braga, outubro 2024

Carolina da Torre Vila Chã

Assinado por: **Carolina da Torre Vila Chã**
Num. de Identificação: 15265128
Data: 2024.10.09 15:56:56+01'00'

Resumo

O objetivo desta tese é explorar as alterações funcionais, técnicas, e de arquitetura envolvidas na transição do eVoto, uma solução de votação online, de um modelo de vendas cliente a cliente para um modelo de negócio de Software as a Service (SaaS). Esta investigação compila resultados de diferentes análises focadas em diversas categorias: a tecnologia atual associada à arquitetura SaaS, os riscos associados a esta transição, analisando o mercado atual de soluções de votação online, bem como investigando o ambiente jurídico e legal que envolve o eVoto.

Um dos principais pontos de discussão deste documento é a investigação de áreas como a escalabilidade, a integração com aplicações de terceiros, a segurança dos dados e o design de sistema que podem ou não ter de mudar devido à transição para SaaS. Esta investigação resultará numa série de recomendações de mudanças em diversas áreas, como marketing, que funcionalidades estão disponíveis, e até no próprio desenvolvimento, incluindo um roadmap de desenvolvimento e um exemplo real de um site para a promoção do eVoto ao público.

Esta tese tenta oferecer ao Grupo Eurotux um documento que detalha não só a análise do ambiente tecnológico e investigação do mercado que rodeia o eVoto, mas também de mudanças reais e sugestões que podem ser úteis para esta transição de modelo de negócio.

Palavras-chave software-as-a-service, voto eletrónico, acesso remoto, inovação tecnológica, cloud, Internet, infraestrutura de TI

Abstract

The aim of this thesis is to explore the functional, technical, and architectural changes involved in transitioning eVoto, an online voting solution, from a client-by-client sales model to a Software as a Service (SaaS) business model. This investigation compiles results from different analyses focused on various categories: the current technology associated with SaaS architecture, the risks associated with this transition, analyzing the current market of online voting solutions, as well as investigating the legal environment surrounding eVoto.

One of the main talking points of this document is the investigation of areas such as scalability, integration with third-party apps, data security, and system design that may or may not have to change due to the transition to SaaS. This investigation will result in a series of recommendations for changes in various areas, such as the marketing, the functionalities available, and even in the development itself, including a development roadmap and a real-world example of a website for the promotion of eVoto to the public.

This thesis attempts to offer the Eurotux Group a document detailing not only the analysis of the technological environment and investigation of the market surrounding eVoto, but also of real changes and insights that can be useful for this transition in business model.

Keywords software-as-a-service, eletronic vote, remote access, technological innovation, cloud, Internet, IT infrastructure

Conteúdo

I Material Introdutório **1**

1 Introdução **3**

1.1 Objetivos 4

2 Estado da arte **7**

2.1 Software as a Service 7

2.1.1 Categorias de SaaS 10

2.1.2 Fragmentação de bases de dados 10

2.1.3 Modelos de Tenancy 11

2.1.4 Exemplos de Utilização 13

2.2 Contextualização na Área Tecnológica 14

2.2.1 Distinção entre voto eletrónico e voto online 15

2.2.2 Correção de Voto 15

2.2.3 Verificabilidade 16

2.2.4 Rasto de auditoria de voto em papel verificado pelo eleitor 16

2.2.5 Auditabilidade 16

II Core da Dissertação **18**

3 Certificações Relevantes **19**

3.1 ISO/TS 54001:2019 20

3.2 ISO/IEC/IEEE 90003:2018 23

3.3 ISO/IEC 27001:2022 24

3.4 ISO/IEC 15408 24

3.5 ISO/IEC/IEEE 12207:2017 . . . 25
3.6 Investigação aprofundada da certificação ISO/TS 54001:2019 . . . 26
3.7 Solução alternativa . . . 28

4 Análise Histórica e Legal do Voto Eletrónico em Portugal e no Mundo 32
4.0.1 Lei Europeia de Resiliência Cibernética (CRA) . . . 34

5 Benchmarking das soluções de voto online 40
5.0.1 Helios . . . 42
5.0.2 Belenios . . . 44
5.0.3 NemoVote . . . 46
5.0.4 nVotes . . . 48
5.0.5 ElectionBuddy . . . 51

6 Análise do eVotUM 53

7 Alterações para a comercialização do eVoto 61
7.1 Alterações Funcionais . . . 62
7.1.1 Linguagem e tecnologias . . . 62
7.1.2 Ferramentas . . . 62
7.1.3 Funcionamento e Website . . . 63
7.1.4 Roadmap de Alterações . . . 65
7.1.5 Expansão e Alterações ao Roadmap . . . 66
7.1.6 Desenvolvimentos atuais . . . 66
7.2 Alterações da Arquitetura . . . 76
7.2.1 Comparação de Tipos de Arquitetura . . . 76
7.2.2 Arquiteturas Propostas . . . 77
7.2.3 Alterações Propostas . . . 81
7.3 Análise de Riscos . . . 82
7.3.1 Ataques gerais . . . 82
7.3.2 Ataques específicos a software de voto . . . 83
7.3.3 Estratégias de proteção aliadas às tecnologias utilizadas no eVoto . . . 85
7.3.4 Conclusões . . . 87

8 Conclusões e trabalho futuro 89

8.0.1 Resposta às Perguntas de Investigação 91

III Apêndices **98**

A Exemplos de utilização **99**

B Apresentação das Certificações **107**

C CRA - Informações e Instruções Destinadas ao Utilizador **110**

D CRA - Produtos Críticos com Elementos Digitais **112**

E Questionário eVotUM - 05/09/2023 **115**

F Análise Detalhada da certificação ISO/TS 54001:2019 **117**

F.1 4. Context of the organization 117

F.2 5. Leadership 118

F.3 6. Planning 119

F.4 7. Support 120

F.5 8. Operation 130

F.6 9. Performance Evaluation 132

F.7 10. Improvement 133

G Diagrama de estados do processo eleitoral no eVotUM **134**

H Diagrama de estados de uma eleição no eVotUM **135**

I CRA - Palestra FOSDEM 2024 **136**

Lista de Figuras

1 Comparação entre vários tipos de soluções. Fonte: Redhat [2023] 7

2 Classificações das normas definidas 28
3 ElectionBuddy - formato em caixas. 29
4 NemoVote - formato em caixas. 29
5 InVote (Scytl) - formato em caixas. 29
6 Polyas - formato em caixas. 29
7 SimplyVoting - descrição detalhada. 30
8 InVote (Scytl) - tabela de comparação. 31

9 Arquitetura atual do eVotUM. 57

10 Planeamento do projeto eVoto, à data 27/06/2024. 65
11 Header do site 67
12 Banner introdutório. 67
13 Secção Sobre nós. 68
14 Listagem de funcionalidades. 68
15 Garantias do eVoto. 69
16 Customização no eVoto. 69
17 Banner Call to Action. 70
18 Página das Caraterísticas (incompleta). 70
19 Página "Como Funciona". 74
20 Página "Contactos". 75
21 Arquitetura B - Multi-tenant com base de dados fragmentada verticalmente (tipo 3). . . . 78
22 Arquitetura C - Multi-tenant com base de dados fragmentada vertical e horizontalmente (tipo 3). 79
23 Arquitetura D - Múltiplos single-tenant. 80

24 Diiagrama de estados do processo eleitoral. 134

25 Diagrama de estados de uma eleição. 135

Lista de Tabelas

1 Conclusões da análise a plataformas SaaS variadas. 14

2 Comparação de software de votação eletrónica online com modelo de negócios SaaS . . 41

3 NemoVote - Modelo de Subscrição 46

4 nVotes - Modelo de Subscrição 49

5 ElectionBuddy - Modelo de Subscrição 51

6 Caraterísticas do eVotUM. 54

7 Comparação de tipos de arquiteturas: Single-Tenant e Multi-Tenant. As cores denotam a polaridade de cada caraterística. 77

8 Tipos de ataques a produtos de software. 82

9 Matriz de risco de ataques a software de voto. 84

10 Estratégias de proteção para projetos Django. 86

11 Estratégias de proteção para projetos que utilizem Docker. 87

12 Função de cada uma das soluções analisadas. 99

13 Caraterísticas do front-end de cada uma das soluções analisadas. 100

14 Caraterísticas do back-end de cada uma das soluções analisadas. 101

15 Escalabilidade de cada uma das soluções analisadas. 102

16 Soluções para performance em cada uma das soluções analisadas - parte 1. 103

17 Soluções para performance em cada uma das soluções analisadas - parte 2. 104

18 Segurança de cada uma das soluções analisadas - parte 1. 105

19 Segurança de cada uma das soluções analisadas - parte 2. 106

Parte I

Material Introdutório

Notas de Autor

Esta dissertação foi realizada em coordenação com a empresa Dipcode, que se especializa em desenvolvimento web e que faz parte do grupo Eurotux[1]. Ao longo deste documento, tanto a Eurotux como a Dipcode poderão ser referidas não só pelos seus nomes, mas também por "a empresa". Entende-se que ao referir "a empresa"refere-se a ambas em conjunto, já que o projeto eVoto como SaaS será feito em parceria.

Algumas tabelas e figuras deste documento usam cores. Assim, deverá ser impresso a cores ou lido na sua versão eletrónica.

[1] A Eurotux é detentora de 85% da Dipcode

Capítulo 1

Introdução

O mundo político evoluiu consideravelmente desde as primeiras eleições democráticas na Antiga Grécia. O sistema democrático como as gerações atuais o conhecem, é extremamente recente, especialmente quando comparado com a complexa história política e eleitoral da humanidade. Foi apenas em 1994 que as primeira eleição com sufrágio universal foi realizada, em África do Sul. O partido que venceu, o Congresso Nacional Africano liderado por Nelson Mandela, defendia o estabelecimento de um regime democrático "não-racial e não-sexista"[Inter-Parliamentary Union, 1994].

O ano de 1994 pode não ser considerado longínquo, mas o mundo evoluiu drasticamente desde então. A invenção e consequente explosão em popularidade da Internet permitiu uma tremenda evolução tecnológica em todos os aspetos da vida moderna, e os sistemas de votação não são exceção. Hoje, cada vez mais entidades estão a fazer para que o voto presencial, e especialmente o voto em papel, sejam cada vez menos utilizados[Gibson et al., 2016]. Por de trás desta força, são várias as razões motivantes: desde redução de custos, passando pelo aumento da acessibilidade, até à necessidade de evolução tecnológica inerente ao ser Humano, são muitas as razões pelas quais se deve, cada vez mais, estudar e analisar a evolução do modo como escolhemos os nossos líderes, políticos ou não.

É também igualmente importante incidir com um foco especial sobre as questões de segurança, fiabilidade e confiança que este empurrão tecnológico levanta. Sendo uma tecnologia bastante recente, a adoção de sistemas de voto baseados na web ainda não são populares no ambiente político, sendo que a maioria das utilizações provém apenas de votações teste. Alguns destes testes foram realizados em países como a Suíça, o Reino Unido e os Estados Unidos da América [Alvarez et al., 2009]. No entanto, existe um caso a salientar: A Estónia.

A Estónia fez história em 2005 quando implementou um sistema de votação online para todo o seu grupo eleitoral [Laura Sheeter for BBC News, 2005]. Foi novamente pioneira quando utilizou voto baseado na web para as suas eleições parlamentares nacionais em 2007 e 2011, presidenciais em 2011, e Europeias em 2009 [National Democratic Institute, 2023]. O sistema de votação faz parte de uma maior

framework entitulada e-Estonia onde "99 por cento dos serviços públicos estão disponíveis 24 horas por dia (...) exceto para casamentos e divórcios - ainda é necessário sair de casa para esses."[e-Estonia, 2023]. O e-Estonia foi alvo de críticas por parte de diversas entidades, especialmente nos primeiros anos de adoção; no entanto, os oficiais responsáveis consideram o sistema seguro e adicionam que graças a ele "A Estónia poupa mais de 1400 anos de tempo de trabalho anualmente"[e-Estonia, 2023].

É neste espírito de eficiência de trabalho e poupança de tempo que começaram a surgir cada vez mais soluções de votação online. Assim, em 2017, surge um sistema de votação online. Foi desenvolvido por consórcio constituído pela empresa Eurotux, o Centro de Computação Gráfica e a Devise Futures para a Universidade do Minho, adotando o nome eVotUM. O seu código é open source e encontra-se disponível na plataforma Gitlab [1].

O sistema eVotUM é estruturado em 5 fases: criação de um processo eleitoral, criação de uma eleição, verificação do caderno eleitoral, votação e contagem. Uma caraterística distinta de outras soluções de voto online atualmente disponíveis, é que dá total autonomia ao cliente para que este possa configurar a eleição, através da determinação de um administrador.

O sistema eVotUM, atualmente, é acedido via web. Segundo as práticas da Eurotux, este tipo de serviço pode ser adquirido de duas formas:

- Como um serviço em que o cliente utiliza um sistema disponibilizado pela Eurotux;
- Como uma solução que é instalada numa infraestrutura à escolha do cliente.

A empresa pretende apostar num novo eVoto, baseado na plataforma eVotUM e criado em modelo de negócio Software-as-a-Service. Esta proposta de tese foi feita com a intenção de, no final, a empresa ter um plano sobre como proceder à transição da plataforma eVoto para um modelo SaaS, assim como uma análise não só dos riscos inerentes a uma mudança desta natureza, mas também das arquiteturas e soluções que já existem no mercado e as suas caraterísticas.

1.1 Objetivos

O objetivo principal desta dissertação é a realização de uma análise sobre a transição da plataforma eVoto para uma arquitetura SaaS, com as seguintes componentes:

1. Benchmarking das principais soluções de voto online, atualmente disponíveis, que estejam implementadas sobre o modelo SaaS. Estas plataformas de terceiros devem ser estudadas de modo a

[1] Repositório eVotUM: https://gitlab.com/eVotUM (último acesso em 13-06-2023)

permitir retirar conclusões sobre como deve um serviço de votação online, em modelo SaaS, ser implementado.

2. Roadmap de alterações funcionais, e de arquitetura, necessárias para o que o eVoto possa ser comercializado as-a-service.

3. Analisar o impacto desta mudança nas camadas de segurança e performance da aplicação. Existem variados riscos inerentes a uma alteração fundamental no modo como um sistema funciona, assim como, especificamente, precauções a tomar com alterações a um sistema de votação online. Deste modo torna-se necessário analisar o impacto da transformação do eVoto num modelo SaaS.

Como resultados esperados, pretende-se que seja criado um documento que detalhe as alterações necessárias à plataforma para implementá-la em modelo SaaS, assim como os riscos inerentes a essas alterações.

Assim, levantam-se as seguintes Perguntas de Investigação, que pretendemos responder com este projeto de mestrado:

PI1. Qual é o impacto da transição do eVoto para uma arquitetura SaaS na segurança do processo de votação online? Esta questão faz parte dos objetivos, sendo de especial interesse dado que a plataforma eVoto lida (e irá continuar a lidar) com dados sensíveis. É imprescindível assegurar que todos os utilizadores da plataforma, dos clientes aos desenvolvedores, continuarão a estar protegidos enquanto utilizam o produto.

PI2. Quais são as implicações legais e regulatórias da transição do eVoto para uma arquitetura SaaS, considerando os diferentes contextos nacionais e internacionais? Com a alteração do modelo de comercialização, o eVoto poderá deixar de, ou começar a, estar sobre o abrigo de leis diferentes, especialmente considerando que está a ser desenvolvido por uma entidade comercial. Além disto, esta investigação é especialmente crucial uma vez que o eVoto tem, como objetivo, ser comercializado em todo o mundo.

PI3. Como é que será impactada a transparência e auditabilidade do eVoto, na transição para uma arquitetura SaaS? Qualquer produto desenvolvido pela empresa é sujeito a auditorias e verificações por parte de entidades reguladoras. É crítico, então, investigar sobre como estes processos serão afetados com a mudança de modelo de negócios, para assegurar que poderão continuar sem obstáculos.

Estas perguntas serão respondidas ao longo deste documento, e será feito um resumo dos resultados obtidos na Conclusão.

Capítulo 2

Estado da arte

Este capítulo explora o estado atual das tecnologias associadas ao modelo de negócio Software-as-a-Service, nomeadamente, as suas categorias e modelos de *Tenancy*.

2.1 Software as a Service

Software-as-a-Service (SaaS) é uma forma de distribuição de software onde as aplicações são acedidas pelo utilizador através da Internet, ao contrário de outras formas de distribuição, onde geralmente é necessário instalar o programa no local.[Redhat, 2023][Microsoft, 2024].

É uma das três grandes categorias de computação na cloud, sendo que as outras duas são Infrastructure-as-a-Service (IaaS), e Platform-as-a-Service (PaaS).

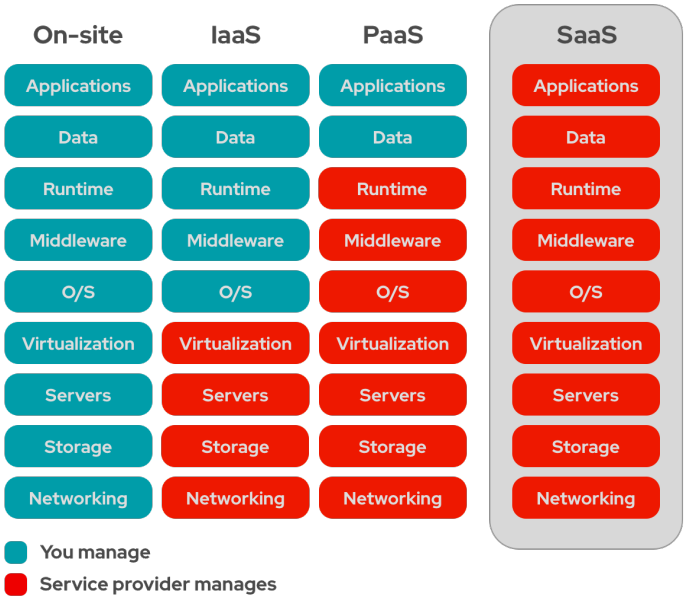


Figura 1: Comparação entre vários tipos de soluções. Fonte: Redhat [2023]

Segundo Redhat [2023] e Microsoft [2024], a primeira (IaaS) consiste em fornecer infraestrutura

como máquinas virtuais, armazenamento e rede para que os clientes possam executar suas próprias aplicações. Alguns exemplos deste tipo de arquitetura são: Amazon Web Services (AWS), Digital Ocean, e Microsoft Azure.

Indicam, também, que a segunda (PaaS) consiste em fornecer uma plataforma para desenvolvimento, implementação e gestão de aplicações sem a necessidade de gerir a infraestrutura subjacente. Alguns exemplos deste tipo de arquitetura são: Red Hat OpenShift, AWS Elastic Beanstalk, e Force.

É também indicado que o modelo SaaS permite reduzir custos relacionados com instalações no local do cliente, que já não seriam necessárias com este tipo de arquitetura. São vários os fatores que são mitigados ou, até, totalmente eliminados:

- Necessidade de infraestrutura no local do cliente
- Custos da manutenção da infraestrutura
- Custos de ensinar ao cliente como gerir a aplicação
- Custos de instalação na infraestrutura, muitas vezes incluindo deslocação por parte de representantes da empresa ao local.
- Etc.

É de salientar que as infraestruturas de sistemas de informação dependem dos mais variados aspetos, e nem sempre apenas da tecnologia disponível. A forma como a própria empresa está organizada, e/ou a sua política de redução de custos são apenas dois de muitos fatores que influenciam o modo como uma determinada solução pode ser implementada.

Axelrod [2011] diz que os sistemas de controlo do processo industrial "são geralmente construídos e testados a um nível muito superior, para lidar com falhas de sistema ou comportamento fora do típico até para sistemas de processamento de informação crítica". Precisamente, Silverback Data Center Solutions [2024] indica que muitas das vezes o fator que limita instalações através da cloud são as *guidelines* de segurança que podem não ser 100% asseguradas pelo serviço cloud. Indica também que, outras vezes, como é o caso com, por exemplo, fábricas, pode ser apenas o facto de que o software, normalmente altamente especializado, não é facilmente portável para a cloud.

Apesar destas dificuldades, Gartner[1] diz: "Prevê-se que os gastos mundiais dos utilizadores finais sobre serviços de cloud pública cresçam 20,7%, num total de 591,8 biliões de US$ em 2023, acima dos 490,3 biliões de US$ em 2022 (..) Isto é superior à previsão de crescimento de 18,8% para 2022.".

[1] https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023 (úlimo acesso em 19-01-2023)

De facto, o modelo SaaS está a evoluir cada vez mais na sua segurança e confiabilidade. Alguns exemplos populares de aplicações que utilizam o modelo SaaS são: GMail, Microsoft Office, Adobe Creative Cloud e Spotify [2].

Como na arquitetura SaaS as aplicações não necessitam de instalação de software, isto significa que não é necessária a obtenção de hardware por parte do cliente, o que aumenta de modo astronómico o número potencial de clientes para uma dada solução de software. A infraestrutura, a manutenção e a gestão do software são feitos por parte da empresa criadora - este modelo é possível e altamente atraente precisamente porque desta forma pode ser cobrado ao cliente o acesso à aplicação, normalmente em pagamentos anuais, mensais, ou semestrais[Silverback Data Center Solutions, 2024].

Este modelo de distribuição de software destaca-se na sua escalabilidade, acessibilidade de utilização, baixo custo, e facilidade de realizar atualizações.

Escalabilidade Como as aplicações SaaS correm na cloud, muitas vezes utilizando serviços como a Amazon Web Services[3] ou a Google Cloud [4], o que permite alterar a escala da aplicação de um modo quase instantâneo.

Acessibilidade Como é um serviço acedido através da Internet, pode ser acedido em qualquer lugar onde exista uma conexão à rede. Isto permite não só uma alta portabilidade, como também estende o seu uso a utilizadores que tenham dificuldades em deslocar-se, tais como quem viva no estrangeiro, ou tenha condições físicas impeditivas.

Baixo Custo de Utilização Arquiteturas SaaS eliminam quase completamente a necessidade da parte do cliente de investir em hardware capaz de correr a aplicação - todos os recursos necessários são da responsabilidade da entidade que cria o produto. No contexto de uma plataforma de voto online, Orman [2019] indica que "O acesso à Internet através de smartphones será quase universal e poderá ter um custo por voto essencialmente nulo."

Atualizações Numa aplicação SaaS, tipicamente é a entidade criadora do produto a única responsável pela realização de atualizações e de manter o seu produto na versão mais recente. A conexão por Internet significa que "podem ser implementados patches de segurança centralmente em toda a infrsestrutura, permitindo atualizações rápidas e consistentes"[v500 Systems, 2024], o que, na eventualidade de uma vulnerabilidade ser descoberta, permite uma mitigação de danos muito maior.

[2] IBM Technology: https://www.youtube.com/watch?v=20QUNgFIrK0 (úlimo acesso em 20-01-2023)

[3] https://aws.amazon.com/ (úlimo acesso em 19-01-2023)

[4] Google: https://cloud.google.com/ (úlimo acesso em 19-01-2023)

2.1.1 Categorias de SaaS

SaaS Vertical

SaaS vertical é "software construído com foco em nichos da indústria claros"[Koombea, 2024], como por exemplo de saúde, de *retail*, ou de finanças, e tem como objetivo ser uma solução única para uma determinada entidade ou grupo de entidades semelhantes.

SaaS Horizontal

Aplicações que seguem SaaS horizontal tendem a focar num grupo restrito de funcionalidades como, por exemplo, Dropbox, Slack, ou Salesforce, onde o objetivo é fornecer um "serviço amplo que pode cobrir uma vasta gama do mercado em vários setores"[Koombea, 2024].
O eVoto será horizontal pois pretende apenas ser uma aplicação de eleições.

2.1.2 Fragmentação de bases de dados

Para que a próxima secção seja compreendida na sua totalidade, é necessário fazer uma breve introdução à fragmentação de bases de dados (*data base sharding*). Esta secção tem como referência o artigo da DigitalOcean "Understanding Database Sharding", por Mark Drake[5].

Fragmentação de bases de dados é o processo de separar as linhas de uma tabela da base de dados em várias tabelas - particionamento horizontal. Estas tabelas denominam-se partições ou fragmentos. Refere-se especificamente à divisão horizontal das tabelas, sendo que existem também particionamento vertical, que não será relevante para esta secção.

Estes fragmentos são chamados de "fragmentos lógicos"e são agrupados em vários nodos da base de dados; estes nodos, por sua vez, são chamados de "fragmentos físicos".

Benefícios da fragmentação de bases de dados

- Facilita a divisão de carga entre várias máquinas, cada uma com o seu fragmento físico, diminuindo o tempo de resposta e permitindo mais tráfego na rede.
- A facilidade de fragmentação dá muita flexibilidade ao sistema.
- *Queries* à base de dados são mais rápidas dado terem de percorrer tabelas mais pequenas.

[5] https://www.digitalocean.com/community/tutorials/understanding-database-sharding (úlimo acesso em 22-11-2023)

- A separação física de fragmentos permite que, no caso de uma interrupção de serviço/rede/energia/etc, é mais provável que apenas um fragmento seja afetado.

Desvantagens da fragmentação de bases de dados

- A fragmentação de uma base de dados é um processo delicado.
- Existem múltiplos pontos de acesos aos dados, em vez de apenas um, dificultando o trabalho da equipa de desenvolvimento.
- Os fragmentos ficam, eventualmente, desequilibrados, à medida que mais e mais dados são inseridos. Por exemplo, uma empresa cliente tem uma grande expansão no negócio relativamente a outros clientes, o que causa que o seu fragmento fique mais "pesado".
- Reverter a fragmentação é um processo difícil e propenso a erros.
- A fragmentação não é suportada por defeito por muitos dos motores de bases de dados mais comuns; no entanto, existem variantes que o permitem, tais como MySQL Cluster ou MongoDB Atlas.

O eVoto poderá ou não beneficiar de uma base de dados fragmentada. Dado que a base de dados é apenas um dos componentes da arquitetura do sistema, a decisão de fragmentação deverá ser tomada considerando todos os aspetos da arquitetura.

2.1.3 Modelos de Tenancy

Existem diversos modelos de arquitetura, classificados consoante o tipo de *tenancy*, que serão explorados nesta secção. A informação aqui apresentada foi elaborada com base em informações vetadas pelo Senior Software Developer Sandro Rodrigues, e pelas seguintes referências: Fortra [2018], Microsoft [2023].

Arquitetura Single-Tenant

Cada utilizador tem a sua instância dedicada, assim como a sua própria infraestrutura, servidor, e base de dados. Isto permite que os utilizadores não tenham de competir por recursos e permite que cada um personalize e escale a sua instância em relação ao que necessita.

Arquitetura Multi-Tenant

Este tipo de arquitetura carateriza-se pela partilha de componentes por mais do que um utilizador. É particularmente útil para o caso de um utilizador necessitar de um ou mais componentes dedicados, mas pode partilhar outros componentes com outros utilizadores. Um dos componentes que mais frequentemente é dedicado a cada utilizador é a base de dados.

Modelos de bases de dados em arquitetura multi-tenant

Fonte de dados: Microsoft [2023].

1. Uma base de dados por utilizador

   Cada utilizador tem a sua própria base de dados dedicada, e pode ser escalada tanto horizontalmente (mais nodos) como verticalmente (mais recursos por nodo).

2. Uma base de dados por vários utilizadores

   Uma base de dados é partilhada por vários utilizadores. Tem o problema de que, como os recursos são partilhados, se um utilizador estiver a utilizar bastantes recursos, os outros utilizadores vão ver uma queda no desempenho e aumento no tempo de resposta. É uma solução de menor custo comparativamente com a anterior, sacrificando desempenho e isolamento de *tenants*.

3. Base de dados *multi-tenant* fragmentada

   Fazer a fragmentação de uma base de dados permite melhorar o desempenho e a eficiência operacional de uma base de dados. As mesmas bases de dados fragmentadas podem ser movidas entre grupos para aumentar a eficiência operacional (ver 2.1.2).

4. Base de dados *multi-tenant* fragmentada híbrida

   Todas as bases de dados possuem um identificador de *tenant* no seu *schema*[6]. Todas são capazes de conter mais do que um *tenant*, e podem ser fragmentadas.

   Para o *schema*, são todas bases de dados multi-tenant - no entanto, algumas serão dedicadas a apenas um.

É feita uma análise mais aprofundada destas arquiteturas, incluindo qual será a mais indicada para o eVoto, na secção 7.2.

6 *Schema* é o esquema que define a estrutura de uma base de dados, incluindo tabelas, campos, relações e restrições.

2.1.4 Exemplos de Utilização

Esta secção contém uma análise superficial de vários produtos de software que seguem o modelo SaaS, com o intuito de encontrar caraterísticas comuns entre plataformas que seguem esse serviço. No entanto, para preservar uma leitura fluída, esta análise e as suas referências foram transferidas para o apêndice A, mantendo-se nesta secção apenas um resumo das conclusões obtidas.

A análise foi feita segundo várias categorias: função, front-end, back-end, escalabilidade, desempenho e segurança, com as seguintes conclusões:

Caraterística	Conclusões da Análise
Front-end	Utilização de tecnologias já estandardizadas: Javascript, PHP, HTML/CSS
Back-end	Utilização de tecnologias já estandardizadas: Javascript, PHP, e para bases de dados MySQL e PostgreSQL
Escalabilidade	Utilização de serviços como Google Cloud e Amazon Cloud Services; é altamente dependente do hardware onde está instalada a solução
Desempenho	São quase sempre oferecidas ao cliente o mesmo conjunto de opções para melhoramento de desempenho (limpeza de cache, desativar add-ons, redução da qualidade/compressão de dados, etc)
Segurança	É utilizada uma miríade de soluções diferentes para assegurar a segurança do utilizador enquanto interage com a plataforma, nomeadamente: (1) utilização de inteligência artificial para deteção de tentativas de fraude (2) fornecimento de uma ferramenta de deteção de ameaças *all-inclusive* (3) adoção de políticas durante o desenvolvimento da plataforma que aumentam a segurança, tais como: encriptação de várias camadas utilizando SSL/TLS[a], princípios de segurança tais como SSO[b]/SAML[c] e 2FA[d] (4) existência de uma plataforma dedicada à reportagem, por parte dos utilizadores, de erros e falhas de segurança (5) ferramentas de monitorização e criação de logs (6) diferentes perfis de utilizador que detalham permissões de acesso a partes mais vulneráveis do software e definição de passos a seguir pelo utilizador que tenha detetado uma falha na segurança

Tabela 1: Conclusões da análise a plataformas SaaS variadas.

[a] Secure Sockets Layer (SSL) e Transport Layer Security (TLS) são protocolos de criptografia que fornecem comunicação segura pela Internet.

[b] Single Sign-On (SSO) é um sistema que permite aos utilizadores aceder várias plataformas com apenas um *set* de credenciais.

[c] Security Assertion Markup Language (SAML) é um padrão para troca de dados de autenticação e autorização entre partes.

[d] Autenticação de dois fatores (2FA) é um processo de segurança que exige que sejam fornecidos dois fatores de autenticação diferentes.

2.2 Contextualização na Área Tecnológica

Esta secção tem o objetivo de contextualizar o leitor na área tecnológica referente, especificamente, ao software de voto, e pretende estabelecer e definir conceitos comuns utilizados nesta área.

2.2.1 Distinção entre voto eletrónico e voto online

Ao longo deste documento, irão surgir dois termos: voto eletrónico (ou e-voto), e voto online. Á primeira vista, parecem referir-se ao mesmo tipo de votação - no entanto, existe uma distinção, muito relevante para este projeto de mestrado.

Voto eletrónico/e-voto trata-se de um termo genérico, que engloba vários tipos de voto. Segundo o artigo "Voto eletrónico: o que é, onde existe e como funciona", da plataforma da Caixa Geral de Depósitos[7]:

> *"Quando é feito à distância, através da internet, exige uma plataforma específica e um sistema de autenticação como, por exemplo, a Chave Móvel Digital. Nestes casos, têm de ser tomadas medidas para garantir não só a confidencialidade do voto, mas também que a plataforma resista a ataques informáticos capazes de corromper a eleição.*
>
> *"Mas o voto eletrónico também pode ser feito no local de votação, sem recurso a boletins físicos. Ou seja, usando máquinas para registar o seu voto. Mais uma vez, os sistemas criados têm que ser confiáveis, seguros e, ao mesmo tempo, de fácil utilização, para evitar a exclusão de pessoas com menos competências digitais."*

Segundo esta definição, conclui-se que o voto eletrónico pode ser feito de modo remoto ou presencial, sendo que o primeiro é feito através da internet com recurso a um dispositivo propriedade do eleitor, enquanto que o segundo dá uso a máquinas de votação sem papel, normalmente instaladas pela entidade responsável pela organização da eleição.

O **voto online** pertence ao grupo de votos descritos pelo termo "voto eletrónico", mas refere-se, especificamente, ao voto descrito no primeiro parágrafo.

2.2.2 Correção de Voto

O termo "correção de voto"(em inglês, *voting correctness*) é definido por Juels et al. [2005] do seguinte modo:

> *"Esta propriedade tem, de facto, duas facetas: primeiro, estabelece que um adversário A não pode antecipar, alterar, ou cancelar os votos honestos, ou seja, votos de eleitores que não são controlados [por A]; segundo, estabelece que A não poderá causar com que eleitores votem de modo que seja alcançado um voto múltiplo, ou seja, a utilização de uma única*

[7] https://www.cgd.pt/Site/Saldo-Positivo/leis-e-impostos/Pages/voto-eletronico.aspx (úlimo acesso em 09-10-2024)

credencial para votar múltiplas vezes, onde é contado mais do que um voto por credencial na contagem de votos."

Entende-se, então, que correção de voto é a propriedade que garante que os votos são emitidos e contados corretamente, mesmo quando existe uma entidade maliciosa com controlo sobre uma parte dos eleitores e, consequentemente, capaz de influenciar os seus votos.

2.2.3 Verificabilidade

Juels et al. [2005] define verificabilidade (em inglês "verifiability") como sendo:

"Dada a capacidade de um adversário A, no entanto, para corromper algum número de autoridades [de contagem], não podemos ter certeza de que a contagem seja sempre computada corretamente. A propriedade da verificabilidade é a capacidade de qualquer jogador verificar se a contagem (...) foi calculada corretamente, ou seja, detetar qualquer mau comportamento [da autoridade de contagem] ao aplicar a função [de contagem]."

Ou seja, podemos definir verificabilidade como a capacidade que um sistema de voto eletrónico tem de permitir que cada utilizador do produto verifique que o seu (ou um dado) voto foi contado corretamente.

2.2.4 Rasto de auditoria de voto em papel verificado pelo eleitor

Em inglês "Voter-verified paper audit trail"(VVPAT), é um sistema de votação eletrónica que serve de suporte para eleições físicas. ACE Electoral Knowledge Network [2023] indica que, com este sistema, quando um eleitor se desloca a uma máquina de voto eletrónico e confirma a sua opção no sistema informático, é impresso um cartão onde o eleitor pode verificar se a opção apresentada coincide com a sua escolha.

Devido a estas caraterísticas, o sistema VVPAT só pode ser utilizado em "sistemas de e-voto não-remotos (e-voto no local de votação)"[ACE Electoral Knowledge Network, 2023].

Indica também que este processo cria um rasto de votos em papel que permitem realizar auditorias ou novas contagens pós-eleição, de modo a comparar com os votos marcados pelo sistema eletrónico e, assim, detetar alterações não planeadas no sistema informático.

2.2.5 Auditabilidade

ACE Electoral Knowledge Network [2023] diz que "o maior risco para sistemas de e-voto é se interferência externa nos sistemas é possível e consegue permanecer indetetável, afetando os resultados da votação". É neste contexto que auditabilidade ("auditability") é definida.

Auditabilidade significa que o processo eleitoral pode ser examinado e verificado para garantir a sua integridade, incluindo a capacidade de rastrear e verificar qualquer uma das etapas do processo de eleição, especialmente as mais cruciais - votação e contagem. Também deve permitir verificar quaisquer medidas administrativas e de segurança.

O sistema de auditoria tem, essencialmente, que ser capaz de "detetar fraude do voto e disponibilizar provas de que todos os votos contados são autênticos"[ACE Electoral Knowledge Network, 2023], mantendo o anonimato do voto e protegendo-o contra acesso não autorizado.

Parte II

Core da Dissertação

Capítulo 3

Certificações Relevantes

Esta secção é dedicada à análise de várias certificações relevantes e ao estudo da aplicação destas mesmas no contexto do eVoto.

A caraterística que é possivelmente a mais crucial para o sucesso do eVoto reside não na Dipcode, nem nos seus colaboradores ou processos internos, mas sim no público-alvo; e, mais importante, na sua perceção da segurança oferecida pela plataforma.

De facto, o maior fator impeditivo da implementação generalizada de sistemas de votação online é a segurança, e a capacidade destes sistemas de não só a assegurarem, como também possuírem os mecanismos necessários para deteção de falhas.

Schürmann et al. [2015] diz que a tecnologia usada em eleições tem dois objetivos: o primeiro, de "garantir que toda a informação produzida durante o processo eleitoral (...) seja correta e confiável"; o segundo, de "gerar ampla aceitação de que o resultado eleitoral é uma representação verdadeira e justa da vontade dos cidadãos".

A obtenção de uma certificação é importante para não só assegurar internamente a natureza democrática de uma eleição, como também para que qualquer entidade externa (seja como administrador, eleitor, cliente, *stakeholder*, etc) que interaja com o eVoto tenha um nível de confiança elevado em relação a todo o processo eleitoral, algo que só é alcançável com uma certificação relevante.

Nomeadamente, segundo Schürmann et al. [2015], com a obtenção de uma certificação todas as entidades eleitorais terão um "maior nível de confiança"de que as tecnologias eleitorais irão:

- corresponder às suas expectativas;
- estar livre de erros óbvios;
- ser documentado para que especialistas e utilizadores futuros possam entender e operar as tecnologias adequadamente;

- fornecer um meio de controlo eficaz sobre todos os stakeholders eleitorais - e não apenas sobre os utilizadores imediatos dentro do corpo de gestão eleitoral.

Esta opinião de que obter certificação é um passo crucial é também partilhada pelo próprio Conselho Europeu, que indica que "Embora cada um destes protocolos possa desempenhar um papel no processo de certificação, uma combinação deles pode ser mais útil."[Council of Europe, 2011]. Aponta inclusive alguns exemplos concretos, nomeadamente: ISO 9001, o ISO 9000-3, ISO/IEC 27001, e o "Content Management System and Common Criteria (ISO 15408)".

A Eurotux já é detentora de uma certificação em ISO 9001, pelo que não será explorado nesta secção. Já em relação ao ISO 9000-3, foi revisto e reescrito desde a publicação de Council of Europe [2011], tendo sido substituído pelo ISO/IEC/IEEE 90003:2018, que será explorado abaixo. Finalmente, o ISO 15408 é no momento denominado por ISO/IEC 15408-1:2022.

Council of Europe [2011] levanta também uma questão relevante, que é a de que a certificação ISO é "limitada no tempo"e, por isso, "o processo de certificação ISO precisará ser repetido a cada eleição", levando a possíveis custos proibitivos. Este terá de ser um fator a considerar relativamente à decisão de obtenção de certificações.

Para efeitos de investigação, para cada uma das certificações listadas, foram apenas consultados os excertos abertos ao público, consistindo nas secções 1, 2, e 3. Deve também ser notado que as certificações foram analisadas sob o contexto específico do eVoto - logo, mesmo se forem demonstradas como benéficas para a Dipcode, se não beneficiarem particularmente o projeto do eVoto não serão consideradas.

3.1 ISO/TS 54001:2019

Quality management systems — Particular requirements for the application of ISO 9001:2015 for electoral organizations at all levels of government[1]

Este documento[ISO, 2019] é um guia para um outro documento, o ISO 9001:2015. É, de facto, estruturado à volta do ISO 9001:2015, acompanhando cada uma das suas secções e esclarecendo quais as nuances e quais os detalhes relevantes para entidades no setor de organização eleitoral.

Como a Eurotux já é certificada no standard descrito em ISO 9001:2015[ISO, 2015], esta pode ser uma certificação a considerar obter.

[1] Em português: Sistemas de gestão de qualidade — Requisitos particulares para a aplicação da ISO 9001:2015 para organizações eleitorais a todos os níveis de governo.

Um ponto importante a reparar é para que tipo de entidade é destinado este documento: "organizações eleitorais em todos os níveis do governo". Segundo o ISO/TS 54001:2019, uma organização eleitoral é definida do seguinte modo:

> *"Órgãos eleitorais são instituições que têm como responsabilidade a administração do processo eleitoral, incluindo a preparação, organização, gestão, acompanhamento e promoção da eleição, a votação e apuramento dos votos, a resolução de litígios eleitorais ou a declaração oficial dos resultados eleitorais."*

Embora não realize estas tarefas diretamente, a Dipcode seria classificada como um dos órgãos eleitorais descritos, uma vez que é responsável pelo desenvolvimento do eVoto, que por sua vez terá a função de implementar os procedimentos acima descritos.

O ISO/TS 54001:2019 oferece várias indicações ao longo de todo o documento, onde se salientam as seguintes[2]:

1. "O registo e identificação dos eleitores elegíveis e o registo das organizações políticas e dos candidatos são essenciais para o processo eleitoral."

2. "O processo eleitoral é composto por um conjunto de processos interrelacionados, conduzidos pelos órgãos eleitorais, pelas organizações políticas e pela cidadania. Esses elementos essenciais incluem determinar quem é elegível para votar, registo de organizações políticas e candidatos, logística eleitoral, votação, contagem e registo preciso dos votos, declaração de resultados, educação eleitoral, supervisão do financiamento de campanha e resolução de disputas eleitorais."

3. "A implementação completa e transparente de cada processo constitui a base para que o corpo eleitoral seja legítimo."

   Dado que o código do eVoto será open-source, considera-se que este ponto é respeitado.

4. "A criação e implementação do sistema de gestão da qualidade de um órgão eleitoral é influenciada por suas obrigações sob o quadro jurídico aplicável conforme determinado pelo direito internacional, pelas constituições nacionais e pela legislação nacional."

   Apesar de não ter sido concebido com eleições governamentais como objetivo, o eVotUM está preparado para tal. No entanto, devido ao modelo de negócio do eVoto poderão surgir

[2] Os elementos enumerados constituem citações que foram traduzidas.

novas regras a seguir e, por isso, foi feita uma investigação da lei em torno de sistemas de voto online na secção 4.

5. "É fundamental que o eleitor conheça as diferentes etapas do processo eleitoral. (...) São estabelecidos processos para garantir que a informação relativa aos candidatos, propostas de voto e locais de votação esteja disponível para os eleitores antes da eleição."

   Utilizando o exemplo de uma eleição fictícia na Universidade do Minho, bastaria ser enviado um email ao corpo estudantil com informações relativas à eleição, logo este ponto é considerado como sendo já cumprido pelo sistema eVotUM atual e prevê-se que será respeitado pelo eVoto.

6. "(...) deve haver resolução e comunicação justas e oportunas de reclamações e de apelos eleitorais."

   Havendo um formulário de contacto na página do eVoto, em princípio, este ponto já será coberto.

7. "[O QMS] especifica requisitos para um sistema de gestão de qualidade onde uma organização eleitoral:

   (1) "Precisa de demonstrar a sua capacidade de administrar eleições por voto secreto, fornecer resultados confiáveis, transparentes, livres e justos que cumpram os requisitos eleitorais;

   (2) "No quadro legal estabelecido, visa aumentar a confiança dos cidadãos, dos candidatos, das organizações políticas e de outras entidades eleitorais interessadas através da implementação efetiva do sistema de gestão da qualidade eleitoral, incluindo processos para melhoria contínua."

   A obtenção de uma certificação será o caminho mais certo a tomar para demonstrar estes dois pontos.

Considera-se que poderia ser vantajoso obter esta certificação, desde que o custo não fosse proibitivo, especialmente considerando a natureza temporal cíclica das eleições versus as revisões constantes das certificações. É uma certificação especialmente apelativa de obter dado que não é muito comum entre concorrentes da Dipcode atualmente no mercado.

Deve-se indicar, no entanto, que este documento não se destina especificamente a eleições online, mas sim a eleições em geral, abordando assuntos como, por exemplo, o marketing relacionado com uma

eleição. Neste exemplo, o marketing não parece ser algo pelo qual o eVoto deva ser responsável, uma vez que é apenas uma plataforma para as eleições (se não considerarmos o envio de emails como marketing). Por outro lado, se estivermos a falar sobre eleições presenciais, faz mais sentido que a organização eleitoral seja responsável pelo marketing (tal como o documento indica), pois é ela que organiza toda a eleição.

Não obstante, entende-se que a linguagem utilizada possa ser aplicada também às eleições online, o que significa que obter esta certificação poderá ser não só viável, como útil.

3.2 ISO/IEC/IEEE 90003:2018

Software engineering — Guidelines for the application of ISO 9001:2015 to computer software[3]

Este documento[ISO, 2018] é um guia baseado no ISO 9001:2015 com foco na "aquisição, fornecimento, desenvolvimento, operação e manutenção de software de computador", e define as questões que devem ser abordadas "independentemente da tecnologia, modelos de ciclo de vida, processos de desenvolvimento, sequência de atividades e estrutura organizacional utilizada por uma dada organização".

Essencialmente, o documento fornece orientação para auxiliar na compreensão de como as cláusulas do ISO 9001:2015 se aplicam no contexto de software de computador.

No prefácio, o documento recomenda também que organizações interessadas podem consultar os processos do ISO/IEC/IEEE 12207, entre outros.

Seria preciso obter o documento completo para analisar em detalhe se realmente é necessário adquirir a certificação, contudo, esta análise preliminar indica que tal não seria vantajoso para a Dipcode.

A Dipcode é uma empresa com bastante experiência e uma vasta presença no mercado informático, sendo que ao longo dos seus anos de operação e até à data atual, não foi sentida a necessidade de obter esta certificação. Poderia ser considerado vantajoso obtê-la em algum ponto futuro, no entanto, o âmbito específico do eVoto não levanta necessidade para tal.

Não se considera, então, que esta certificação seja vantajosa de obter.

[3] Em português: Engenharia de Software - Diretrizes para a aplicação do ISO 9001:2015 a software de computador.

3.3 ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements[4]

Este documento[ISO, 2017b] especifica os requisitos para "estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação" e para a "avaliação e tratamento de riscos de segurança da informação" de uma dada organização.

Na introdução, é salientado que uma organização que esteja certificada no ISO/IEC 27001:2022 tem, obrigatoriamente, de cumprir todas as cláusulas relevantes (4 a 10, sendo que 1, 2, e 3 são apenas de introdução ao documento). É também mencionado que o sistema de gestão de segurança de informação seja "parte e integrado aos processos da organização e à estrutura geral de gestão", incluindo que estes devem ser considerados a todos os níveis da empresa, nomeadamente "no desenho de processos, sistemas de informação e controlos de informação".

Relacionado com o trabalho realizado para uma outra dissertação organizada pela Eurotux, foi delineado trabalho futuro para a implementação da versão de 2013 desta certificação, com a eventual atualização para a versão de 2022 através de pequenos ajustes que estejam em falta. A obtenção desta certificação é especialmente relevante considerando que vários concorrentes da Eurotux também a têm, nomeadamente o invote[5], criado pela empresa espanhola Scytl.

3.4 ISO/IEC 15408

ISO/IEC 15408-1:2022 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model[6]

Este documento[ISO, 2022a] estabelece os "conceitos e princípios gerais de avaliação de segurança de TI" e especifica o "modelo geral de avaliação" fornecido por várias partes desta norma que é a base para a avaliação das propriedades de segurança de produtos de TI de uma dada organização.

Também oferece uma visão geral de todas as partes da norma ISO/IEC 15408 e estabelece vários conceitos necessários ao bom cumprimento dela, assim como uma introdução a "conceitos básicos de segurança necessários para avaliação de produtos de TI".

ISO/IEC 15408-2:2022 - Information security, cybersecurity and privacy protection — Eva-

[4] Segurança de informação, cibersegurança, e proteção de privacidade - Sistemas de gestão de segurança de informação - Requisitos

[5] Scytl: https://www.scytl.com/portfolio#INVOTE (úlimo acesso em 09-10-2024)

[6] Em português: Segurança de informação, cibersegurança e proteção de privacidade — Critérios de avaliação para segurança de TI — Parte 1: Introdução e modelo geral

luation criteria for IT security — Part 2: Security functional components[7]

O grupo-alvo deste documento[ISO, 2022b] é definido como sendo consumidores, developers, e avaliadores de produtos de TI. Também define a estrutura e o conteúdo necessários para os componentes funcionais de segurança que serão avaliados para os padrões desta norma. Inclui, ainda, um catálogo de componentes funcionais que cumprem os requisitos de segurança mais comuns no mundo de TI.

Tal como mencionado antes, a segurança é um dos fatores mais limitantes da expansão de uma solução de voto online no mercado. A obtenção de uma certificação nesta área informática seria uma mais valia para a Dipcode; no entanto, as alterações necessárias para cumprir esta norma poderiam resultar num custo proibitivo.

3.5 ISO/IEC/IEEE 12207:2017

Systems and software engineering — Software life cycle processes[8]

Este documento[ISO, 2017a] define a estrutura comum aos processos que compõem o ciclo de vida de um pedaço de software, define a terminologia associada, e contém "processos, atividades e tarefas aplicáveis"durante a todo o ciclo de vida do software, desde a aquisição até à desativação. Define, também, processos para "definir, controlar e melhorar os processos"para uma dada organização.

Esta norma tem como audiência todas as partes participantes na criação e manutenção de um pedaço de software, desde os compradores, os *developers*, os gestores, até aos utilizadores.

No entanto, nota-se que este documento não prescreve um modelo específico de "ciclo de vida de software, metodologia de desenvolvimento, método, abordagem de modelo ou técnica", sendo que são os utilizadores desta norma os responsáveis por tal. O documento também não define qualquer metodologia, método, modelos ou técnicas em relação a um dado tipo de projeto.

Uma mais valia deste documento é que é explicitamente compatível com o sistema de gestão de qualidade definido na norma ISO 9001[ISO, 2015], que a Eurotux já cumpre, assim como também é compatível com várias outras normas, nomeadamente o ISO/IEC 20000-1 (IEEE Std 20000-1) e ISO/IEC 27000.

7 Em português: Segurança de informação, cibersegurança e proteção de privacidade — Critérios de avaliação para segurança de TI — Parte 2: Componentes funcionais de segurança

8 Em português: Sistemas e Engenharia de Software - Processos de Ciclo de Vida de Software

3.6 Investigação aprofundada da certificação ISO/TS 54001:2019

É possível consultar a análise completa desta certificação no anexo F.

Depois de uma reunião interna[9], chegou-se à conclusão de que seria vantajoso comprar e analisar mais profundamente a especificação ISO/TS 54001:2019.

A análise foi realizada em duas fases, com uma terceira fase final dedicada à sua apresentação aos responsáveis da empresa e à decisão de prosseguir, ou não, com a certificação.

A primeira fase consistiu em analisar cada uma das cláusulas, anotando os pontos importantes e indicando de que modo é que a Dipcode as cumpre ou pode cumprir.

De modo a obedecer à política de privacidade da certificação, não é possível citar qualquer excerto, pelo que se segue um resumo das notas tomadas durante esta fase da análise:

- A maioria das cláusulas classificadas como "Não Cumprido"são referentes à criação de documentação do sistema de gestão do voto, incluindo a definição de entidades, a definição das suas responsabilidades e necessidades, e também a definição de todos os processos que constituem uma eleição, entre outros.

- As cláusulas marcadas com "Difícil"são cláusulas que focam explicitamente em processos que só são relevantes para eleições físicas, como por exemplo, a definição dos trabalhadores que irão realizar a supervisão da eleição. Estas constituem o maior entrave à obtenção desta certificação, e serão exploradas nas secções seguintes.

- A análise permitiu notar que uma possível vertente pela qual o eVoto poderia enveredar é o da acessibilidade. Acessibilidade já é uma das grandes razões pela qual o voto online está a ganhar importância no mercado - comercializar o eVoto como sendo uma opção altamente acessível poderia ser uma boa estratégia.

  Por exemplo, garantir que o eVoto:

  1. é acessível a leitores de ecrã;
  2. não necessita de muita destreza (p.e. pessoas com tremores de mãos);
  3. é navegável e utilizável apenas por teclado;
  4. possui modo de alto contraste;

[9] Presentes: Daniela Costa (COO) e Andreia Félix (Senior Project manager).

5. possui modo para daltonismo (quer com mudança de cores, quer com a utilização de símbolos por cor);
6. indique o foco do cursor claramente;
7. entre outros.

- Também poderia ser interessante fornecer um serviço de suporte em formato de chatbot, considerando os avanços atuais no ramo da inteligência artificial. Uma das soluções já existentes no mercado, o ElectionBuddy, possui um destes serviços na sua página inicial.
- Uma das cláusulas da certificação é referente ao levantamento de opiniões dos utilizadores. Seria interessante implementar, por exemplo, um pop-up que apareceria ao eleitor depois do lançamento e registo do voto a pedir para classificar a aplicação. Isto podia ser aplicado apenas a uma parte do corpo eleitoral, ou apenas durante um intervalo de tempo, ou apenas para a primeira eleição de uma dada conta.

A segunda fase da análise consistiu em determinar em que classificação é que cada uma das cláusulas se enquadra. As classificações são as seguintes:

Sem Informação Caso não exista informação adicional à do ISO 9001, ou caso a informação dada não seja relevante. Estes pontos podem ser contados como cumpridos.

Não Cumprido São pontos que podem ser cumpridos. A esmagadora maioria dos pontos com esta classificação são referentes a documentação que deve ser criada e não a limitações técnicas.

Cumprido Já cumprido.

Semi Cumprido Estes pontos já têm partes de si cumpridas, mas falta algum desenvolvimento ou documentação para cumprir na totalidade.

Difícil A maior parte destes pontos têm referências explícitas a eleições físicas que, pela natureza do eVoto, são (quase) impossíveis de satisfazer.

A distribuição percentual destas classificações pelas cláusulas da certificação estão ilustradas no gráfico 2.

Podemos observar que 89% das normas definidas estão ou podem ser satisfeitas, sendo que os restantes 11% são dificilmente cumpridas do modo definido pela norma.

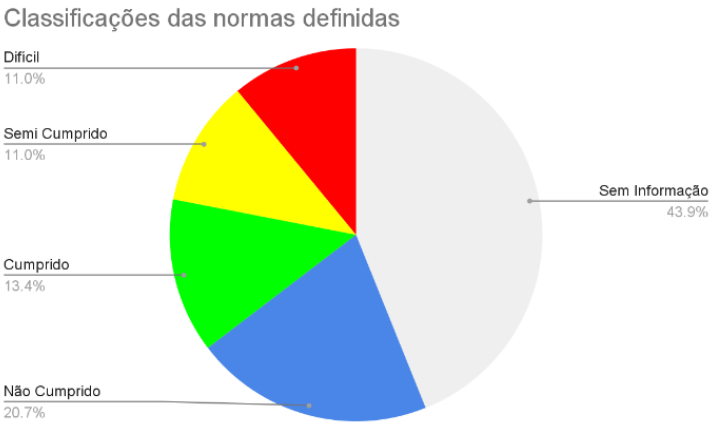


Figura 2: Classificações das normas definidas

As normas com classificação Difícil referem diretamente procedimentos e logística de eleições físicas, tais como a estipulação do acesso à saída e à entrada do local de voto, algo que não existe numa eleição online. Tornam-se, assim, impossíveis de cumprir para o eVoto.

Este foi o maior problema encontrado. Não parece existir alguma forma de implementar estas cláusulas no eVoto, pelo que, mesmo que todas as outras fossem cumpridas, a empresa não conseguiria obter a certificação na ISO/TS 54001:2019.

No entanto, o facto de que o eVotUM já cumpre a maioria destas cláusulas pode mesmo assim ser aproveitado. Na sequência de uma reunião interna[10], foi sugerida uma solução alternativa à da obtenção da certificação, que consiste na criação de uma página web com uma comparação entre o que os requisitos da norma ISO/TS 54001:2019 definem, e o modo como o eVoto satisfaz essas cláusulas. Em essência, apresentar uma lista de pares Requisito-Caraterística.

No entanto, considera-se que esta opção terá de ser descartada, pois poderia induzir o cliente em erro, dado poder implicar que o eVoto é detentor desta certificação, quando não é. Pode também gerar desconfiança, pois estaria a ser apresentada informação de que o eVoto cumpriria (maioritariamente) os requisitos da norma e que, no entanto, não a obteve.

3.7 Solução alternativa

No seguimento de uma reunião[11], foi explorada uma solução alternativa para a apresentação das várias caraterísticas do eVoto. O *power-point* utilizado na apresentação pode ser consultado na íntegra no

[10] Com Daniela Costa (Chief Operating Officer) e Andreia Félix (Senior Project Manager).

[11] Com Andreia Félix (Senior Project Manager).

apêndice B.

Esta solução alternativa consiste em apresentar, no site do eVoto, uma listagem das suas caraterísticas. Este tipo de listagem é muito utilizado, dado que quase todas as soluções de voto online já presentes no mercado apresentam algo deste estilo.

1. O primeiro tipo de apresentação de caraterísticas é no formato de caixas.

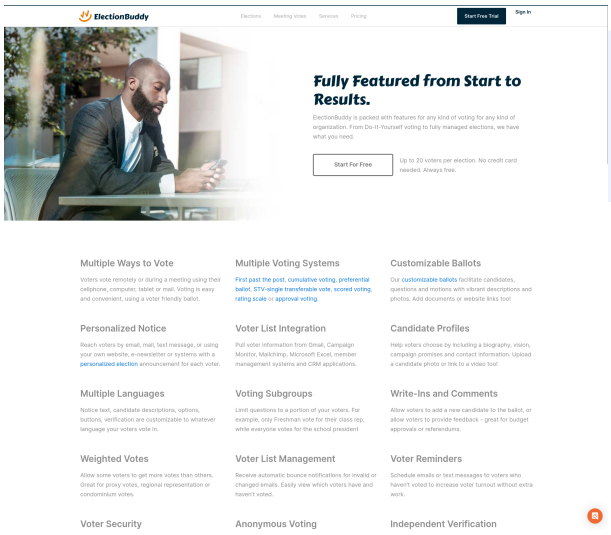


Figura 3: ElectionBuddy - formato em caixas.

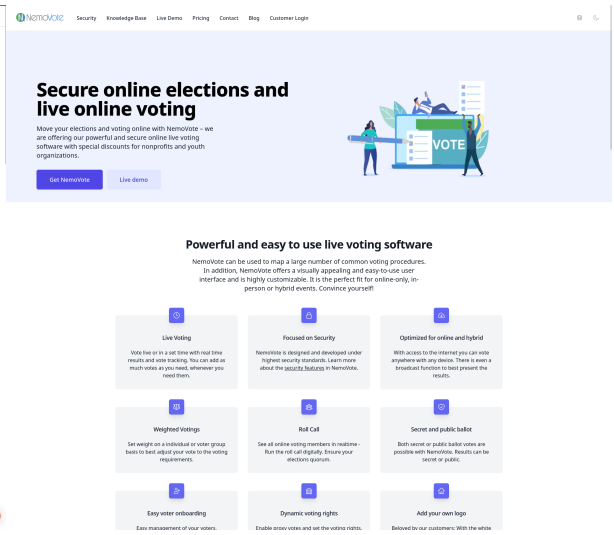


Figura 4: NemoVote - formato em caixas.

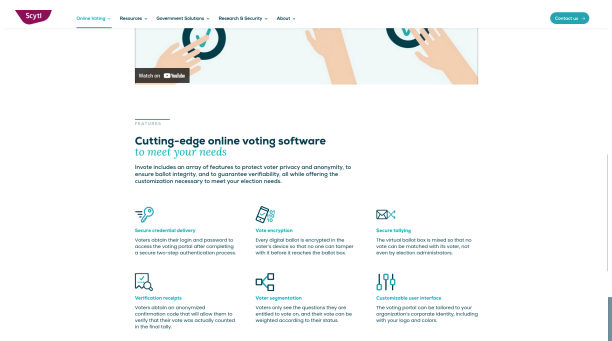


Figura 5: InVote (Scytl) - formato em caixas.

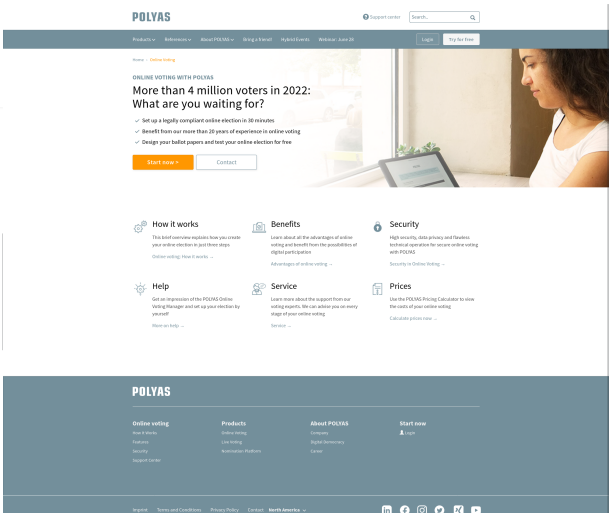


Figura 6: Polyas - formato em caixas.

Cada caixa é dedicada a uma característica distinta da plataforma em questão, geralmente composta por um título, um pequeno parágrafo com a descrição da característica, e um ícone ilustrativo. É um estilo de apresentação que captura e retém a atenção do utilizador, e parece ser o mais utilizado para este

contexto. A utilização de ícones fornece ainda mais informação ao utilizador e permite uma experiência de navegação mais rápida, eficiente, e apelativa.

2. Outro tipo de apresentação é o da descrição detalhada.

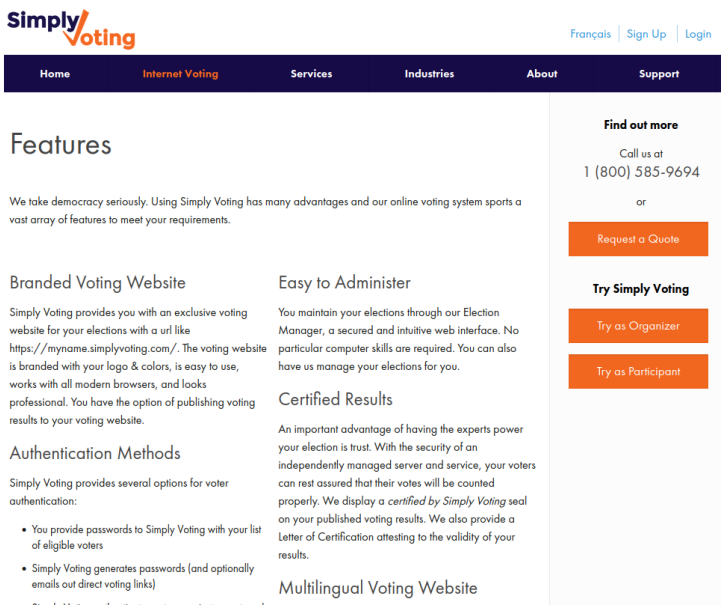


Figura 7: SimplyVoting - descrição detalhada.

É o mais fácil de implementar numa página web, e é a opção que oferece mais informação. No entanto, para um utilizador que ainda não tenha interesse na ferramenta, uma página de texto não é apelativa, pois requer mais trabalho para descobrir informação, para além de ser mais demorado. No entanto, como uma página secundária, funcionaria perfeitamente.

Por exemplo, o eVoto poderia ter uma página principal com as caraterísticas resumidas em caixas, e cada caixa poderia ter um link "Saber mais"para a secção relevante na página secundária. Esta página secundária teria o formato de descrição detalhada e ofereceria informação mais detalhada acerca da plataforma.

3. Por fim, o último tipo de apresentação é o da tabela de comparação.

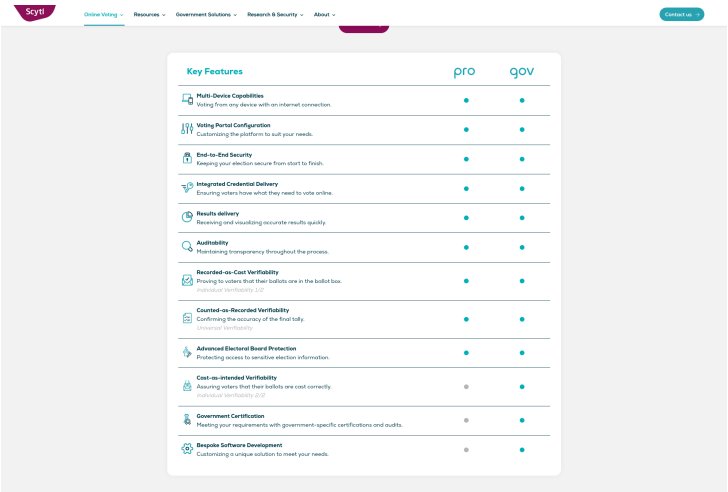


Figura 8: InVote (Scytl) - tabela de comparação.

O tipo de apresentação em tabela de comparação é particularmente útil para mostrar ao utilizador quais as diferenças entre diversos planos de subscrição, de um modo rápido e fácil de ler. É o modo mais comum para ferramentas com vários tipos de subscrições, pois permite uma comparação rápida entre os serviços oferecidos, sem ocupar demasiado espaço na página.

Considera-se que este é o método mais eficiente para apresentar informação sobre as diferentes subscrições do eVoto.

Capítulo 4

Análise Histórica e Legal do Voto Eletrónico em Portugal e no Mundo

Segundo Comissão Nacional de Eleições [2023], foram desenvolvidas em Portugal "quatro experiências de voto eletrónico, respetivamente em 1997, 2001, 2004 e 2005", todas apenas para efeitos de teste, onde o voto não foi vinculativo.

Particularmente, em 2005, foram realizadas duas experiências de voto eletrónico, uma presencial e a outra não presencial:

> *"(...) a experiência de voto electrónico não presencial foi disponibilizada aos eleitores portugueses residentes no estrangeiro mediante a disponibilização de uma plataforma de voto por Internet.*
>
> *"Deve referir-se que as experiências de voto electrónico presencial apresentaram níveis de adesão dos eleitores bastante significativos, particularmente por banda dos cidadãos eleitores invisuais que, com a implementação desta solução, passariam a votar por si e não, como fazem actualmente, acompanhados por outro eleitor."*

Através destas experiências concluiu-se que a utilização de voto eletrónico, tanto presencial como não presencial, permitiram "combater algumas causas do abstencionismo que, no caso português, se têm vindo a evidenciar em alguns actos eleitorais."É também salientado que o voto eletrónico é "mais eficaz e cómodo", o que contribui para a mitigação do absentionismo mencionado anteriormente.

Uma outra experiência mais recente foi realizada no distrito de Évora em 2019[SGMAI - Administração Eleitoral, 2019], para as eleições dos Deputados ao Parlamento Europeu, cujo âmbito era o teste de voto eletrónico presencial e a desmaterialização dos cadernos eleitorais. A experiência foi um sucesso, notando que:

- O sistema permitiu "evitar a impressão de 643 mil folhas de papel A4 (3,2 toneladas)"

- "Os resultados eleitorais expressos na urna informática revelaram ser autênticos"
- Possibilitou "obter o apuramento dos resultados eleitorais, logo após o encerramento da votação"
- "A média de eleitores por mesa de voto eletrónica foi o dobro da média do número de eleitores nas mesas de voto tradicional"

Num inquérito feito após a experiência, a qualidade mais referida por parte dos cidadãos de Évora acerca deste sistema de voto eletrónico foi a "facilidade de utilização do equipamento"[SGMAI - Administração Eleitoral, 2019].

Podemos concluir que a eventual implementação de um sistema de voto online - que seria ainda mais conveniente para os cidadãos, considerando que não precisariam de se deslocar para o local de voto - só iria facilitar ainda mais todo o processo de voto.

De facto, isto é corroborado por uma Resolução da Assembleia da República, onde se "Recomenda ao Governo que elabore e apresente à Assembleia da República os estudos necessários à introdução de voto eletrónico não presencial"[Assembleia da República, 2021], mencionando a Chave Móvel Digital como um possível método de autenticação seguro.

Apesar de as eleições eletrónicas (tanto presenciais como não presenciais) ainda não terem sido implementadas em Portugal para além de alguns testes, ao longo das últimas décadas têm ocorrido avanços significativos nesse sentido, especialmente nos processos e entidades relacionados com a organização das eleições.

Um exemplo com o qual a maioria dos cidadãos estará familiarizada é o recenseamento eleitoral, que já é realizado de forma eletrónica[SGMAI - Administração Eleitoral, 2023].

Apesar da existência de todos estes exemplos de tentativas de voto eletrónico, não existem leis explícitas para eleições online em Portugal, apenas leis que se aplicam a todas as eleições, físicas ou não:

- Tal como é de esperar, a constituição portuguesa deve ser cumprida, e nela é definido o sufrágio universal, o voto secreto e igualitário, e a transparência nas eleições.
- O SGMAI[1] define a Lei Eleitoral para a Assembleia da República[SGMAI, 2021].
- A Comissão Nacional de Eleições publicou recomendações, previamente mencionadas nesta secção.

Existem, no entanto, uma série de leis e diretrizes criadas pela União Europeia que cobrem este tipo de eleições, embora também de um modo geral:

[1] Secretaria-Geral do Ministério da Administração Interna.

- O Regulamento Geral sobre a Proteção de Dados (GDPR) define regras para o processamento e proteção de dados pessoais.

- Do mesmo modo que a Constituição portuguesa define os direitos básicos de um cidadão em relação ao seu voto, também o Parlamento Europeu os define para toda a União Europeia, na Diretiva sobre Eleições para o Parlamento Europeu[European Union, 1993].

- A Lei Europeia de Resiliência Cibernética[2] (CRA) é uma lei que foi proposta em setembro de 2022, que poderá entrar em vigor no futuro próximo. Esta lei é explorada na próxima secção.

Todos estes pontos terão de ser tidos em conta na criação do eVoto com modelo de negócio SaaS, para garantir que continuam a ser cumpridos.

4.0.1 Lei Europeia de Resiliência Cibernética (CRA)

Proposta em setembro de 2022, a CRA [Comissão Europeia, 2022] é um regulamento sobre requisitos de cibersegurança para produtos com elementos digitais, ou seja, produtos incluídos na *Internet of Things*[3] *(IoT)*, e será a primeira no mundo a fazê-lo. Abrange qualquer produto com elementos digitais.

A CRA indica que a cibercriminalidade tem "um custo anual global estimado (...) de 5.5 biliões de EUR até 2021". Os produtos-alvo destes ataques sofrem de certos problemas de segurança, tais como "vulnerabilidades generalizadas" e atualizações de segurança insuficientes e pouco frequentes, assim como "um entendimento e um acesso deficientes dos utilizadores à informação". Ou seja, que a informação sobre as propriedades de cibersegurança e sobre como utilizar devidamente um dado produto não são fáceis de encontrar, algo que a CRA visa resolver e regular.

Isto resulta em lacunas de segurança que enfraquecem "toda uma organização ou toda a cadeia de abastecimento" - devido à natureza destes produtos, estas falhas de segurança podem facilmente atravessar fronteiras "numa questão de minutos", o que significa que estes ataques são especialmente nocivos.

Tendo em conta que "a maioria dos produtos de hardware a software não está atualmente abrangida por nenhuma legislação da UE que aborde a sua cibersegurança", a CRA torna-se uma lei mais do que necessária, de modo a proteger os cidadãos da União Europeia.

Sendo uma empresa tecnológica, a Eurotux poderá ser afetada por esta lei. O objetivo desta secção é de investigar quais os produtos desenvolvidos pela empresa, tais como o eVoto, que poderão ver o seu

[2] Em inglês, European Cyber Resilience Act.

[3] Internet das Coisas.

desenvolvimento afetado caso esta lei entre em vigor.

Objetivos e Produtos Afetados

A CRA define dois objetivos principais para "assegurar o bom funcionamento do mercado interno", que seguem:

1. Criar condições para o desenvolvimento de produtos com elementos digitais seguros
2. Criar condições que permitam aos utilizadores ter em conta a cibersegurança aquando da seleção e da utilização de produtos com elementos digitais

São definidos quatro objetivos específicos:

1. Assegurar que os fabricantes melhorem a segurança dos produtos com elementos digitais
2. Assegurar um quadro de cibersegurança coerente
3. Aumentar a transparência das propriedades de segurança dos produtos com elementos digitais
4. Permitir que as empresas e os consumidores utilizem produtos com elementos digitais de forma segura

Ao longo do documento, é frequentemente salientado que só será possível atingir um nível superior de cibersegurança na UE com o trabalho conjunto de todos os seus estados-membros, para evitar fragmentação da lei e diferentes níveis de padrões de cibersegurança (que abrem as portas à exploração de vulnerabilidades, que facilmente atravessam fronteiras). Por isso, uma grande parte da CRA consiste em definir regras que facilitem a criação, distribuição, e manutenção de produtos com elementos digitais, de modo a garantir uma adesão mais rápida por parte de todos os estados-membros europeus.

A CRA aplica-se a qualquer tipo de produto com software, exceto "produtos abertos e em open-source, exceto [se o produto] for usado para processar remotamente os dados gerados por um produto de hardware vendido no mercado europeu"[4]. Define algumas regras para os criadores dos produtos[5]:

- Obriga a ter a funcionalidade de "call home"[6] e de atualizações frequentes de segurança.
- Obriga a fornecer suporte do produto durante pelo menos 5 anos

[4] https://www.cyberresilienceact.eu/cra-guide-for-software-developers/ (úlimo acesso em 09-10-2024)

[5] Eclipse Foundation: https://www.youtube.com/watch?v=AmsM5_5QO5A (úlimo acesso em 21-07-2023)

[6] Esta funcionalidade permite aos produtos comunicar com a "casa"(empresa criadora) para serem, por exemplo, atualizados.

- Restringe a publicação de software não terminado com o intuito de testes
- Obriga a documentar o desenvolvimento completo, a implementação, e a manutenção dos processos para cada projeto.
- Define vários níveis de criticidade de software. A maioria dos produtos (90%) poderá ser verificado pela própria empresa, enquanto que os restantes 10% terão de ser alvo de auditorias externas.

No entanto, levanta-se a questão de como este regulamento afetará os projetos open-source, especialmente os amadores ou sem fins lucrativos. O regulamento menciona que "o software livre e de código-fonte aberto desenvolvido ou fornecido à margem do exercício de uma atividade comercial não deve ser abrangido pelo presente regulamento". Segundo Eclipse Foundation [2023], "atividade comercial"significa que o projeto:

- É lançado regularmente
- É de qualidade comercial
- Tem como objetivo ser utilizado para comércio

Podemos então concluir que estes pontos abrangem praticamente todos os projetos open-source. Só não são abrangidos projetos amadores e caridades. Esta abrangência é propositada, pois o conselho europeu não tem como alvo apenas projetos proprietários, mas também quer regular projetos open-source. O não cumprimento das normas definidas no regulamento implicará uma multa de 15M € ou, se for uma empresa, até 2.5% do volume total anual do negócio - conforme o que for de maior valor.

Atualmente, o risco de que as contribuições em código aberto possam incorrer em responsabilidade para a empresa que as publica é baixo. No entanto, a CRA vai alterar essa relação de modo fundamental e, como resultado, as empresas europeias poderão começar a restringir as suas colaborações em código aberto, possivelmente até parar de as fazer. Isto pode ser extremamente prejudicial para a "economia de inovação"na Europa [7].

Levanta-se também a questão de que esta restrição sobre código aberto pode até ser contrário a algumas estratégias europeias, como por exemplo [Eclipse Foundation, 2023]:

- Soberania digital - Consiste em países e organizações europeias terem a capacidade de tomar decisões sobre os seus dados, tecnologia e infraestrutura digital sem serem demasiado dependentes de entidades não europeias.

[7] Eclipse Foundation: https://www.youtube.com/watch?v=AmsM5_5QO5A (úlimo acesso em 21-07-2023)

- GAIA-X - Iniciativa para desenvolver uma infraestrutura de dados segura e federada para a Europa.
- Catena-X - Ecossistema de dados aberto e colaborativo para a indústria auto-motiva.
- Dataspaces - Sistema de programação direcionado a sistemas atuais de grande escala e projetado para apoiar padrões dinâmicos de interação e coordenação entre aplicações científicas.
- Digital twins - Uma representação digital de um objeto físico, pessoa ou processo, contextualizado numa versão digital do seu ambiente. Por exemplo, modelos em tempo real de aviões, satélites, e sondas planetárias e aquáticas.
- Industrie 4.0 - A quarta revolução industrial, caracterizada pela integração de tecnologias digitais nos processos de indústria e produção.

Níveis de Criticidade

Tal como mencionado anteriormente, a CRA define vários níveis de criticidade, conforme a área e o propósito do produto de software. Todos os tipos de produtos mencionados pela CRA, e as suas classes, estão descritos no anexo D. Existem também regras que todos os utilizadores deverão seguir, descritas no anexo C.

Esclarecimentos após FOSDEM 2024

Durante a FOSDEM 2024[8], um evento para partilha de conhecimento entre *developers* realizada em Bruxelas, participei numa palestra entitulada "The Regulators are Coming: One Year On". Esta palestra teve como objetivo esclarecer dúvidas acerca da CRA e da Diretiva de Responsabilidade do Produto[9] (PLD).

A palestra foi dada pelos próprios autores da CRA, e permitiu esclarecer muitas das dúvidas que a investigação inicial levantou:

- **O que é que a CRA implica relativamente à responsabilidade de quem encontra vulnerabilidades?** A CRA tenta diminuir a responsabilidade dos *developers*. Quem encontrar uma vulnerabilidade, deverá avisar o *developer* e, se tiver feito uma correção, deverá lha fornecer.
- **Quando é que podemos esperar que a CRA entre em efeito?** Está estimado que a CRA ficará terminada a meio de 2024, e dentro de 3 anos deverá entrar em efeito.

8 https://fosdem.org/2024/ (úlimo acesso em 20-04-2024)

9 Em inglês: Product Liability Directive.

- **Alguns developers do Debian, presentes na paltestra, estavam preocupados acerca dos utilizadores secundários**[10]**, apesar da Debian não ser "comercial".** Se o computador for vendido com o Debian, então sim, serão afetados pela CRA. A solução neste caso seria de fornecer a esses utilizadores secundários um documento acerca de como cumprir a CRA.

- **Um desenvolvedor perguntou o seguinte: O que é que faço, então, se alguém se oferecer para pagar pelo meu trabalho? O meu instinto é não o fazer.** A CRA não é para os *developers* pequenos, e tem como objetivo fazer com que os *developers* sejam mais explícitos sobre o que estão a fazer.

No anexo I encontra-se disponibilizado o power-point apresentado durante a palestra.

Como é que isto afeta a empresa?

Segundo a listagem de categorias de produto[11] da CRA, a Eurotux e Dipcode desenvolvem produtos nas seguintes categorias[12]:

- Classe I: 1.
- Classe II: 5-11, 13.

Dado que a empresa desenvolve produtos incluídos nestas categorias, terão de ser tomados passos para uma transição rápida e fluída, na eventualidade da proposta CRA ser aceite.

Especificamente em relação ao eVoto, dado ser um produto puramente SaaS, não será afetado por esta lei. Existe a seguinte passagem do regulamento[Comissão Europeia, 2022]:

> *"Não regulamenta serviços, como o software como serviço (software-as-a-service – SaaS), com exceção das soluções de tratamento remoto de dados relativas a produtos com elementos digitais, entendidas como qualquer tratamento de dados à distância para o qual o software tenha sido concebido e desenvolvido pelo fabricante dos produtos em causa ou sob a sua responsabilidade e* **cuja inexistência impediria os produtos com elementos digitais de desempenhar uma das suas funções**."

[10] "Downstream users".

[11] Ver D.

[12] Informação obtida após consultar responsáveis na Dipcode (*Senior Software Architect* Sandro Rodrigues) e na Eurotux (*Chief Technology Officer* Fernando Gomes)

Como fonte de informação adicional, existe também um novo website para a CRA[13]. Este website tem também a seguinte passagem (traduzida)[14]:

> *"Por outro lado, o software gratuito e de código aberto, bem como o software SaaS puro, não são visados pelo CRA, a menos que, para este último, sejam utilizados para processar remotamente os dados gerados por um produto de hardware vendido a retalho no mercado europeu."*

Como o eVoto será uma solução 100% SaaS, e não um produto com elementos de software (por exemplo, uma máquina de voto), conclui-se que não será afetado por esta lei.

[13] https://www.cyberresilienceact.eu/ (úlimo acesso em 09-10-2024)

[14] https://www.cyberresilienceact.eu/cra-guide-for-software-developers/ (úlimo acesso em 09-10-2024)

Capítulo 5

Benchmarking das soluções de voto online

Este capítulo é dedicado à análise e exploração de outras soluções de voto online existentes no mercado, como mencionado nos Objetivos (1.1).

Características	Soluções				
	Helios	**Belenios**	**NemoVote**	**nVotes**	**ElectionBuddy**
País de Origem	EUA	França	Alemanha	Espanha	Canadá
Código aberto	✓	✓	✗	✗	✗
Acesso gratuito[a]	✓	✓	✗	✗	✓
Recursos de segurança[b]	✓	✓	✓	✓	✓
Integração com software de terceiros[c]	✗	✓	✗	?	✓
Relatórios e análises em tempo real	✓	✓	✓	✓	✓
Lembretes e notificações automáticas	✓	✓	✗	✓	✓
Verificabilidade do voto	✓	✓	✗	✓	✓

[a] Por oferta da primeira subscrição, pela existência de uma Demo, pela opção de um modelo de subscrição grátis, ou pelo produto em si não ter custo associado.

[b] Por exemplo, criptografia ou *multiple-factor authentication.*

[c] Se permite exportar os dados para, por exemplo, um ficheiro .csv.

Tabela 2: Comparação de software de votação eletrónica online com modelo de negócios SaaS

5.0.1 Helios

Informação básica

O Helios Voting é um sistema de votação online open-source baseado na web. No sistema do Helios Voting, qualquer pessoa pode votar, mas para que o voto seja contado a identidade do eleitor deve ser verificada, uma vez que a solução utiliza encriptação homomórfica[1] para garantir o sigilo do boletim de voto.

O Helios Voting foi criado em 2008 e é atualmente liderado por Ben Adida, em conjunto com vários contribuidores de código, e também vários consultores.

O Helios não tem modelo de subscrição, pois é de acesso gratuito.

Análise

Informação sobre o Helios pode ser consultada na documentação[2] e no repositório do github[3].

O Helios utiliza um serviço de integração contínua chamado Travis CI (Continuous Integration). "Integração Contínua"significa fazer pequenas alterações no software com frequência, em vez de esperar até o final de um ciclo de desenvolvimento para aplicar grandes alterações, o que permite testar e resolver problemas antes que se tornem demasiado complexos. Sendo uma plataforma de integração contínua, o Travis CI automatiza a implementação e teste de mudanças ao código, dando também feedback.

Relativamente às tecnologias utilizadas no desenvolvimento do Helios, consta-se que a maioria do código escrito é em Python 3, utilizando a framework Django 1.9. Também é utilizado Javascript com JQuery.

Naturalmente, sendo um sistema em modelo SaaS, o Helios tem também código HTML para a criação das suas páginas web. O Helios faz uso do Mustache, uma *template language* que permite gerar código HTML dinâmico.

Algumas caraterísticas sobre como os dados são tratados no Helios:

- A transmissão de dados entre o browser do utilizador e os servidores do Helios utiliza SSL[4].
- Segundo a documentação do helios, "o voto individual nunca é desencriptado". Os votos encriptados são combinados numa contagem usando o tipo de encriptação previamente falado (encriptação

[1] Forma de encriptação que permite realizar operações sobre os dados encriptados sem antes os desencriptar.

[2] Helios: https://documentation.heliosvoting.org/verification-specs/helios-v4 (úlimo acesso em 05-05-2023)

[3] Helios: https://github.com/benadida/helios-server (úlimo acesso em 05-05-2023)

[4] Secure Sockets Layer, protocolo de segurança ente um web browser e um web server.

homomórfica) e "apenas a contagem final - nunca uma contagem intermédia - é desencriptada"[5].

- Uma das caraterísticas do Helios é que permite a obtenção de dados com um simples pedido HTTP GET, tais como: a lista de eleitores, o último boletim lançado, o resultado de uma eleição, e a lista dos *trustees* de uma dada eleição.

- Outra caraterística é que todos os dados fornecidos pelo Helios são em formato JSON[6]. Todas as chaves relativas a estes dados são apresentadas por ordem alfabética e sem espaços em branco desnecessários, para garantir que o *hashing* de estruturas de dados cria sempre a mesma *hash*.

Utilização

Esta secção contém notas relevantes acerca da utilização do Helios, de um ponto de vista do utilizador.

- Só é permitido fazer o login através do Google ou do Github.

- Uma eleição é composta por questões, eleitores, boletins de voto, e administradores. O administrador padrão é o Helios Bot, e a autenticação de administradores funciona à base de chaves públicas e chaves privadas, geradas pelo Helios.

- Depois da criação de uma eleição, é possível enviar um email a todos os eleitores. O corpo do email é customizável, sendo que o resto é gerado automaticamente e contém o URL da eleição e os dados de autenticação do eleitor em questão. A password é enviada em texto simples.

- No final, após o lançamento do boletim de voto, o eleitor recebe um email a informar que o seu voto foi submetido com sucesso.

Conclusões

Um dos pontos fortes do Helios é a segurança. A encriptação homomórfica, previamente falada, é especialmente indicada para sistemas de votação uma vez que permite que o voto seja contado sem quebrar a privacidade do eleitor.

Outro ponto positivo do Helios é o simples facto de ser um serviço open source. É uma solução capaz de realizar eleições dos mais variados tipos, sem a necessidade de integração com serviços externos, tais como serviço de envio de emails em massa, ou um servidor onde a eleição esteja *hosted*.

[5] Helios: https://documentation.heliosvoting.org/verification-specs/helios-v4 (úlimo acesso em 05-05-2023)

[6] JavaScript Object Notation.

Outra vantagem relacionada com a sua natureza open-source é a da transparência. A plataforma ser baseada em código aberto significa que há uma camada extra de proteção sobre o serviço, dado que o código-fonte é mantido e observado por toda uma comunidade de *developers*, onde conhecimento sobre fraquezas e outros pontos fracos são detetados e rapidamente resolvidos.

Apesar do seu aspeto arcaico, o Helios é uma plataforma de votação de fácil utilização. Existem alguns pontos onde a *interface* pode tornar-se confusa, nomeadamente nas áreas restritas ao administrador, mas estes pontos são escassos e apenas são problemáticos numa primeira abordagem.

5.0.2 Belenios

Informação básica

Belenios é um sistema de votação online cujo objetivo é ser fácil de usar, garantindo a segurança do utilizador, e a privacidade do voto. Pode ser utilizado em vários tipos de eleições e referendos, desde conselhos científicos a associações desportivas.

O Belenios foi criado em 2012 por uma pequena equipa, sendo o developer principal Stéphane Glondu, com dois consultores, Véronique Courtier e Pierrick Gaudry.

O Belenios não possui modelo de subscrição, pois é de acesso gratuito.

Análise

Informação sobre o Belenios pode ser consultada na documentação[7] e no repositório Gitlab[8].

O Belenios foi construído parcialmente a partir do Helios. Mais especificamente, a partir do protocolo Helios-C. o Helios-C é um protocolo de construção de software que assegura correção de voto completa a um custo reduzido[Cortier et al., 2013].

Nos protocolos do tipo Helios, o quadro de avisos *(bulletin board)* é a única entidade responsável pelo controlo do direito de voto, sendo possível adicionar facilmente boletins de voto ao sistema. No Helios, esta falha de segurança não é relevante uma vez que a lista de eleitores é conhecida, e qualquer discrepância seria facilmente detetada.

Para garantir o controlo adequado do quadro de avisos em eleições onde não deve ser conhecido quem votou, é necessário considerar uma autoridade adicional. Cortier et al. [2013] propõe fornecer a cada eleitor uma chave privada que possui uma parte pública.

O conjunto de todas as credenciais públicas é público e, especialmente, conhecido pelo quadro de

7 Belenios: https://www.belenios.org/documentation.html (úlimo acesso em 07-05-2023)

8 Belenios: https://gitlab.inria.fr/belenios/belenios (úlimo acesso em 07-05-2023)

avisos. Assim, cada eleitor simplesmente assina o seu boletim com a sua credencial privada. É importante ressaltar que a associação entre uma credencial pública e a identidade do eleitor correspondente não precisa ser conhecida, nem deve ser divulgada, a fim de preservar o anonimato do eleitor e o sigilo do voto.

Relativamente às tecnologias utilizadas para o desenvolvimento, segundo a informação indicada pelo Gitlab, o Belenios é escrito em OCaml (com algumas dependências a bibliotecas de partes externas) e Python, com uma pequena parte em Javascript e CSS, como era expectável de uma aplicação web. O motor de base de dados é fornecido por uma biblioteca baseada em C chamada SQLite. A documentação nota ainda que enquanto que há suporte para Linux, em Windows o suporte é limitado.

Utilização

Esta secção contém notas relevantes acerca da utilização do Belenios, de um ponto de vista do utilizador.

- Autenticação de eleitores com dois fatores: credenciais e senhas.
- Para o envio de credenciais aos eleitores, a escolha é entre um servidor externo, ou um servidor do Belenios, que o próprio Belenios não recomenda.
- Pode ser atribuído peso a eleitores específicos através da estrutura do arquivo .csv.
- Uma eleição é composta por questões, eleitores, boletins de voto, e administradores. Cada administrador possui uma chave própria, e a eleição só poderá dar início após a validação de todas as chaves administrativas.
- Para submissão do voto, o utilizador deve inserir um código recebido por email depois de responder à última questão.
- É possível fazer a exportação dos resultados em formato JSON para tratamento de dados e integração com programas externos.

Conclusões

Podemos concluir que o Belenios é uma ferramenta eficaz na sua função, e uma melhoria significante em relação ao Helios. No entanto, não se considera que está completamente apto para uso numa eleição, especialmente uma de natureza governamental - em particular, a necessidade de utilizar servidores externos de modo a garantir uma comunicação mais segura é talvez a sua maior falha.

Mesmo assim, o Belenios consegue ser uma opção sólida no mundo de software de voto online. A fraca segurança dos servidores padrão só é relevante para eleições onde é expectável existirem ataques de cibersegurança, como eleições governamentais, ou para entidades de maior porte (por exemplo, universidades, empresas, sindicatos, etc). Para uso mais simples, contido, e comum - como, por exemplo, para decidir o representante de uma turma escolar - é mais do que suficiente.

5.0.3 NemoVote

Informação básica

Nemovote disponibiliza soluções de voto para eleições e eventos e consiste num conjunto de produtos, como o Nemocloud (sistema de voto baseado na nuvem) e o Nemobox (sistema de voto offline).

O NemoVote foi criado em 2018 e o seu CEO e cofundador é o Dr. Jannis Beger. Foi fundado também por Marco Hämmerle, engenheiro de software.

Plano	**Preço (EUR)**	**Caraterísticas**
Evento Único	59€ 29.90€(não ao vivo)	Todas as caraterísticas de voto básicas Acesso dedicado único ao NemoVote Cloud para o horário do evento Acesso ao NemoVote três dias antes e depois do evento
Subscrição	19€/mês ou 206€/ano 9.50€/mês ou 103€/ano (não ao vivo)	Todas as caraterísticas de voto básicas Acesso permanente ao NemoVote Retenção de Dados Substituição de todos os logótipos do NemoVote pelos do cliente e escolha de cores personalizadas

Tabela 3: NemoVote - Modelo de Subscrição

Análise

Devido à sua natureza de código fechado, não é possível analisar a tecnologia utilizada no NemoVote. No entanto, podemos obter alguma informação interna a partir da secção Perguntas Frequentes e, também, de diversos documentos tais como a Política de Privacidade.

Como recursos de segurança[9] o NemoVote utiliza, por exemplo, encriptação SSL e votação gerida/auto-gerida que "cumpre leis de privacidade da Alemanha e da União Europeia"[10]. Na sua Política de Privacidade, é indicado que os "votos transmitidos são imediatamente transferidos para a base de dados"[11]. Detalha também qual a informação que é processada, o tempo que permanece em memória, e o procedimento a seguir caso o utilizador pretenda eliminar os seus dados da plataforma.

Relativamente à infraestrutura, esta é hospedada por Heroku e pela Amazon AWS, *cloud providers* com as seguintes certificações: ISO/IEC 27001, 27017, e 27018[12]. Indica também que cada cliente recebe "a sua própria instância logicamente fechada do NemoVote", sendo que todos os dados transmitidos são encriptados com HTTPS, e os dados em repouso são encriptados com o *standard* AES-256.

Utilização

Para testar a utilização, recorreu-se à Live Demo disponível, com as credenciais fornecidas pelo NemoVote especialmente para esse propósito.

Esta secção contém notas relevantes acerca da utilização do NemoVote, de um ponto de vista do utilizador.

- A usabilidade é excelente, tanto no painel administrativo quanto para os eleitores, sendo comparável ao Google Forms.
- Os eleitores não têm a possibilidade de verificar se os seus votos foram contados corretamente.
- Não é possível enviar um e-mail customizado aos eleitores, a comunicação é feita apenas a partir do próprio sistema. É possível, no entanto, enviar dois tipos de mensagens:
  - A cada eleitor, um email (com corpo parcialmente customizável) com as suas credenciais;
  - Uma mensagem personalizada, enviada apenas a todos os utilizadores ativos no momento do envio. É bastante limitada, sendo igual a uma notificação que poderia facilmente ser ignorada.
- O sistema funciona com base em listas de eleitores, permitindo características diferentes a cada uma, como, por exemplo, o peso atribuído a cada voto de cada eleitor pertencente a uma dada lista.

[9] Estas caraterísticas e processos foram criados com cooperação com a empresa alemã ThinkSecure.

[10] NemoVote: https://nemovote.com/knowledge-base (úlimo acesso em 07-05-2023)

[11] NemoVote: https://nemovote.com/privacy/Privacy_Policy_Webpage.pdf (úlimo acesso em 07-05-2023)

[12] NemoVote: https://nemovote.com/security (úlimo acesso em 07-05-2023)

- Não há funcionalidade de *trustees* nem de definição de administradores adicionais.
- É possível exportar as informações principais de uma eleição para pdf, mas não existe maneira de exportar os resultados nem lista de eleitores para um ficheiro .csv ou outro que permitisse análise por parte de uma ferramenta externa.
- O eleitor e o seu voto podem ser secretos, no entanto, é possível criar uma eleição onde o administrador terá acesso a não só quem votou, mas também qual foi o seu voto. Esta mudança não é percetível ao eleitor e só está disponível a utilizadores com permissões de administrador.

Conclusões

O NemoVote é uma ferramenta de utilização fácil e intuitiva, ainda que com opções de comunicação bastante limitadas. Isto, com as soluções de segurança explicadas anteriormente, resultam num produto eficaz e confiável para o utilizador comum.

No entanto, uma das suas limitações mais significativas é a impossibilidade dos eleitores verificarem se os seus votos foram contabilizados corretamente, o que significa que o NemoVote não possui verificabilidade de voto, ao contrário de outras opções menos sofisticadas como o Helios e o Belenios.

Outra limitação está relacionada com a falta de *trustees*, o que prejudica a integridade de todo o processo de votação, uma vez que uma única entidade é responsável por todas as caraterísticas e passos da eleição.

Apesar de oferecer uma solução sólida para a realização de eleições, dependendo dos requisitos específicos do processo de votação que um dado cliente pretenda, poderá ser necessário procurar alternativas. Tal como o Belenios, o NemoVote parece mais indicado para um tipo de uso mais comum e de baixo risco.

5.0.4 nVotes

Informação básica

nVotes é uma plataforma de votação online que pretende fornecer um sistema de votação que, para o eleitor, é simples e fácil de utilizar, enquanto que para o administrador, é fácil e de confiança, e que "não causa dores de cabeça".

O nVotes foi desenvolvido por uma equipa de especialistas em diversas áreas, nomeadamente: Eduardo Robles, formado em engenharia das ciências de computação na Universidad de Sevilla; David Ru-

escas, formado em física no Imperial College of London; e Lucas Cervera, formado em administração empresarial na Universidad Complutense de Madrid.

Plano	Preço	Caraterísticas
Prime	Por contacto	Todas as caraterísticas de voto básicas Sem dias de antecedência necessários para um contrato assinado Infraestrutura partilhada Sem manutenção de infraestrutura
Enterprise	Por contacto	Todas as caraterísticas de voto básicas 30 dias de antecedência necessários para um contrato assinado Possibilidade de obter um orçamento para caraterísticas de voto avançadas Infraestrutura dedicada 2 meses de manutenção de infraestrutura

Tabela 4: nVotes - Modelo de Subscrição

Análise

O nVotes é software de código fechado, pelo que não é possível analisar a tecnologia utilizada internamente para o seu desenvolvimento e implementação, embora seja possível obter alguma informação acerca dos seus processos e metodologias internas.

A verificabilidade de voto é uma caraterística central do nVotes, especificando que um eleitor poderá verificar que[13]:

1. A sua escolha foi codificada corretamente no boletim pelo sistema;
2. O seu boletim foi recebido da maneira que o enviou;
3. O seu boletim foi registado e conta para o voto.

Inclusive, o nVotes mantém os boletins de voto "verdadeiramente secretos", onde o voto não identifica de modo algum o eleitor, e que é removida "qualquer ligação entre o voto e o eleitor", onde "nem os administradores do sistema de voto (...) podem violar esta privacidade".

[13] nVotes: https://nvotes.com/security/ (úlimo acesso em 07-05-2023)

Utilização

O nVotes não oferece opções sem custo associado (quer seja um oferta de uma subscrição, quer seja a existência de uma versão de teste/demo), logo toda a informação contida nesta secção é referente ao vídeo de demonstração[14] e, por isso, os pontos a seguir devem ser considerados com alguma reserva[15].

- Algo atípico acerca do nVotes é a necessidade de criar uma eleição de teste antes de uma real, sendo que esta última é sempre criada a partir da primeira, e apenas depois da eleição teste ter sido completada.

- São enviados emails para os eleitores a cada passo importante do processo (envio de credenciais, abertura e fecho da eleição, entre outros), cujo corpo não é personalizável.

- Apesar de não ser demonstrado no vídeo, existe uma secção em cada eleição referente às autoridades (os *trustees*). No entanto, não é possível ter a certeza acerca se é possível personalizar este campo e adicionar autoridades, ou não.

- Também não é possível discernir se o utilizador é capaz de exportar os dados da eleição para um ficheiro.

Conclusões

Não foi possível discernir muita informação relevante acerca do nVotes. Um ponto a retirar da sua análise é que a existência de, pelo menos, uma versão para demo do eVoto seria algo importante para a atração de clientes, pois permitiria ao potencial cliente experimentar a ferramenta e ter as suas dúvidas respondidas.

No caso do nVotes, embora pareça uma plataforma competente, a impossibilidade de experimentar o produto antes de se comprometer com uma subscrição pode ser um obstáculo para clientes de menor escala. Estes clientes têm menos recursos para subscrever a um serviço dessa natureza apenas para realizar testes e, possivelmente, descartar a opção ao final do período inicial de subscrição.

No entanto, este fator não é relevante para clientes de média e grande escala, que serão os clientes com mais capacidades para não só realizar uma subscrição inicial, como de manter essa subscrição durante um período de tempo maior.

Não oferecer uma primeira subscrição grátis impediria entidades de aceder e utilizar o eVoto para, por exemplo, uma única eleição, e depois não renovar a subscrição para o modelo pago.

[14] nVotes: https://www.youtube.com/watch?v=eTZ3TQw5G_c (úlimo acesso em 07-05-2023)

[15] O nVotes apenas oferece planos adaptados a empresas e outras entidades, não tendo uma opção para particulares.

A melhor solução seria, então, oferecer uma eleição demo não aplicável no mundo real, do mesmo modo que o NemoVote oferece uma demo ao vivo, para impedir situações como o nVotes - onde o cliente apenas tem acesso à informação limitada, e um vídeo de demonstração não muito detalhado.

5.0.5 ElectionBuddy

Informação básica

O ElectionBuddy foi criado em 2017 e é uma solução de voto online com foco em todo o tipo de votos, desde eleições até questionários durante conferências. Carateriza-se especialmente pelo alto nível de personalização que é possível aplicar às votações.

Tem por grupo-alvo desde entidades de escala muito pequena (por exemplo, eleições para diretor de turma) até de grande escala, incluindo organizações governamentais.

Plano	Preço (USD)	Caraterísticas
Free	$0	Até 20 Eleitores
Plus	$29	Até 350 Eleitores
Premium	$99	Até 1,000 Eleitores
Professional	>$299	Até 100,000 Eleitores

Tabela 5: ElectionBuddy - Modelo de Subscrição

Análise

Uma vez que o ElectionBuddy é um software de código fechado, não é possível realizar uma análise direta da sua tecnologia, mas podemos obter informações através da sua página de caraterísticas[16].

Em termos de acessibilidade, é possível votar em qualquer tipo de dispositivo, seja em formato *mobile* ou *desktop*, incluindo a partir de software de videoconferência, tais como Google Meet, Microsoft Teams e Zoom. Também permite que os eleitores enviem *feedback* diretamente do boletim.

Já para a segurança, indica que "as chaves de voto pessoais são criadas e usadas uma única vez utilizando encriptação de 256-bit", permitindo também autenticação de dois fatores ou confirmação por telemóvel. Adiciona que todos os votos eleitorais são "confidenciais e não podem ser ligados ao eleitor"e, também, que os resultados podem ser escondidos até o final da eleição como medida extra de anonimato.

[16] ElectionBuddy: https://electionbuddy.com/features/ (úlimo acesso em 12-05-2023)

Quanto à verificabilidade de voto, indica que os boletins e os resultados "são observáveis e auditáveis para verificar que os votos foram corretamente lançados".

Utilização

Esta secção contém notas relevantes acerca da utilização do ElectionBuddy, de um ponto de vista do utilizador.

- O ElectionBuddy faz a distinção entre voto online remoto (por exemplo, a partir de casa) e voto online presencial (por exemplo, audiência de conferências).
- Permite personalizar várias caraterísticas de segurança:

  Nível de segurança da eleição Link pessoal com chave de acesso pessoal, link genérico com chaves de acesso pessoal, e link genérico sem chave de acesso.

  Anonimato do voto Par eleitor-voto secreto, apenas visível a administradores, ou a administradores e outros eleitores.

  Acesso aos resultados Apenas o administrador tem acesso, permite definir se estão disponíveis durante ou apenas depois da eleição. Os resultados só são enviados aos eleitores de forma manual.

- O boletim é personalizável: logótipo organizacional, descrição, instruções, adicionar imagens e descrição a cada opção de resposta, voto em branco, entre outros.
- Tem disponível uma série de métodos de autenticação, incluindo: email, 2FA[17], envio de carta, envio por SMS.
- Permite exportar os resultados para .csv, .xls, ou texto simples.
- Para a verificabilidade de voto, o eleitor só pode verificar se o seu voto não foi alterado apenas quando os resultados forem enviados para os eleitores, procurando pela sua chave na listagem de chaves dos votos submetidos.

Conclusões

O ElectionBuddy é um serviço eficiente, flexível e altamente personalizável, uma caraterística muito atraente para potenciais clientes. O eVoto pode beneficiar da incorporação de recursos semelhantes, impulsionados por algumas destas características.

[17] Autenticação de 2 fatores.

Capítulo 6

Análise do eVotUM

À semelhança da análise de cada uma das soluções concorrentes, nesta secção será também analisado o eVotUM de modo a contextualizar o leitor na sua construção atual, tendo como objetivo obter conclusões acerca da reestruturação para modelo SaaS na forma do eVoto.

Como auxílio para esta secção, foi realizada uma reunião com o *Senior Software Developer* Sandro Rodrigues. As notas tiradas durante esta reunião estão disponíveis em E.

Informação Básica

O eVotUM foi criado em 2017, construído em consórcio pela Eurotux, o Centro de Computação Gráfica e a Devise Futures para a Universidade do Minho. Tem como público-alvo entidades de grande dimensão, incluindo organizações governamentais.

É software de código aberto, pelo que com a equipa e as ferramentas certas, pode ser implementado por qualquer entidade.

Análise

Nesta secção é apresentada uma tabela semelhante à tabela utilizada para as soluções concorrentes (5) aplicada ao eVotUM[1].

Serão também analisadas não só as tecnologias utilizadas no desenvolvimento e implementação do eVotUM, como também as suas caraterísticas, tais como a verificabilidade do voto e a auditabilidade do produto.

[1] Note-se que os concorrentes analisados são modelo SaaS, ao contrário do eVotUM.

Características	eVotUM
País de Origem	Portugal
Código aberto	✓
Acesso gratuito	✓
Recursos de segurança[a]	✓
Integração com software de terceiros[b]	✗
Relatórios e análises em tempo real	✓
Lembretes e notificações automáticas	✓
Verificabilidade do voto	✓

[a] Por exemplo, criptografia ou *multiple-factor authentication*.

[b] Se permite exportar os dados para, por exemplo, um ficheiro .csv.

Tabela 6: Caraterísticas do eVotUM.

O eVotUM (e, por consequência, o eVoto) ser software de código aberto representa uma mais-valia para a comunidade informática, como partilha de conhecimento e tecnologia. Dos concorrentes analisados, os com mais sucesso apresentam ser de código fechado (ElectionBuddy 5.0.5, nVotes 5.0.4 e NemoVote 5.0.3). Dado o eVotUM estar ao abrigo da licença GPL v3, não é possível restringir o acesso ao código do eVoto - ser código aberto é imutável.

Um ponto a melhorar para a implementação do eVoto seria a integração com software de terceiros. Atualmente, o eVoto não permite a exportação dos dados para qualquer tipo de ficheiro. Dois dos concorrentes analisados (ElectionBuddy 5.0.5 e Belenios 5.0.2) apresentam esta funcionalidade, pelo que seria interessante adotá-la para o eVoto.

Para um utilizador de uma ferramenta de voto online, poder exportar os dados estatísticos ou quantitativos das suas eleições pode ser uma grande mais-valia. Para o eVoto, esta é uma funcionalidade especialmente atrativa, dado que poucos concorrentes a oferecem - e quando o fazem, é bastante limitada.

Segundo o Guia do Eleitor[Universidade do Minho, 2017], as caraterísticas do eVotUM são as seguintes:

1. Autenticidade - Apenas pessoas autorizadas podem votar;
2. Unicidade - Voto único por eleitor;
3. Anonimato - Não é possível fazer a associação eleitor-voto;

4. Integridade - O voto não pode ser destruído ou modificado;
5. Irrevelável - O eleitor não pode revelar o seu voto;
6. Verificabilidade - É possível verificar que a contagem dos votos foi corretamente executada de modo independente.
7. Auditabilidade - É possível uma entidade independente testar e auditar o eVotUM.
8. Mobilidade - Voto em qualquer lugar.
9. Transparência - O sistema é "claro, exato, preciso e seguro".
10. Disponibilidade - Está sempre disponível durante o período de votação.
11. Deteção e Recuperação - O sistema "deteta erros, falhas e ataques e, recupera a informação até ao ponto de falha."

Estas caraterísticas são comuns ao software de voto online, tal como observado na secção 5, pelo que não devem ser ignoradas. Será importante salientar estas caraterísticas ao utilizador final do eVoto, através do website.

O guia oferece também instruções sobre como utilizar a plataforma, indicando como aceder, verificar o caderno eleitoral, votar e verificar a contagem do voto. Também indica como contactar a administração eleitoral e como alterar a informação guardada na plataforma: os dados de contacto e os dados de mudança de chave de segurança - os dados pessoais não são alteráveis uma vez que estão vinculados ao sistema da Universidade do Minho.

A página de Perguntas Frequentes[Universidade do Minho, 2023] do eVotUM fornece também algumas informações em relação à estrutura da plataforma:

- Tipos de eleições suportados:
    1. Eleição com limite de escolhas assinaláveis;
    2. Eleição *Write-in*[2];
    3. Eleição por votação ordenada/com ordem de preferência;
    4. Eleição por método de Hondt[3] ou método proporcional;

[2] Permitir a escolha de um candidato que não apareça no boletim de voto, embora que restrito aos nomes carregados pela Comissão Eleitoral.

[3] Versão utilizada nas eleições para a Assembleia da República Portuguesa; ver https://www.cne.pt/content/metodo-de-hondt (úlimo acesso em 09-10-2024).

- Intervenientes no sistema:

    1. Responsável Institucional - Responsável pela configuração dos processos eleitorais[4].
    2. Comissão Eleitoral - Gere o processo eleitoral e as respetivas eleições.
    3. Eleitor - O eleitor é a entidade com permissões para votar, e que detém acesso à área privada do eVotUM.
    4. Público - O público não tem acesso à área privada do eVotUM e, como tal, não possui permissão para votar. Consegue, no entanto, consultar as páginas públicas do eVotUM, tais como as páginas informativas, a consulta de processos eleitorais, e a verificação de cadernos eleitorais, podendo apresentar reclamações em caso de algum erro ser detetado.
    5. Administrador Técnico - Responsável pela monitorização, manutenção e suporte técnicos, pela elaboração de páginas estáticas do website, e pelo carregamento de chaves e certificados digitais no sistema.

- O voto é encriptado no browser do eleitor antes de ser colocado na urna digital e, segundo Universidade do Minho [2023], o voto "só pode ser decifrado no final da eleição"através da chave de desencriptação da Comissão Eleitoral.

- Quando os votos são contados e os resultados são lançados, é gerada uma lista de referências, onde cada referência corresponde a um voto da eleição em questão. Para verificar se o seu voto foi devidamente contado, o eleitor apenas tem de procurar nessa lista a sua referência de voto, que recebeu por email e que pode também consultar na plataforma.

O eVotUM está ao abrigo da GPLv3, o que significa que qualquer pessoa pode utilizar, estudar, modificar, e/ou redistribuir o programa (com ou sem custo associado, desde que o código seja aberto). Também fornece proteção contra patentes que possam limitar o uso do programa, além de obrigar a que qualquer cópia do programa tenha de estar ao abrigo da mesma licença [GNU, 2023]. Esta é uma das razões pela qual o eVoto será também de código aberto.

Sendo uma solução de código aberto, podemos analisar as tecnologias utilizadas no eVotUM de forma direta.

O projeto é composto por vários módulos:

Webapp (Módulo principal) Sistema de voto.

[4] Esta entidade é nomeada pelo reitor da Universidade do Minho.

Anonymizer Service Garante o voto anónimo e a impossibilidade de identificar eleitores através do voto, e vice-versa.

Counter Service Decifra e conta os votos.

Cripto-js Distribuição do código javascript do projeto Cripto[5].

Cripto-py Distribuição do código python do projeto Cripto.

O eVoto é construído quase inteiramente em Python, com a framework Django. O arranque do projeto é feito com Docker e utilizando Docker Compose, para um desenvolvimento prático e fácil.

Atualmente, o eVotUM é estruturado da seguinte maneira:

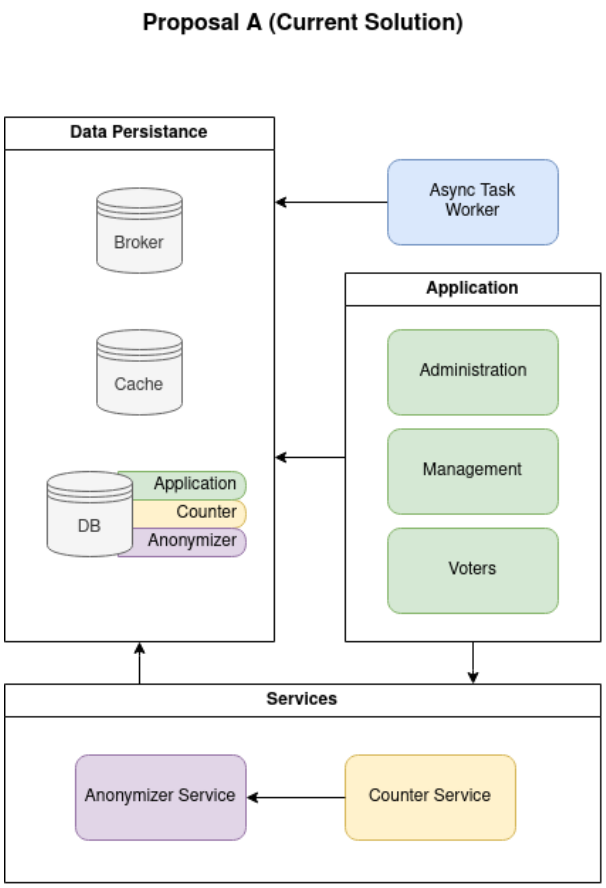


Figura 9: Arquitetura atual do eVotUM.

A solução atual consiste num único sistema single-tenant, que é dedicado a todos os utilizadores, sendo todos os componentes do sistema são partilhados. Esta solução não foi pensada para servir o

[5] Mais do que uma biblioteca, o projeto Cripto é toda uma framework para encriptação e desencriptação, entre outras functionalidades.

número de utilizadores simultâneos que a transição para SaaS irá gerar, dado que o eVoto será fornecido a vários clientes; o eVotUM serve apenas a Universidade do Minho, os seus estudantes e *alumni*.

Este tipo de arquitetura é vantajoso na medida em que, para um número relativamente baixo de utilizadores, a plataforma funciona como esperado - com o benefício de que é mais simples de montar, gerir, e manter do que outros tipos de arquitetura[6].

Caso a arquitetura atual do eVotUM fosse mantida para o eVoto, com o aumento do número de utilizadores e de clientes irão surgir vários aspetos negativos:

1. Riscos de segurança: vulnerabilidades afetam todos os utilizadores em simultâneo;
2. Competição por recursos: um grande número de utilizadores simultâneos causa lentidão na resposta da aplicação - o que resulta num serviço com desempenho inconsistente e pouco fiável;
3. Personalização limitada: como o eVoto está projetado para servir vários clientes, personalização é imprescindível. Isto inclui necessidades de espaço e de performance requeridas por certos clientes;
4. Desafios de escalabilidade: escalar bases de dados mantendo a consistência e a integridade dos dados é uma tarefa complexa quando estes componentes são partilhados por todos os utilizadores;
5. Conformidade com regulamentos: infraestrutura partilhada por múltiplos clientes significa que será mais difícil assegurar que os regulamentos europeus relevantes são respeitados;
6. Equidade no pagamento: uma plataforma à base de subscrições como o eVoto terá, inevitavelmente, vários clientes com vários tipos de subscrições. Assegurar que cada cliente tem a qualidade do serviço pela qual paga é mais complicado num sistema partilhado, com competição por recursos, que pode diminuir esta qualidade;
7. *Downtime*: qualquer atualização ou manutenção da infraestrutura causará uma interrupção para todos os clientes de modo simultâneo;

Para transformar o eVoto numa plataforma SaaS, estes problemas têm de ser mitigados.

Utilização

Existe uma versão de teste do eVotUM, tendo sido essa a utilizada para obter a informação nesta secção.

- O eVotUM está estruturado em processos eleitorais, e cada processo eleitoral tem um painel de eleições.

[6] Para uma análise detalhada de vários tipos de arquiteturas, é favor referir à secção 2.1.3.

- Tanto o processo eleitoral como as votações contidas no seu painel de eleições são traduzíveis para inglês, em campos preenchidos pelo administrador do processo.

- Cada tipo de eleição pode ainda permitir (ou não) eleitores com pesos de voto diferentes.

- Um detalhe a notar é que, para utilizadores administrativos com um grande leque de processos eleitorais a eles atribuídos, seria útil a implementação de um campo de pesquisa por texto livre.

- Cada processo eleitoral precisa da definição de várias datas: apresentação de listas candidatas, caderno eleitoral provisório e definitivo e o período de reclamação para tal[7], período de votação, data de publicação de resultados e, finalmente, o período de homologação destes.

- Cada processo eleitoral tem também uma secção dedicada à configuração de níveis de segurança das suas ações. Estas ações incluem: publicação de documentos, início da contagem de votos, início e fecho da votação da eleição, entre outros. Quanto mais forte o nível de segurança, mais restrita é a autorização necessária para a executar (por exemplo, maior número de chaves).

Foram criados dois diagramas que ilustram a mudança de estados de um processo eleitoral (apêndice G) e de uma eleição (apêndice H) em relação às ações manuais ou automáticas realizadas na plataforma.

Conclusões

Existem algumas caraterísticas do eVotUM que devem ser salientadas:

- A plataforma permite definir datas para cada um dos passos do processo eleitoral. Isto é algo que não é oferecido pelos concorrentes e, por isso, é uma mais-valia;

- Associado ao ponto anterior, a definição de datas dos vários passos do processo eleitoral é necessária, mas extensa. É do interesse do eVoto que o processo eleitoral seja sucinto e fácil de criar, pelo que seria interessante implementar uma alternativa a este passo, de modo a manter a funcionalidade, mas oferecer outra opção ao cliente que não necessite dela;

- O eVotUM tem também uma funcionalidade de definição de permissões de utilizador, o que torna todo o processo muito mais profissional e seguro, pois permite separar responsabilidades;

- O modo de *login* está associado aos serviços de autenticação da Universidade do Minho, o que significa que o eVoto terá de implementar um sistema de autenticação diferente;

[7] Por exemplo, um eleitor deve efetuar uma reclamação durante este período caso deva estar no caderno eleitoral, mas não se encontre nele.

- Uma outra funcionalidade existente é a da consulta pública dos votos. Tal como o ponto anterior, este serviço é dependente dos serviços da Universidade do Minho, pelo que a sua implementação vai implicar uma reestruturação desde a raiz. Esta funcionalidade pode ou não ser um ponto positivo para o eVoto, dado que, para a esmagadora maioria das entidades que vão realizar votos com a plataforma, não é do seu interesse a votação ser pública.

Através das conclusões da análise do eVotUM, definem-se algumas das funcionalidades e caraterísticas que devem ser implementadas no eVoto:

- O modo de login terá de ser alterado;
- Poderão ser implementados alternativas a certos passos do processo eleitoral para simplificar eleições;
- Aliado ao ponto anterior, é importante dar prioridade a uma experiência de navegação da plataforma simples e intuitiva. Seria interessante a implementação de funcionalidades de pesquisa livre e pesquisa avançada, possibilitar a criação de grupos de processos eleitorais, e talvez algum modo de etiquetagem ou classificação de processos eleitorais. Estas caraterísticas estão aliadas ao ponto sobre acessibilidade, na análise da certificação ISO/TS 54001:2019, na secção 3.6;
- A arquitetura do eVoto terá necessariamente de ser diferente à do eVotUM, para conseguir responder às necessidades de desempenho de um produto SaaS (ver 2.1).

Estas conclusões serão consideradas no planeamento de alterações funcionais(7.1) e arquiteturais (7.2) para o eVoto.

Capítulo 7

Alterações para a comercialização do eVoto

Neste capítulo serão apresentadas as alterações sugeridas para a comercialização do eVoto, tal como mencionado nos Objetivos (1.1). Primeiramente, serão apresentadas as alterações funcionais, abrangendo a linguagem e a tecnologia utilizada, assim como também as ferramentas de desenvolvimento de código, e também as alterações para o website que terá visibilidade pública. Será também apresentado o roadmap de alterações, assim como também os desenvolvimentos atuais sobre o website público.

De seguida, serão apresentadas as alterações de arquitetura necessárias, desde o tipo da arquitetura, como também algumas sugestões acerca da comercialização do eVoto, relacionadas com a arquitetura da solução.

Finalmente, será feita uma análise de riscos associados com a transição do eVotUM para o eVoto, em modelo SaaS.

7.1 Alterações Funcionais

Nesta secção são apresentadas as alterações funcionais sugeridas, desde a linguagem e a tecnologia que são utilizadas, as ferramentas de desenvolvimento de código, e também alterações para o desenvolvimento do site. É também apresentado o roadmap de alterações funcionais, assim como os desenvolvimentos já em progresso, relativos ao site de apresentação do eVoto.

7.1.1 Linguagem e tecnologias

Uma vez que a Dipcode trabalha com linguagens (Python e PHP) já bem estabelecidas no corpo laboral e no mercado, não será possível propor algo diferente (ver 2.1.4). Para tal, seria necessário despender tempo em formações, para além de que estariam a ser introduzidas potenciais falhas na segurança dado que a tecnologia a introduzir poderia não ser familiar à equipa.

Assim, as ferramentas base do eVoto deverão ser Python (Django) com a utilização do Docker para o *deployment*. Deve ser seguida a estrutura de ferramentas com a qual a equipa já está familiarizada. Isto irá poupar tempo de aprendizagem, e permitir que um produto superior seja criado.

7.1.2 Ferramentas

Após reuniões internas foi decidido que o eVoto teria duas "frentes": um site aberto ao público que teria a informação básica acerca do eVoto e também a loja/modelos de subscrição; e um site aberto apenas para clientes que subscreveram a uma das modalidades de pagamento.

A recomendação será a criação do site público em WordPress ou em Django, sendo que têm caraterísticas diferentes:

- WordPress
  - \+ modular, adição e remoção de plugins/caraterísticas/ferramentas muito facilitada;
  - \+ permite fazer alterações ao site sem ser necessário aceder ao código, o que significa que membros menos técnicos da empresa serão capazes de realizar manutenção e resolução de problemas, libertando tempo para a equipa de desenvolvimento;
  - \+ a Dipcode já detém muita experiência com WordPress, o que irá agilizar todo o processo;
  - \- devido à sua natureza *low-code*, significa que quaisquer alterações feitas em ambientes de desenvolvimento ou produção através da interface do site terão de ser replicadas manualmente no outro ambiente; isto pode levar a diferenças significativas entre os ambientes,

que podem afetar o teste de código para, por exemplo, uma nova *feature* - apresentando resultados diferentes conforme o ambiente onde está a ser testado.

- Django
  - **+** o Python é muito modular, e o acesso à abundância de bibliotecas e novas funcionalidades criadas pela comunidade open-source é uma grande mais-valia;
  - **+** o Python tem à sua disponibilidade uma miríade de bibliotecas focadas em *Machine Learning* e em Inteligência Artificial, que poderão ser vertentes interessantes para explorar;
  - **-** As caraterísticas do site só poderão ser alteradas através de código. De momento, está a ser investigada a utilização da *framework* Wagtail, que permitirá um maior nível de customização de páginas *à la* WordPress - no entanto, a sua utilização está em fase de investigação. Não é, também, tão poderosa e complexa como o WordPress.

Como o eVoto não é para um cliente externo, mas sim para ser gerido pela empresa, recomenda-se a utilização do Django. Irá perder-se a utilização *low-code* típica do WordPress[1], mas irá ganhar-se a escalabilidade e flexibilidade que o Python e o Django oferecem.

7.1.3 Funcionamento e Website

Existem várias recomendações em relação ao funcionamento da plataforma em si:

1. Eleições simples 6: atualmente, as eleições são processos complexos que incluem, mas não só: a definição do processo eleitoral, a definição de datas de início, conclusão e abertura de vários passos do processo eleitoral, entre outros. Nem todos os clientes-alvo do eVoto terão a necessidade de ter votações tão complexas e rígidas - assim, seria uma mais-valia a implementação de uma nova modalidade de eleições, as eleições simples. As eleições simples podem ser also tão simples como a definição dos candidatos, a definição do grupo de votantes, e um botão de abertura e conclusão das urnas;

2. Demo grátis 5.0.4: a oferta de uma demo grátis, ou de um modelo de subscrição mais barato (mas também mais limitado) será uma boa estratégia a adotar para atrair e reter potenciais clientes. Poder experimentar o produto antes de se comprometer a pagar o valor mensal/anual é uma das estratégias de atração e retenção de clientes que existe no mercado atualmente, e é praticado por muitos dos competidores (ver 5);

[1] Que se torna ainda menos relevante considerando que o eVoto é um produto interno à empresa.

3. Modo de login alterado 6: tal como mencionado na secção em referência, o modo de login terá de ser alterado do eVotUM para o eVoto, não só porque a Universidade do Minho deixará de ser o único cliente, mas também porque estaremos a lidar com clientes internacionais e/ou não governamentais que precisarão de um login mais estandardizado;

4. Exportação dos dados para um ficheiro: atualmente, o eVotUM não permite a exportação dos dados das eleições para um ficheiro ou para uma aplicação de terceiros; a adição desta funcionalidade ajudaria a reter clientes, pois dar-lhes-ia a oportunidade de utilizar os dados, gerados pelo eVoto, para as suas próprias ferramentas já existentes. Esta exportação de ficheiros é também uma caraterística oferecida por alguns dos concorrentes.

5. Implementação de funcionalidades extra: pesquisa livre, pesquisa avançada, e etiquetagem/classificação de processos eleitorais.

6. Acessibilidade F: a acessibilidade é, mais do que nunca, uma caraterística crucial à utilização de apps e websites, pelo que deverão ser tomadas iniciativas para assegurar a utilização do eVoto pelos utilizadores com dispositivos alternativos, modos de navegação não visuais, e também devem ser implementados modos de visualização de, por exemplo, alto contraste, ou letras maiores.

7. Listagem de caraterísticas e marketing 3.7: para o site aberto ao público, mencionado na secção anterior, será necessária uma tabela de comparação de subscrições e, também, uma listagem de caixas, cada uma com uma caraterística ou funcionalidade do eVoto.

7.1.4 Roadmap de Alterações

O seguinte roadmap foi fornecido pela *Senior Project Manager* Andreia Félix, e foi realizado para uma candidatura aos projetos de I&DT[2] do eVoto.[3]

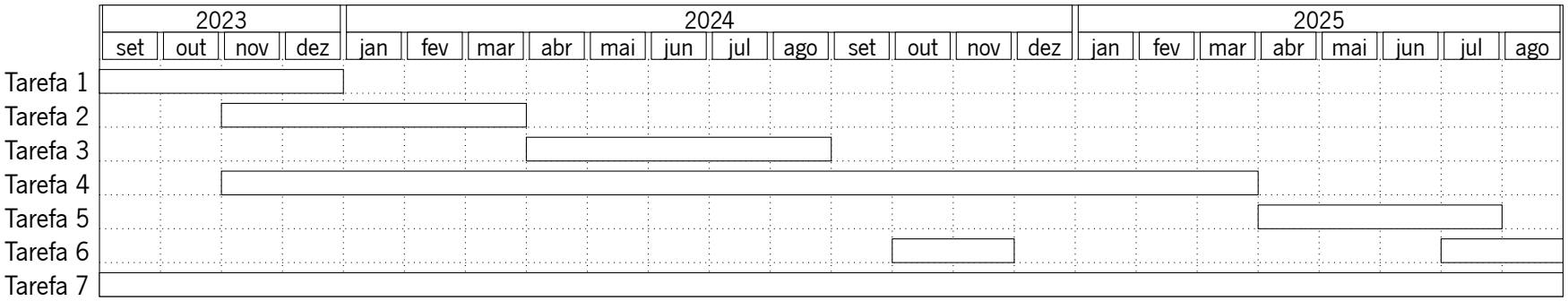


Figura 10: Planeamento do projeto eVoto, à data 27/06/2024.

Legenda das tarefas:

1. Vigilância Tecnológica
2. Definição de arquitetura tecnológica e funcional
3. Implementação da infraestrutura e Cloud
4. Desenvolvimento do protótipo
5. Testes em ambiente real e simulado
6. Promoção e divulgação dos resultados
7. Gestão de projeto

[2] https://eportugal.gov.pt/servicos/submeter-a-candidatura-aos-projetos-de-i-dt-em-copromocao-i-dt- (úlimo acesso em 09-10-2024)

[3] Devido à necessidade urgente deste roadmap para o envio da candidatura I&DT, a empresa criou-o antes que eu pudesse fazê-lo. Assim, ele é fornecido aqui apenas como uma base para a subsecção a seguir, onde será expandido e onde são sugeridas algumas alterações.

7.1.5 Expansão e Alterações ao Roadmap

Nesta secção irão ser exploradas algumas das possíveis adições ao roadmap do projeto eVoto.

Uma das sugestões será a realização de demos da utilização do eVoto. Estas demos poderão ser internas ou externas à empresa, e terão como objetivo mostrar e dar a conhecer o estado atual do projeto.

Outra sugestão será a da comercialização e apresentação do eVoto em eventos tais como a FOSDEM[4]. Quer seja como palestrantes, quer seja numa mesa, seria importante dar a conhecer este produto num mercado europeu, mercado este que é cada vez mais competitivo. A promessa de segurança é especialmente atrativa para audiências europeias, dado que a União Europeia tem apostado cada vez mais em regular a segurança do consumidor.

Outro evento onde seria uma mais-valia apresentar o eVoto seria a DjangoCon[5], já que é relevante em termos da tecnologia utilizada. De modo idêntico ao anteriormente dito, tem também a vantagem de que o eVoto estará a ser exposto a milhares de pessoas, em particular no contexto europeu.

Estas apresentações podem ser realizadas no âmbito da Tarefa 6 "Promoção e divulgação dos resultados", no entanto, poderão ter de acontecer durante um período não contemplado no roadmap, dado que ambas são convenções com datas fixas. Acredita-se que a visibilidade do projeto eVoto poderá ser aumentada, e interesse gerado, se a ferramenta for apresentada neste tipo de eventos, e que os investidores e clientes agregados irão mais do que compensar o investimento inicial necessário para participar nestas convenções.

7.1.6 Desenvolvimentos atuais

À data de 1 de julho de 2024, algumas das sugestões mencionadas na secção anterior foram já postas em prática - nomeadamente, as respetivas ao conteúdo e estrutura do site. Esta secção dedica-se a percorrer o site e explicar quais as alterações feitas, e algumas das decisões tomadas. O site foi implementado por mim e pelo Senior Software Developer Luís Silva (especificamente, com a sua orientação[6]), perante a aprovação do grupo de administradores e, também, do departamento comercial da empresa.

O website final apenas será aberto ao público quando a plataforma eVoto for lançada e comercializada - no entanto, é já possível analisar o trabalho realizado. O website tem como objetivo comercializar a solução eVoto, para que seja possível agregar clientes interessados nesta solução, assim como servir de

[4] Mencionada anteriormente neste documento, a FOSDEM é uma convenção anual de *developers*, em Bruxelas.

[5] A DjangoCon é uma convenção de developers dedicada à utilização da framework Django, para Python. Mais informações em https://2024.djangocon.eu/ (úlimo acesso em 09-10-2024).

[6] O papel do *developer* Luís Silva foi maioritariamente de aprovação e apoio; no entanto, o "esqueleto"inicial do site, assim como o estilo e a filosofia de design foram definidas por ele.

portal para agregação de feedback.

Página inicial

A página inicial contém várias secções. Enquanto que o estado inicial foi realizado pelo *developer* Luís Silva, foi alvo de reescrita por mim, com foco em tornar o site mais apelativo e colocar em maior evidência as caraterísticas do eVoto (como a segurança).

Figura 11: Header do site

No topo da página está o header. Salientam-se os seguintes elementos:

- Selecionador de linguagem: crucial para comercializar o eVoto para clientes no mundo;
- Menu de navegação com os três tipos de páginas: listagem de caraterísticas, mencionada na secção 3.7; uma secção sobre a empresa, crucial para gerar um sentimento de confiança pela parte de possíveis clientes; e uma secção sobre o funcionamento da plataforma eVoto.
- Botão "Contacte-nos": crucial para facilitar a comunicação cliente-empresa.

Figura 12: Banner introdutório.

O primeiro elemento que um visitante vê é um banner introdutório, cujo objetivo é captar e reter a atenção do cliente. Este banner indica, de modo imediato, quais são as caraterísticas mais fortes do eVoto, com especial foco na segurança. De um modo imediato, o cliente tem também a opção de pedir

uma demonstração - isto assegurará que não existem obstáculos ou atrasos entre a apresentação do site no ecrã do utilizador e a apresentação dos contactos.

Figura 13: Secção Sobre nós.

É para esta secção que aponta a opção "Sobre nós"do menu do header. Está logo após o banner introdutório, para que o cliente tenha conhecimento de quem está a desenvolver esta ferramenta, da história do eVoto, e também que o código é aberto, de modo imediato.

Figura 14: Listagem de funcionalidades.

De seguida encontra-se uma listagem detalhada das funcionalidades que o eVoto oferece. São mencionados os métodos de login disponíveis (ver 7.1 e 6); detalhes sobre o *backend* da plataforma (nomeadamente, o método de contagem de votos, extração de dados, e tipos de eleições); são, também, mencionadas certas funcionalidades disponíveis apenas para administradores, como, por exemplo, a dashboard de controlo dos processos eleitorais.

Figura 15: Garantias do eVoto.

A próxima secção, a secção de garantias oferecidas pelo eVoto, é talvez a mais importante, pelo que é também a mais apelativa: contém pouco texto, e o texto que contém é sucinto e comunica informação de um modo eficaz. Deste modo, é mostrado ao cliente todas as garantias oferecidas pelo eVoto, mas diminuindo o quanto possível o aborrecimento ou abandono do site.

Esta secção foi referenciada em 7.1 e também em 3.7.

Figura 16: Customização no eVoto.

De seguida, é apresentada a secção de customização do eVoto. Processos eleitorais e eleições estão cobertos de *branding* de marcas e de partidos, pelo que é crucial que o cliente final possa apresentar as suas eleições com a sua marca própria. Esta secção demonstra que opções de customização estão disponíveis aos utilizadores administradores, fixando a ideia de que o eVoto é, para além de seguro,

também flexível, adaptando-se às necessidades de cada cliente.

Figura 17: Banner Call to Action.

Sendo o eVoto um produto comercial, é crucial que sejam apresentadas ao cliente o maior número possível de oportunidades de adquirir o produto - mas não tantas que causem num afastamento. Este banner "Call to Action"serve como um leve lembrete de que o cliente está apenas a um passo de poder experimentar o eVoto.

Página das Caraterísticas

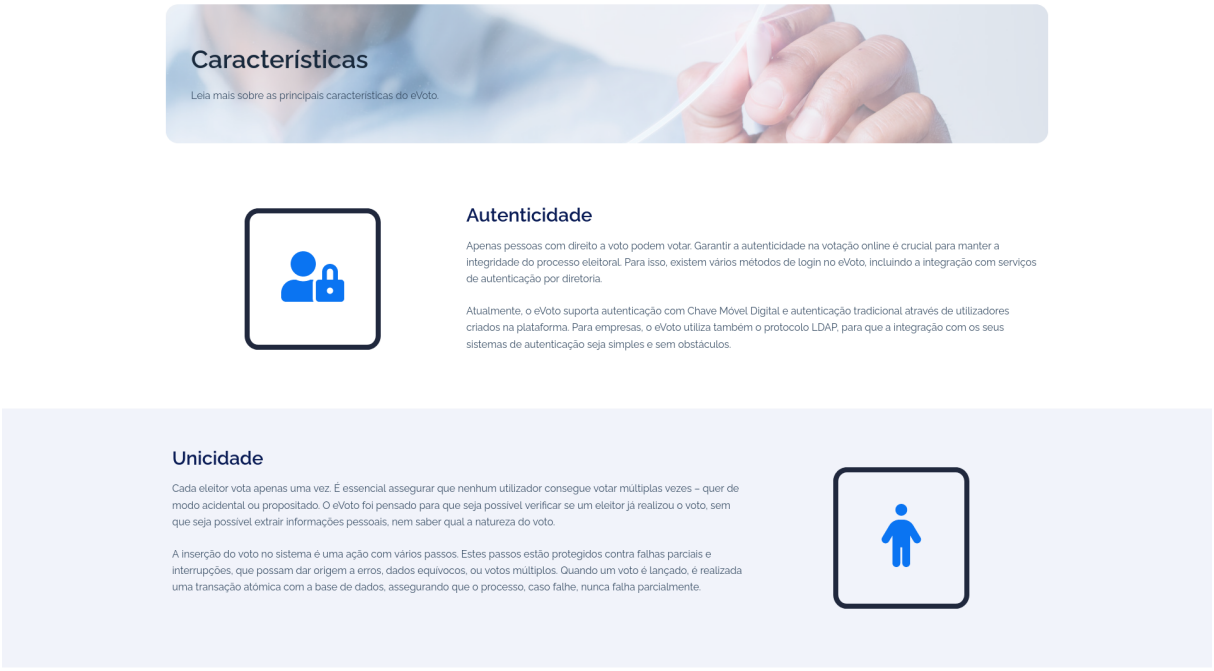


Figura 18: Página das Caraterísticas (incompleta).

Tal como mencionado no Header, existe uma página de Caraterísticas. Esta página foi sugerida e desenvolvida por mim, durante o desenvolvimento do site. Esta página é crucial para clientes que tenham interesse em saber mais sobre o eVoto, de um modo mais detalhado, o que tende a ser o caso de grandes empresas e outros grupos de grande dimensão (universidades, agrupamentos, entre outros).

Na sua totalidade, são apresentadas onze caraterísticas:

Autenticidade Apenas pessoas com direito a voto podem votar. Garantir a autenticidade na votação online é crucial para manter a integridade do processo eleitoral. Para isso, existem vários métodos de login no eVoto, incluindo a integração com serviços de autenticação por diretoria.

Atualmente, o eVoto suporta autenticação com Chave Móvel Digital e autenticação tradicional através de utilizadores criados na plataforma. Para empresas, o eVoto utiliza também o protocolo LDAP, para que a integração com os seus sistemas de autenticação seja simples e sem obstáculos.

Unicidade Cada eleitor vota apenas uma vez. É essencial assegurar que nenhum utilizador consegue votar múltiplas vezes – quer de modo acidental ou propositado. O eVoto foi pensado para que seja possível verificar se um eleitor já realizou o voto, sem que seja possível extrair informações pessoais, nem saber qual a natureza do voto.

A inserção do voto no sistema é uma ação com vários passos. Estes passos estão protegidos contra falhas parciais e interrupções, que possam dar origem a erros, dados equívocos, ou votos múltiplos. Quando um voto é lançado, é realizada uma transação atómica com a base de dados, assegurando que o processo, caso falhe, nunca falha parcialmente.

Anonimato Não é possível associar um voto a um eleitor, nem vice-versa. Uma das componentes principais do eVoto é o Anonimizador, responsável por garantir que o voto é anónimo, e assegurar a impossibilidade de identificar eleitores através do voto, e vice-versa. O voto é encriptado no próprio dispositivo do eleitor; deste modo, nunca é exposto desprotegido.

A encriptação dos dados sensíveis é feita através do mecanismo de autenticação de mensagens HMAC-SHA256. Este método consiste na geração de um código autenticador de mensagens (MAC) através da função hash criptográfica SHA256 em combinação com uma chave secreta. Qualquer tipo de MAC é utilizado para verificar a integridade e também a autenticidade de uma dada mensagem, sem relevar dados sensíveis.

Integridade Os votos não podem ser danificados ou destruídos. A integridade é um dos principais pilares do eVoto, dado que suporta todas as outras vertentes do sistema. A nossa plataforma implementa um sistema de logs compreensivo, onde apenas é possível acrescentar informação, e nunca retirar ou alterar quer o conteúdo, quer a ordenação das entradas.

Além disso, cada entrada utiliza o sistema HMAC-SHA256 para que seja possível verificar que as entradas anteriores não foram comprometidas. Deste modo, se um agente malicioso alterar, danificar, ou criar entradas, estas alterações serão facilmente detetadas, verificadas, e auditadas.

Irrevelável Nenhum eleitor pode provar qual o voto que efetuou. Todo o sistema eVoto foi criado para

suportar a irrevelabilidade dos dados sensíveis; desde o sistema criptográfico, que assegura a anonimidade e a unicidade dos votos e dos eleitores; até ao sistema de logs, que assegura a integridade e fiabilidade do sistema.

Apesar de conseguir verificar se o seu voto foi corretamente contado, o eleitor nunca tem acesso ao conteúdo dele. Esta separação de dados assegura que, mesmo se um eleitor for coagido a revelar o seu voto, nunca conseguirá provar qual o voto efetuado.

Verificabilidade É possível verificar de forma independente que todos os votos foram contados corretamente. O sistema eVoto foi preparado para que seja possível verificar a correta contagem de votos, sem nunca expôr quaisquer associações eleitor-voto, ou dados sensíveis, tais como dados pessoais de eleitores, ou o conteúdo de votos individuais.

Cada voto é encriptado, enviado, guardado e contabilizado de modo seguro, através de várias camadas de segurança, com métodos criptográficos atuais e universalmente comprovados.

Após o lançamento da cédula preenchida, o eleitor tem a possibilidade de verificar se o seu voto foi corretamente contado, sem ter acesso a dados identificativos ou à natureza do seu voto. O voto está, assim, protegido contra terceiros através da verificação da identidade do eleitor que lhe corresponde; e também está protegido contra o próprio eleitor (ou vice-versa).

Auditabilidade O sistema de votos pode ser testado e auditado por entidades independentes. Sendo open-source, todas as componentes do eVoto estão disponíveis para consulta pelo público. Além disso, o sistema de logs é resistente a alterações no conteúdo ou na ordem de cada entrada, assim como também permite a verificação da autenticidade de entradas anteriores.

Para além da exposição do código ao público em geral, são também feitas auditorias regulares ao Grupo Eurotux, para assegurar os padrões de segurança e conformidade com as certificações obtidas, nomeadamente, a certificação de sistemas ISO 9001 e a certificação de segurança de informação ISO 27001.

Mobilidade Um dos pilares do eVoto é a votação em qualquer lado. O voto online permite que os eleitores votem em qualquer local, utilizando os próprios dispositivos. A participação eleitoral aumenta, já que o voto não está dependente dos horários das mesas de voto, e torna-se muito mais acessível a qualquer eleitor – quer este tenha uma agenda ocupada, se encontre numa localização remota, ou que tenha dificuldades no deslocamento para a mesa de voto.

Quer vote no telemóvel no metro a caminho de casa, no tablet enquanto relaxa no sofá, ou no computador antes de iniciar o dia de trabalho – nós garantimos que cada voto é registado com

precisão e segurança.

Transparência Processos eleitorais claros, exatos, precisos e seguros, construídos a pensar tanto no eleitor, como no administrador. O nosso sistema permite uma vista geral de todos os processos eleitorais da sua empresa ou grupo.

Para uma total transparência, todos os processos internos estão explícitos no código fonte. Adicionalmente, cada eleitor tem a possibilidade de verificar a correta contabilização do seu voto, em apenas 3 cliques, num processo desenhado para ser simples e intuitivo.

Disponibilidade O eVoto está disponível durante todo o período de votação. Construído com uma infraestrutura robusta, o nosso sistema consegue lidar com grandes volumes de tráfego, e inclui mecanismos que reduzem a possibilidade de falhas. Deste modo, os eleitores podem aceder à plataforma com segurança, e votar a qualquer hora e em qualquer lugar.

Prioritizamos a disponibilidade para garantir um processo de votação confiável e prático. Com a infraestrutura gerida por nós, pode ter a certeza que os seus eleitores terão uma experiência de votação fluída e sem interrupções, independentemente do volume de tráfego.

Deteção e Recuperação Deteção de erros, falhas, e ataques, com recuperação da informação até ao ponto de falha. O nosso sistema está equipado com vários mecanismos de deteção de erros e recuperação de dados, para que não fique prejudicado na eventualidade de uma falha.

Prioritizamos a resiliência do nosso serviço para garantir que a experiência do utilizador é livre de obstáculos. Com os nossos mecanismos de deteção e recuperação, garantimos que os dados dos eleitores estão protegidos e que o seus processos eleitorais permanecem seguros e sem perdas.

Página Como Funciona

Esta página visa explicar qual o fluxo de utilização do eVoto, do ponto de vista do utilizador. Esta página foi também sugerida e desenvolvida por mim, e considera-se que a sua existência é especialmente relevante para o utilizador eleitor, e não tanto para o administrador. Este site será visitado também pelos eleitores, e é importante que exista uma secção que satisfaça alguma dúvida que tenham em relação à utilização do eVoto. É também importante para o cliente administrador, dado que poderá verificar como é estar do lado do eleitor.

Figura 19: Página "Como Funciona".

Página Contactos

Finalmente, existe também a página de contactos do site. Como o eVoto está em fase de desenvolvimento, e tal como mencionado no início deste capítulo, o objetivo do site é de agregar clientes para que exista apoio e feedback durante este processo de criação da plataforma. Assim, o único método de compra do eVoto será através do contacto direto com a empresa.

Esta necessidade de contacto e pedido de demonstração pode ser um fator que afaste clientes não tão investidos na ferramenta - pelo que será necessário criar uma página dedicada às subscrições, como mencionado na secção 7.1 ("Funcionamento e Website").

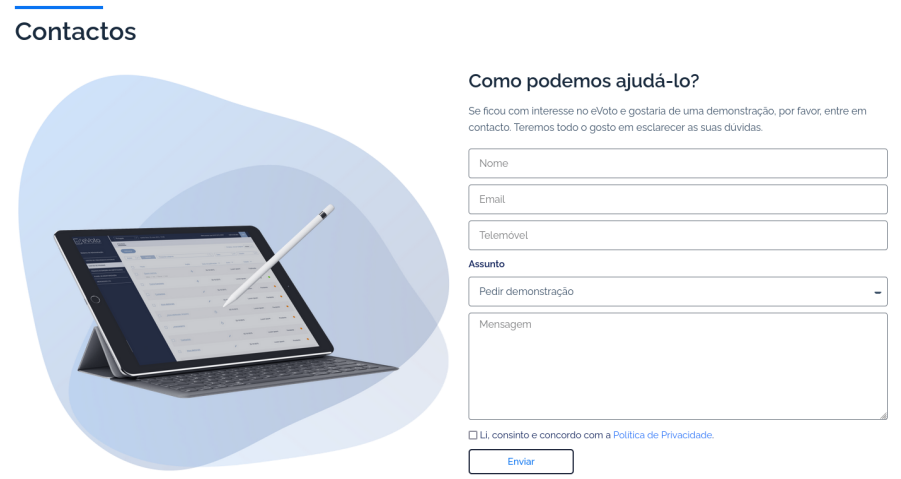


Figura 20: Página "Contactos".

7.2 Alterações da Arquitetura

Este capítulo consiste nas alterações de arquitetura propostas para o eVoto SaaS, tal como definido nos objetivos (ver 1.1).

7.2.1 Comparação de Tipos de Arquitetura

Para determinar qual a arquitetura mais acertada para o eVoto, foi realizada uma comparação utilizando as arquiteturas exploradas na secção 2.1.3 em conjunto com as caraterísticas exploradas na secção 6, e outros critérios relevantes.

A tabela compara as diferentes arquiteturas, segundo o nível de cada uma das caraterísticas. Estas caraterísticas foram escolhidas a partir da análise das necessidades comuns de software em modelo de negócio SaaS (ver 2.1). Cada uma das caraterísticas é determinada seguindo as seguintes questões:

Segurança: Quantos fatores de riscos estão inerentemente presentes neste tipo de arquitetura? Por exemplo: bases de dados partilhados, dificuldade em isolar e conter incidentes e falhas de segurança dos restantes utilizadores, partilha de serviços críticos, entre outros.

Competição por recursos: Que caraterísticas da arquitetura permitem mitigar a competição por recursos?

Personalização: Qual o grau de personalização da máquina por parte do cliente?

Escalabilidade: É possível escalar o sistema quando tal for necessário? Qual é a facilidade com que essa alteração pode ser feita?

Equidade no pagamento: O quão fácil é assegurar o tempo de resposta subscrito pelo utilizador, dado que outros utilizadores com planos mais exigentes podem estar a levar a competição por recursos?

Disponiblidade: Com que frequência é que um utilizador passa por *downtime*? Quantos utilizadores é que esse *downtime* afeta em comparação com toda a base de utilizadores?

Manutenção: O quão fácil é realizar a manutenção da instância? Qual a frequência necessária?

Por sua vez, cada uma das arquiteturas (descritas em detalhe na secção 2.1.3) pode ser resumida pelo seguinte:

- Single-Tenant: Cada *tenant* tem uma instância, infraestrutura, e base de dados dedicada.

- Multi-Tenant: Múltiplos *tenants* partilham instâncias da aplicação a diferentes graus:

    1. Tipo 1: Uma base de dados por *tenant*.
    2. Tipo 2: Base de dados partilhada.
    3. Tipo 3: Base de dados fragmentada.
    4. Tipo 4: Base de dados fragmentada, com fragmentos que podem servir um ou vários *tenants*.

Nesta tabela de comparação, as cores estão ordenadas do seguinte modo: vermelho (pior) < laranja < amarelo < verde < azul (melhor).

Caraterísticas	**Nível**				
	Single-Tenant	**M.T. 1**	**M.T. 2**	**M.T. 3**	**M.T. 4**
Segurança	Mais Alto	Alto	Mais Baixo	Baixo	Médio
Competição por Recursos	Mais Baixo	Baixo	Mais Alto	Alto	Médio
Personalização	Mais Alto	Alto	Mais Baixo	Baixo	Médio
Complexidade em Escalar	Alto	Mais Baixo	Mais Alto	Baixo	Médio
Equidade no pagamento	Mais Alto	Médio	Mais Baixo	Baixo	Alto
Tolerância a falhas[a]	Mais Alto	Alto	Mais Baixo	Baixo	Médio
Manutenção	Mais Alto	Médio	Mais Baixo	Baixo	Alto
Custo	Mais Alto	Médio	Mais Baixo	Alto	Baixo

Tabela 7: Comparação de tipos de arquiteturas: Single-Tenant e Multi-Tenant. As cores denotam a polaridade de cada caraterística.

[a] Quanto maior a percentagem de utilizadores que fica sem acesso à plataforma na eventualidade de uma queda algures no serviço, menor o nível de tolerância a falhas.

7.2.2 Arquiteturas Propostas

A arquitetura A é a arquitetura atual (figura 9) e é do tipo Single-tenant[7].

A possível necessidade de implementar uma arquitetura diferente para o eVoto foi discutida na secção 6 e, no seguimento de uma reunião interna, foram propostas várias arquiteturas com estruturas diferentes.

[7] Dado que o eVotUM foi feito especialmente para a Universidade do Minho, esta é o único *tenant*.

Arquitetura B

A arquitetura B é do tipo multi-tenant com base de dados fragmentada (tipo 3) verticalmente (por serviços). Este tipo de arquitetura permite que os dados dos vários serviços do eVoto (Application, Counter, e Anonymizer) estejam mais isolados - o que significa uma maior segurança e proteção de dados.

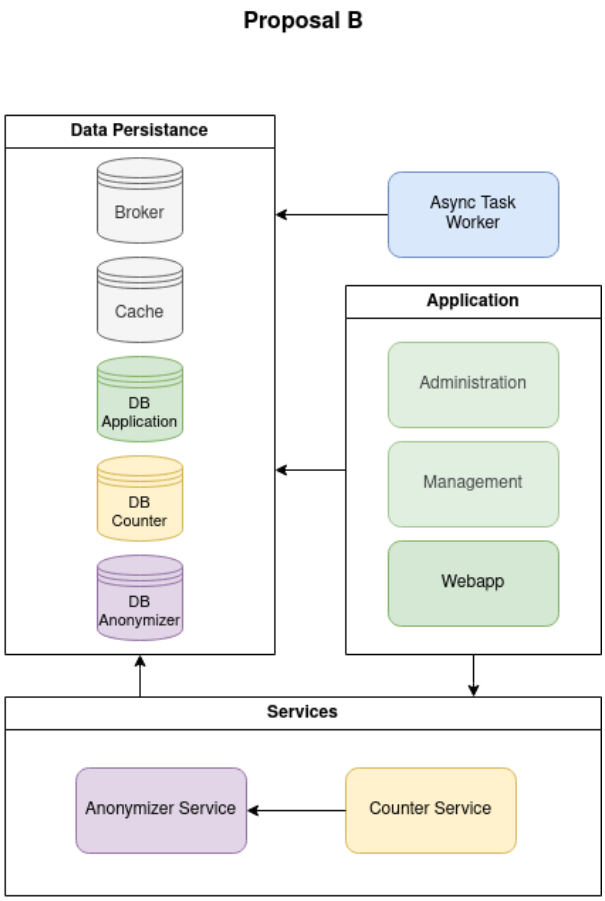


Figura 21: Arquitetura B - Multi-tenant com base de dados fragmentada verticalmente (tipo 3).

Fragmentar a base de dados significa também que os acessos a ela serão mais rápidos, resultando numa melhoria no tempo de resposta do serviço, algo imprescindível quando se trata de uma base de dados partilhada.

Esta solução tem a vantagem de que não é necessária muita reestruturação a nível dos blocos *Application* e *Services*, dado que a única diferença para o esquema atual (9) é a fragmentação da base de dados.

Arquitetura C

A arquitetura C é do tipo multi-tenant com base de dados fragmentada (tipo 3), à semelhança da arquitetura B - no entanto, é fragmentada tanto verticalmente (por serviços) como horizontalmente (por *tenants*).

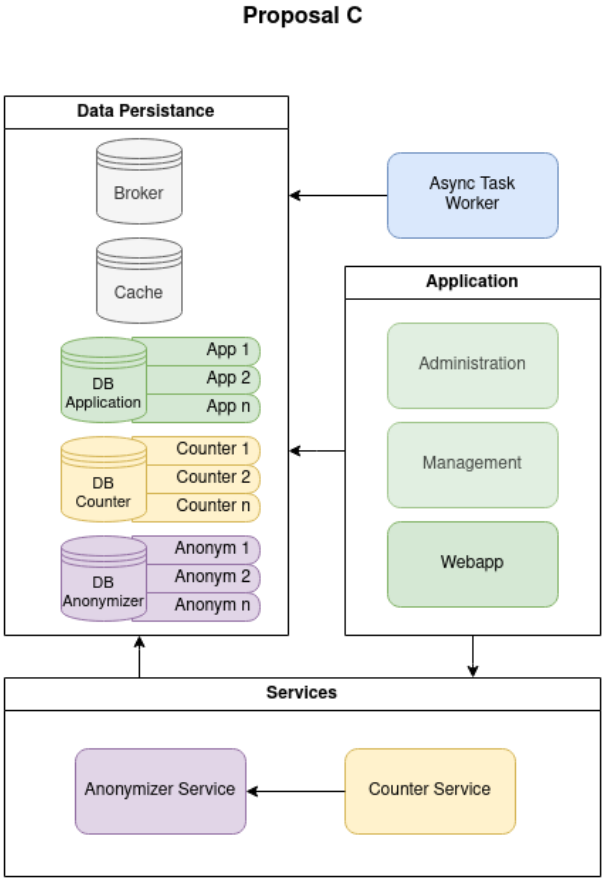


Figura 22: Arquitetura C - Multi-tenant com base de dados fragmentada vertical e horizontalmente (tipo 3).

À semelhança da arquitetura B, fragmentar a base de dados verticalmente permite diminuir o tempo de resposta do serviço, e garante um melhor isolamento de dados.

A fragmentação horizontal permite melhorar ainda mais os tempos de resposta, já que os dados de cada *tenant* irão ficar isolados dos restantes.

Arquitetura D

A arquitetura D é do tipo single-tenant. É, essencialmente, a mesma arquitetura que é atualmente utilizada no eVotUM (arquitetura A), sendo que várias instâncias serão criadas à medida que o número de clientes cresce.

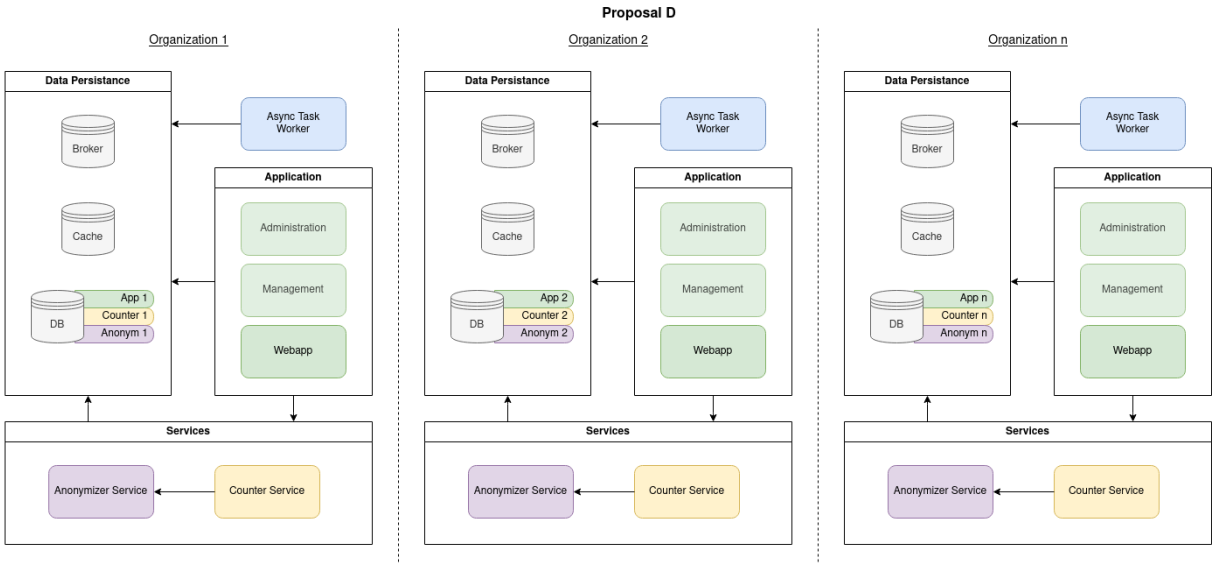


Figura 23: Arquitetura D - Múltiplos single-tenant.

O esquema acima detalha como se procederia à adaptação do serviço para vários *tenants* - com a criação de uma instância isolada para cada um.

Este tipo de arquitetura tem muitas vantagens, especialmente quando utilizado para um produto SaaS (tabela 7):

1. Ótimo isolamento de dados. Este facto permitirá que a proteção de dados seja mais facilmente assegurada;

2. Ótima personalização da plataforma. Cada *tenant* pode escolher as caraterísticas da sua instância (memória, tempo de resposta, etc), o que vai de encontro com a monetização por subscrições. O facto de que cada instância nova não interfere, de todo, com as preexistentes, significa que a criação (ou eliminação) de uma instância pode ser automatizada;

3. A competição por recursos é mantida no mínimo, já que os tempos de resposta não serão afetados por outros *tenants*. Assim, o cliente é assegurado que o serviço pelo qual paga, é o serviço que terá.

4. Apesar do custo de manutenção ser o maior de entre os tipos de arquiteturas exploradas, com a automatização da criação/eliminação de instâncias este problema é mitigado.

5. O processo descrito no ponto anterior também mitigará o custo total da plataforma, já que não será necessário alocar vários colaboradores para a criação e manutenção de instâncias - podendo ficar apenas uma pequena equipa de reserva para a manutenção e atualização do sistema automático, e para resolução de problemas que possam surgir ao longo da vida do eVoto.

7.2.3 Alterações Propostas

Após a análise dos diferentes tipos de arquiteturas (tabela 7), e da exploração dos diferentes esquemas apresentados na reunião interna (9, 21, 22, 23) podemos chegar à conclusão de que a Arquitetura D (múltiplo single-tenant) é a mais vantajosa para o modelo de negócio pretendido para o eVoto.

A arquitetura single-tenant pode apresentar um desafio na escalabilidade. O sistema terá de ser capaz de lidar com aumentos e diminuições bruscos do número de instâncias, e sustentar não só um elevado número de utilizadores simultâneos (como é caraterístico de um *Software-as-a-Service*), como também conseguir fornecer um serviço de qualidade quando está na capacidade máxima[8].

O tipo de arquitetura single-tenant apresenta não só o melhor rácio de vantagens-desvantagens quando comparado com as outras arquiteturas, como também apresenta a maior vantagem: a automatização da criação e eliminação de instâncias.

Como o eVoto irá seguir um modelo de monetização à base de subscrições com diferentes níveis, é instrumental garantir que o cliente final obtém o serviço pelo qual pagou - não só para causar uma boa impressão da marca da empresa e fornecer um serviço de qualidade, mas também para salvaguardar contra possíveis conflitos legais que seriam levantados caso o serviço fornecido não fosse de encontro com o serviço anunciado para a subscrição.

Esta automatização permite também globalizar o eVoto. Não sendo necessário um colaborador para criar uma instância, o cliente receberá o acesso ao serviço momentos após a subscrição, quer seja dentro ou fora do horário de trabalho da empresa. Observa-se o mesmo no caso contrário, onde cada cliente pode cancelar o seu serviço a qualquer hora, sem depender da empresa.

Aliada à segurança dos dados, esta flexibilidade na subscrição é imperativa para atrair clientes e oferecer o melhor serviço possível.

[8] Apesar do eVotUM (e, por consequência, o eVoto) ser um produto *open source*, a parte *server-side* do serviço não poderá ser explorada ou discutida aqui, por motivos de sigilo profissional.

7.3 Análise de Riscos

Esta secção pretende identificar e avaliar os potenciais ataques e ameaças à plataforma eVoto, primeiro de modo geral e, depois, com foco no voto online. Esta análise irá permitir identificar os riscos específicos e, assim, desenvolver estratégias de mitigação e controlo adequados, com o intuito de proteger a plataforma e garantir não só a segurança, como também a confiança dos utilizadores.

7.3.1 Ataques gerais

A tabela seguinte indica quais os métodos mais indicados para combater os diferentes tipos de ataques mais conhecidos.

Tipo de Ataque	**Estratégias de Mitigação**
Geral (precauções básicas)	Autenticação forte (p.e. de vários fatores) Criptografia de dados Cópias de segurança regulares Monitorização constante da rede Atualizações regulares do software
Manipulação de dados	Logs/registos auditáveis
Palavras-passe	Limites de palavras-passe falhadas Renovação de palavras-passe *Rate limits* no formulário de acesso
Man in the middle (rede comprometida e tráfego intercetado)	Usar comunicações encriptadas (com SSL)
Engenharia Social (p.e. *phishing*)	Treino da equipa Treino dos utilizadores

Tabela 8: Tipos de ataques a produtos de software.

Para além da informação apresentada na tabela, é também crucial que os administradores de serviços críticos procurem e investiguem, ativamente, vulnerabilidades do software. Seja a seguir jornais sobre cibersegurança e outros tipos de fontes de informação, seja a testar ou tentar comprometer o produto diretamente[9].

[9] Conhecido na indústria como "pentesting", ou penetration testing - um ataque a um sistema informático, conhecido e autorizado.

Estas estratégias de mitigação, e outras, são utilizadas pela empresa para proteger os seus produtos, clientes, parceiros, e colaboradores.

7.3.2 Ataques específicos a software de voto

Em 2003, o Conselho Europeu emitiu um documento[Council of Europe, 2003] com recomendações de segurança e práticas recomendadas para votação eletrónica, identificando vários riscos[10].

A seguinte matriz de risco apresenta os riscos classificados consoante a probabilidade e a gravidade de cada um. Os riscos apresentados foram agregados a partir de três fontes: o documento acima mencionado, uma análise interna à plataforma e à Empresa, e a lista dos 10 maiores riscos para aplicações web da OWASP[11][OWASP, 2021].

[10] É importante salientar que o documento em questão é um rascunho, e não fornece detalhes específicos sobre se a eleição eletrónica seria presencial ou não. Devido à data de publicação, considera-se que o intuito original é o de abranger votação eletrónica presencial, no entanto, as conclusões obtidas também se podem aplicar a votação eletrónica não presencial.

[11] OWASP: Projeto Aberto de Segurança em Aplicações Web.

		Gravidade				
		1 Negligenciável	2 Menor	3 Moderado	4 Maior	5 Catastrófico
Probabilidade	5 Muito Provável	5	10	15	20	25
			Acesso à plataforma por dispositivos infetados com malware	Ataques Denial of Service		
	4 Provável	4	8	12	16	20
				Falsificação de um eleitor elegível	Divulgação das listas eleitorais ou de candidatos a terceiros	Má configuração da plataforma
	3 Possível	3	6	9	12	15
		Perda de energia temporária nas instalações		Falsificação durante o registo de candidatos ou nomeações de candidatos	Falhas no sistema de criptografia	Acesso não autorizado Contorno de medidas de segurança
	2 Pouco provável	2	4	6	8	10
			Perda de disponibilidade dos boletins de voto	Perda de integridade dos boletins de voto Modificação ou destruição da lista de candidatos e listas eleitorais Perda irrecuperável de votos emitidos	Divulgação, modificação ou destruição dos dados na base de dados Perda de integridade ou disponibilidade de registos de auditoria Rastos de dados que permitem atribuir um voto único a um eleitor	Injeção (p.e. *Cross-site Scripting*)
	1 Muito pouco provável	1	2	3	4	5
				Emissão de múltiplos votos Erros no processo de contagem		Perda da capacidade de detetar ataques ou erros

Tabela 9: Matriz de risco de ataques a software de voto.

Os riscos apresentados na tabela anterior podem ser agregados em três grupos:

- Baixo Risco (1-6): Estes riscos são caraterizados por um baixo nível de gravidade e/ou uma baixa probabilidade de ocorrência. Entre estes, estão incluídos riscos que, por exemplo: não apresentam uma perda permanente de dados; não apresentam um risco direto à segurança do utilizador final; ou representem pontos de falha que são facilmente resolvidos através de sistemas redundantes. Um exemplo deste último, é o da falha de energia nas instalações, que é facilmente remediado através de um gerador.

- Risco Moderado (8-12): nesta categoria estão agregados riscos que, por exemplo: podem afetar o acesso à plataforma; onde o agente malicioso se faz passar por um eleitor/candidato; onde partes do sistema de votação falham (sejam eles o website, o componente de criptografia, o acesso pelos utilizadores, etc).

- Grande Risco (15-25): esta categoria está reservada para aqueles riscos que significam uma perda total de informação, a divulgação de dados privados, ou que permitam a um dado agente malicioso obter controlo sobre (ou afetar de modo significativo) a plataforma. Por exemplo, um agente malicioso conseguirá afetar o website através de ataques *Denial of Service*, que impediriam tanto potenciais clientes, como utilizadores atuais, de o utilizar. Um exemplo de uma invasão e obtenção de controlo sobre a plataforma, seria através de más configurações. Com cada vez mais produtos de software a evoluírem para serem "altamente configuráveis"[OWASP, 2021], este risco torna-se cada vez mais relevante. De facto, "90% das aplicações que foram testadas tinham algum tipo de má configuração."[OWASP, 2021]

7.3.3 Estratégias de proteção aliadas às tecnologias utilizadas no eVoto

Esta secção detalha os riscos associados às tecnologias que são utilizadas no eVoto. Devido à necessidade de sigilo empresarial, não será possível entrar detalhe acerca das tecnologias utilizadas para além do que está disponível no código-fonte, nomeadamente: informações relativas ao servidor, à proteção de ameaças, entre outros.

Assim, esta secção é relevante apenas para as seguintes tecnologias:

- Django - Tabela 10[12]

- Docker - Tabela 11[13]

[12] Informação retirada de https://docs.djangoproject.com/en/5.0/topics/security/ (úlimo acesso em 09-10-2024).

[13] Informação retirada de https://docs.docker.com/engine/security/ (úlimo acesso em 09-10-2024).

Tipo de proteção	**Descrição**
Cross site scripting (XSS)	Os templates utilizados pelo Django fazem *escape* de certos carateres que podem ser particularmente perigosos para HTML.
Cross site request forgery (CSRF)	Em cada pedido POST, é verificado um segredo (através de uma cookie), evitando ações não autorizadas que utilizam as credenciais de outro utilizador. O segredo é específico a cada utilizador.
Injeção de SQL	As queries dos querysets do Django estão protegidos de injeção de SQL dado que são feitas por parâmetros *escaped*, e o código SQL é definido de modo separado.
Clickjacking	Um site Django é protegido de clickjacking através do middleware X-Frame-Options que impede que o site seja renderizado num *frame*.
SSL/HTTPS	É sempre recomendado o *deployment* do site em HTTPS.
Validação do *host header*	Compara os *Host headers* com a uma lista de hosts permitidos, a *ALLOWED_HOSTS*, nas definições do site.
Referrer policy	Restringe as circunstâncias sob as quais o *Referer header* é definido, para proteger a privacidade do utilizador.
Cross-origin opener policy (COOP)	O *header* COOP permite aos browsers isolar uma janela (por exemplo, um pop-up) de outros documentos porque os coloca num grupo de contexto diferente. Assim, estes documentos não conseguem interagir diretamente com a janela.
Segurança da sessão	Os subdomínios de um site podem definir cookies para todo o domínio. Isto permite a fixação de sessão possível, caso os cookies permitidos sejam de subdomínios não controlados por utilizadores conhecidos.
Conteúdo submetido pelo utilizador	Para prevenção de ataques DoS[14] recomenda-se limitar o tamanho máximo dos ficheiros submetidos por utilizadores. Além disso, certos *handlers* (por exemplo, o *mod_php* do Apache) permitem a execução de ficheiros estáticos como se se tratassem de código e devem ser desativados.
Tópicos adicionais	Para prevenir que o código Python seja acidentalmente mostrado como plain-text/executado, não pode estar na *root* do projeto. Além disso, o sistema de autenticação não está protegido contra ataques de força bruta, e recomenda-se instalação de um plugin ou módulo que o faça.

Tabela 10: Estratégias de proteção para projetos Django.

Tipo de proteção	Descrição
Kernel namespaces	Os processos de um *container* estão isolados dos processos de outro, ou do *host*. Cada *container* também tem a sua própria stack de rede, o que significa que não tem acesso privilegiado às *sockets* ou interfaces de outro *container*.
Grupos controladores	Os grupos controladores asseguram-se de que cada *container* tem apenas o que lhe é necessário em termos de memória, CPU, I/O de disco, etc. Isto é essencial para impedir ataques DoS e assegura que um dado *container* não consegue "deitar a baixo"todo o sistema através do abuso dos recursos mencionados.
Superfície de ataque do *Docker daemon*	O Docker daemon deve ser controlado apenas por utilizadores confiáveis, dado que nada impede um desses utilizadores de partilhar, por exemplo, todo o sistema de ficheiros *root* com uma das máquinas virtuais.
Linux kernel capabilities	O Docker foi feito de modo a que o utilizador *root* de um *container* tenha menos privilégios do que o *root* real. Assim, mesmo que um atacante consiga obter privilégios de *root* dentro de um *container*, é mais difícil que faça danos sérios ou, até, que consiga progredir para o *host*.
Verificação de assinaturas *Docker Content Trust*	O Docker Engine pode ser configurado para apenas correr imagens que tenham sido assinadas.
Outras funcionalidades de segurança do *kernel*	A documentação indica que é possível utilizar sistemas como TOMOYO, AppArmor, SELinux, GRSEC, etc com o Docker. Estes sistemas podem ser vários *patches*, módulos, arquiteturas, ou *frameworks* focadas em segurança que, neste caso, são integradas no *kernel* do linux.

Tabela 11: Estratégias de proteção para projetos que utilizem Docker.

7.3.4 Conclusões

Segundo as secções anteriores, é possível agregar alguns conselhos acerca das tecnologias a ser utilizadas no eVoto.

Em relação a ataques gerais (7.3.1), é necessária uma procura por novas soluções, por falhas encontradas, e uma evolução constante na implementação dos projetos como o eVoto, para que o risco de ataques graves seja diminuído o máximo possível.

É também importante investir em formações recorrentes para evitar que atacantes consigam obter

dados confidenciais através de engenharia social e/ou phishing.

Software de voto é particularmente sensível a ataques dado que lida com um grande número de utilizadores e de dados sensíveis. Da secção 7.3.2 podemos concluir que, embora a legislação ainda esteja atrás da tecnologia atual, está a "acelerar"e, em breve, existirão novas leis e regras para a implementação deste tipo de plataformas. Como as falhas podem ser de qualquer categoria (arquitetural, criptográfica, armazenamento, etc), a segurança deve ser o maior foco deste projeto. É imperativo que os utilizadores e os seus dados estejam o mais salvaguardados possível.

Além destas estratégias, é também importante ter em atenção à tecnologia que estamos a utilizar (7.3.3). Como o Django e o Docker são ferramentas já muito familiares à equipa de desenvolvimento, é importante ter um foco adicional na segurança dado que podem surgir lacunas ou falhas que já se tenham estado a "instalar", despercebidas. De igual forma, a familiaridade da equipa com as ferramentas utilizadas pode também significar uma maior segurança, dado que possíveis anomalias serão mais facilmente detetáveis.

Finalmente, é importante manter presente, durante o desenvolvimento do eVoto sobre o modelo SaaS, que podem existir lacunas não consideradas. Num artigo em resposta a Orman [2019], Autor não identificado - CACM Staff [2019] defende que "o voto online ainda é um sonho impossível", indica que "falhas segurança críticas podem permanecer desconhecidas durante anos, mesmo em plataformas bem testadas", fazendo referência a uma falha no sistema IOS e a ataques a nível de estado encontrados pela Google. O autor não faz referência direta a este acontecimento, no entanto, muito provavelmente estará a referir-se aos ataques, que duravam já há dois anos, anunciados em Lee [2019]. É crítico que a equipa de desenvolvimento do eVoto permaneça informada e seja capaz de lidar com este tipo de ameaças mais subtis.

Capítulo 8

Conclusões e trabalho futuro

Ao longo deste documento foi investigada a tecnologia necessária para o modelo de negócio SaaS, como bases de dados e modelos de *tenancy*. Foi também feita uma contextualização na área tecnológica do voto online, e também uma breve introdução a vários conceitos específicos à indústria.

Uma secção com grande importância é a da investigação das certificações. Esta investigação foi pedida no âmbito do tema desta dissertação, dado que alterações ao ambiente legal - que rodeia, não só, o desenvolvimento de uma ferramenta destas, mas também a empresa como um todo - teriam um grande impacto. Concluiu-se de que a lei ainda está atrás do avanço da tecnologia, mas que estão a ser feitos avanços para que este atraso seja diminuído.

Por sua vez, a análise histórica e legal do voto eletrónico em Portugal e no mundo foi um catalisador para a investigação da Lei da Resiliência Cibernética (CRA). A investigação da CRA foi especialmente relevante dado ser um assunto muito atual e em constante mudança e atualização, que vai transformar tanto o espaço económico europeu como o mundial. Apesar de não se aplicar diretamente ao eVoto, permitiu dar uma nova perspetiva acerca do ponto de situação legislativo, por parte da UE, em relação a tecnologia de ponta. Permitiu também pôr em evidência que alguns dos produtos e serviços oferecidos pela empresa poderão, no futuro, ser afetados.

Num âmbito mais restrito ao software de votação, foram também analisadas as principais plataformas de voto em modelo SaaS. Esta análise do mercado de concorrentes permitiu adquirir conhecimento acerca de, nomeadamente, quais as estratégias de monetização mais comuns, qual o método mais atraente para a exposição das caraterísticas da plataforma eVoto, e, também, quais as funcionalidades que permitirão dar ao utilizador a melhor experiência possível.

Uma posterior análise do eVotUM permitiu definir diretrizes para o desenvolvimento e implementação do eVoto, e também pontos de interesse e/ou melhoria tanto do ponto de vista do utilizador, como do *developer*. Entre estes, destacam-se: os desafios associados ao facto de que o eVoto será em código aberto, a integração de métodos de exportação de dados (ausentes no eVotUM), a arquitetura do eVotUM

que não poderá ser reaproveitada devido ao modelo SaaS não o permitir, entre outros.

As alterações necessárias, levantadas durante a análise do eVotUM e do mercado, foram agregadas na secção de Alterações para a Comercialização do eVoto. Estão também presentes sugestões para o melhoramento da plataforma e da experiência do lado do utilizador, mas que não são consideradas essenciais. Um exemplo destas alterações, é a implementação de uma demo grátis, ou a implementação de um modo de navegação para utilizadores invisuais.

Foi também apresentado um roadmap de alterações, e algumas sugestões sobre como expandi-lo ainda mais. Nomeadamente, a apresentação do eVoto em convenções tais como a FOSDEM ou a DjangoCon, que trariam um grande nível de exposição para não só um número incontável de empresas e outras entidades, como também permitiria "marcar presença"no mercado informático europeu.

Logo após a exploração do roadmap, expuseram-se os desenvolvimentos já iniciados para o website que apresenta o eVoto para o público em geral. Estes desenvolvimentos incluem as secções e os tipos de apresentação de conteúdo mencionados no capítulo das Alterações para a Comercialização do eVoto.

Futuramente, será necessário definir quais os passos a tomar para a adaptação da empresa às normas definidas na CRA. Tal como mencionado na secção "Como é que isto afeta a empresa?"(4.0.1), esclarecimentos recentes com os criadores da CRA indicam que o eVoto não será afetado. No entanto, a empresa continua a desenvolver software que é utilizado em máquinas de terceiros. Isto irá, certamente, ser afetado assim que a diretriz for aprovada pela União Europeia.

Especificamente para o eVoto, será necessário definir de um modo mais minucioso quais as tarefas a realizar, à semelhança do modo como funcionam os *sprints* na técnica de desenvolvimento de projetos SCRUM[1].

Poderá ser também necessário ajustar o *design* do site público, para além de criar o *design* da plataforma em si - nomeadamente, o aspeto (cores, tema, estilização), o fluxo de utilização por parte dos vários tipos de utilizador (não pago, pago, administrador), a organização da informação em cada um dos passos de uma eleição, entre outros.

Com o desenvolvimento da plataforma, irão certamente surgir desafios e obstáculos inesperados. Apenas nos é possível investigar, planear, e prevenir, para que estes desvios sejam mitigados e, assim, que seja criada uma plataforma de voto online amiga do utilizador, acessível, rentável e, principalmente, segura e justa.

[1] https://www.atlassian.com/agile/scrum/sprints (úlimo acesso em 09-10-2024)

8.0.1 Resposta às Perguntas de Investigação

Nesta secção final estão expostas as perguntas primeiramente apresentadas na introdução. Embora estas perguntas tenham sido respondidas ao longo deste documento, é feito aqui um resumo dos resultados obtidos, para que sejam respondidas sucintamente e de um modo mais prático para consulta pelo leitor.

PI1. Qual é o impacto da transição do eVoto para uma arquitetura SaaS na segurança do processo de votação online? Deduziu-se que o maior risco associado com a transição do eVoto para SaaS será a exposição desprotegida dos dados pessoais das entidades envolvidas nos processos eleitorais. Atualmente, a ferramenta já detém uma forte componente de segurança - nomeadamente, ao encriptar os dados dos utilizadores nos seus dispositivos, antes sequer de existir algum tipo de comunicação para o exterior. Mesmo assim, é crucial investir em formações e em auditorias internas, para que quaisquer erros ou falhas de segurança tenham menor probabilidade de acontecer e/ou de ser de alto risco. Para uma análise aprofundada desta questão, é favor referir à secção "Análise de Riscos"(7.3).

PI2. Quais são as implicações legais e regulatórias da transição do eVoto para uma arquitetura SaaS, considerando os diferentes contextos nacionais e internacionais? Durante esta investigação, concluiu-se que ainda não existem leis europeias (ou mundiais) reguladoras e concretas acerca deste tipo de software. No entanto, estão a ser dados passos para aumentar a segurança do consumidor final, e também para alterar o modo de funcionamento da indústria informática como um todo. Este facto é provado pela existência da Lei Europeia de Resiliência Cibernética, e é estimado esta entrar em ação no futuro próximo; e embora saibamos que não irá afetar o eVoto diretamente, irá, apesar disso, afetar toda a indústria informática. Para uma análise aprofundada desta questão, é favor referir à secção "Análise Histórica e Legal do Voto Eletrónico em Portugal e no Mundo"(4).

PI3. Como é que será impactada a transparência e auditabilidade do eVoto, na transição para uma arquitetura SaaS? Uma vez que o eVoto é software de código aberto, não se prevê que a transparência nem a auditabilidade do produto seja afetado pela transição para SaaS. Poderão existir nuances acerca dos serviços prestados ao utilizador final, dado que serão feitos de modo diferente (não SaaS vs. SaaS). No entanto, não se considera que estas alterações terão um impacto suficientemente elevado que consiga causar problemas na auditabilidade ou na transparência da ferramenta. Isto é reforçado pelo facto de que a empresa é alvo de auditorias constantes, para

as diferentes certificações ISO que detém, e pelas quais o eVoto é também abrangido. Para mais informações acerca das mudanças necessárias para a comercialização do eVoto como solução SaaS, é favor referir à secção "Alterações para a comercialização do eVoto"(7).

Bibliografia

ACE Electoral Knowledge Network. Auditing of e-voting systems, 2023. URL https://aceproject.org/ace-en/focus/e-voting/e-voting-auditing/mobile_browsing/onePag.

R. Michael Alvarez, Thad E. Hall, and Alexander H. Trechsel. Internet voting in comparative perspective: The case of estonia. *PS: Political Science & Politics*, 42(3):497–505, 2009. doi: 10.1017/S1049096509090787.

Assembleia da República. Resolução da assembleia da república n.º 123/2021, de 27 de abril, 2021. URL https://dre.pt/dre/detalhe/resolucao-assembleia-republica/123-2021-162159136.

Autor não identificado - CACM Staff. Online voting still security pipedream. *Communications of the ACM*, 62(12):9, 2019.

C. Warren Axelrod. Applying lessons from safety-critical systems to security-critical software. In *2011 IEEE Long Island Systems, Applications and Technology Conference*, pages 1–6, 2011. doi: 10.1109/LISAT.2011.5784222.

Fay Chang, Jeffrey Dean, Sanjay Ghemawat, Wilson C Hsieh, Deborah A Wallach, Mike Burrows, Tushar Chandra, Andrew Fikes, and Robert E Gruber. Bigtable: A distributed storage system for structured data. *ACM Transactions on Computer Systems (TOCS)*, 26(2):1–26, 2008.

Comissão Europeia. Proposta de regulamento do parlamento europeu e do conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o regulamento (ue) 2019/1020, 2022. URL https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52022PC0454.

Comissão Nacional de Eleições. Voto eletrónico, 2023. URL https://www.cne.pt/content/voto-electronico.

Veronique Cortier, David Galindo, Stephane Glondu, and Malika Izabachene. A generic construction for voting correctness at minimum cost - application to helios. Cryptology ePrint Archive, Paper 2013/177, 2013. URL https://eprint.iacr.org/2013/177. https://eprint.iacr.org/2013/177.

Council of Europe. Security recommendations and best-practices for e-enabled voting, 2003. URL https://www.coe.int/t/dgap/goodgovernance/Activities/E-voting/Work_of_e-voting_committee/03_Background_documents/05Security_recommendations_draft_en.asp.

Council of Europe. Certification of e-voting systems - guidelines for developing processes that confirm compliance with prescribed requirements and standards, 2011. URL https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059bdf8.

Eclipse Foundation. Update on the european cyber resilience act, 2023. URL https://www.youtube.com/watch?v=AmsM5_5QO5A.

e-Estonia. e-governance, 2023. URL https://e-estonia.com/solutions/e-governance/e-democracy/.

European Union. Council directive 93/109/ec of 6 december 1993. Official Journal of the European Union, 1993. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31993L0109.

Fortra. Saas: Single tenant vs multi-tenant - what's the difference?, 2018. URL https://www.digitalguardian.com/fr/blog/saas-single-tenant-vs-multi-tenant-whats-difference.

J Paul Gibson, Robert Krimmer, Vanessa Teague, and Julia Pomares. A review of e-voting: the past, present and future. *Annals of Telecommunications*, 71(7):279–286, 2016.

GNU. Gnu general public license, 2023. URL https://www.gnu.org/licenses/gpl-3.0.en.html.

Inter-Parliamentary Union. South africa - parliamentary chamber: National assembly - elections held in 1994, 1994. URL http://archive.ipu.org/parline-e/reports/arc/2291_94.htm.

ISO. ISO 9001:2015, 2015. URL https://www.iso.org/standard/62085.html. ISO.

ISO. Systems and software engineering — software life cycle processes, 2017a. URL https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:12207:ed-1:v1:en.

ISO. Information security, cybersecurity and privacy protection — information security management systems — requirements, 2017b. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en.

ISO. Software engineering — guidelines for the application of iso 9001:2015 to computer software, 2018. URL https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:90003:ed-1:v1:en. ISO/IEC/IEEE 90003:2018.

ISO. Quality management systems - particular requirements for the application of iso 9001:2015 for electoral organizations at all levels of government, 2019. URL https://www.iso.org/obp/ui/#iso:std:iso:ts:54001:ed-1:v1:en. ISO/TS 54001:2019.

ISO. Information security, cybersecurity and privacy protection — evaluation criteria for it security — part 1: Introduction and general model, 2022a. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-4:v1:en.

ISO. Information security, cybersecurity and privacy protection — evaluation criteria for it security — part 2: Security functional components, 2022b. URL https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-2:ed-4:v1:en.

Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. *RSA Laboratories*, 2005. Bedford, MA, USA.

Koombea. Vertical vs horizontal saas explained, 2024. URL https://www.koombea.com/blog/vertical-horizontal-saas/.

Laura Sheeter for BBC News. Estonia forges ahead with e-vote, 2005. URL http://news.bbc.co.uk/2/hi/europe/4343374.stm.

Dave Lee. Google finds 'indiscriminate iphone attack lasting years', 2019. URL https://www.bbc.com/news/technology-49520355.

Microsoft. Multi-tenant saas database tenancy patterns, 2023. URL https://learn.microsoft.com/en-us/azure/azure-sql/database/saas-tenancy-app-design-patterns?view=azuresql.

Microsoft. What is saas?, 2024. URL https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas.

National Democratic Institute. Internet voting in estonia, 2023. URL https://www.ndi.org/e-voting-guide/examples/internet-voting-in-estonia.

Hilarie Orman. Online voting: We can do it! (we have to). *Communications of the ACM*, 62(9):25–27, 2019.

OWASP. Owasp top ten, 2021. URL https://owasp.org/www-project-top-ten/.

Redhat. What is software as a service?, 2023. URL https://www.redhat.com/pt-br/topics/cloud-computing/what-is-saas.

Carsten Schürmann, Jordi Barrat, Eden Bolo, Alejandro Bravo, Robert Krimmer, Stephan Neumann, Al Acong Parreno, Melanie Volkamer, and Peter Wolf. *Certification of ICTs in Elections*. International IDEA, 2015. ISBN 978-91-7671-028-9.

SGMAI. Lei eleitoral para a assembleia da república, 2021. URL https://www.sg.mai.gov.pt/AdministracaoEleitoral/EleicoesReferendos/AssembleiaRepublica/Documents/AR2022/Lei%20Eleitoral%20da%20Assembleia%20da%20Rep%C3%BAblica_2022_WEB.pdf.

SGMAI - Administração Eleitoral. Voto eletrónico no distrito de Évora - relatório final, 2019. URL https://www.sg.mai.gov.pt/AdministracaoEleitoral/Publicacoes/RelatoriosAtosEleitorais/Documents/PVEE_DocApoio_07.001%20-%20Relatorio%20AR_Versao%20Final.pdf.

SGMAI - Administração Eleitoral. Consulta dos cadernos de recenseamento, 2023. URL https://www.recenseamento.mai.gov.pt/.

Silverback Data Center Solutions. Cloud vs on-premise? here are five factors to consider, 2024. URL https://teamsilverback.com/cloud-vs-on-premise-five-factors-to-consider/.

Universidade do Minho. evotum - guia do eleitor, 2017. URL https://evotum.uminho.pt/static/voters/files/EVOTUM_GUIA_ELEITOR_V2.pdf.

Universidade do Minho. evotum - perguntas frequentes, 2023. URL https://evotum.uminho.pt/pt/voters/page/frequent-questions/.

v500 Systems. 10 essential steps to safeguard your saas applications in aws cloud, 2024. URL https://www.v500.com/safeguard-saas-apps-in-aws-10-steps/.

Parte III
Apêndices

Apêndice A
Exemplos de utilização

Existem alguns exemplos populares de aplicações que utilizam o modelo SaaS: GMail, Microsoft Office, Adobe Creative Cloud e Spotify [1]. Existem também aplicações SaaS open-source: Nextcloud, SuiteCRM, Odoo[2] e Mautic, entre outras.

É importante explorar soluções de aplicações SaaS não orientadas ao e-voto, uma vez que podem existir distinções claras no modo como são desenvolvidas, implementadas, e geridas. Estas diferenças ajudam a formar uma ideia mais clara do que é necessário para uma plataforma de e-voto versus o que é apenas arquitetura típica para qualquer aplicação SaaS, e é também benéfico para identificar certos padrões da indústria para este modelo de distribuição.

Não é pretendido que esta secção seja uma análise profunda, mas sim apenas uma aproximação inicial. O intuito de explorar estes exemplos variados é precisamente para estudar como diferentes aplicações, para diferentes propósitos e tipos de clientes, são desenvolvidas, e o que diferencia cada uma delas, de um modo mais geral.

Uma análise mais detalhada estará reservada para soluções de e-voto em modelo de negócio SaaS, existentes no mercado.

Função

Aplicação	Função
Gmail	Gestão e comunicação por email.
Microsoft Office	Suíte de software de produtividade.
Adobe Creative Cloud	Suíte de software de criatividade.
Spotify	Serviço de *streaming* de música
NextCloud	Partilha e colaboração de ficheiros.
SuiteCRM	Gestão de relações com clientes.
Mautic	Automatização de marketing.
Odoo	Gestão empresarial.

Tabela 12: Função de cada uma das soluções analisadas.

[1] IBM Technology: https://www.youtube.com/watch?v=20QUNgFIrK0 (2023-01-20)

[2] Também conhecido pelo seu nome antigo, OpenERP

Estas aplicações foram escolhidas por serem bastante variadas, mesmo dentro da sua respetiva categoria de open ou closed-source. Observar como diferentes aplicações funcionam é importante, pois permite obter uma perspetiva mais generalizada das necessidades de uma aplicação SaaS, impedindo que aspetos críticos (ou maneiras melhores e mais eficientes de implementar várias partes da aplicação) não passem despercebidos.

Front-end

Aplicação	Front-end
Gmail	HTML/CSS, biblioteca open-source de javascript chamada Closure Library [a]
Microsoft Office	Windows Forms [b]. Add-ins feitos pelo utilizador permitem estender funcionalidades e interagir com a suíte, utilizando HTML, CSS, e JavaScript. Existem também add-ins antigos (apenas para Office for Windows) que utilizam Component Object Model, Visual Basic for Aplications ou Visual Studio Tools for Office.
Adobe Creative Cloud	HTML, CSS, e JavaScript[c]
Spotify	PHP, HTML/CSS[d]
NextCloud	Javascript, HTML/CSS, PHP para traduções[e]
SuiteCRM	Javascript (Angular)[f]
Mautic	HTML/CSS, Javascript[g]
Odoo	HTML, Javascript, QWeb (proprietário), XML[h]

Tabela 13: Caraterísticas do front-end de cada uma das soluções analisadas.

[a] Google: https://developers.google.com/closure/library (2023-01-20)
[b] Microsoft: https://learn.microsoft.com/en-gb/dotnet/desktop/winforms/overview/?view=netdesktop-6.0 (2023-01-21)
[c] Adobe: https://developer.adobe.com/commerce/php/best-practices/extensions/faq/ (2023-01-21)
[d] James La Broy: https://engineering.atspotify.com/2022/07/what-it-took-to-scale-spotifys-marketing-efforts/ (2023-01-21)
[e] Nextcloud: https://docs.nextcloud.com/server/latest/developer_manual/basics/front-end/index.html (2023-01-21)
[f] SuiteCRM: https://docs.suitecrm.com/8.x/developer/front-end-architecture/ (2023-01-21)
[g] Mautic: https://developer.mautic.org/?php#introduction (2023-01-21)
[h] Ermin Trevisan. https://www.odoo.com/pt_BR/forum/ajuda-1/technical-architecture-for-odoo-12-149657 (2023-01-21)

Através desta tabela conclui-se que são utilizadas as tecnologias standard para o desenvolvimento front-end, começando pelo básico HTML/CSS, até a linguagens como Javascript e PHP.

Backend

Aplicação	Back-end
Gmail	Bigtable[Chang et al., 2008], um sistema de armazenamento distribuído para dados estruturados.
Microsoft Office	C++[a]
Adobe Creative Cloud	PHP[b]
Spotify	Java, Python[c] (serviços back-end e análise de dados), e alguns serviços mais antigos em C ou C++
NextCloud	PHP, Javascript[d]. Suporta MySQL/MariaDB, PostgreSQL e Oracle[e]
SuiteCRM	PHP, mySQL[f]. Para webservers, está oficialmente preparado para usar Apache ou IIS, embora existam soluções com Nginx não mencionadas na documentação.
Mautic	PHP (framework Symfony), suporta bases de dados MySQL/MariaDB[g].
Odoo	PostgreSQL, Python, XML[h]

Tabela 14: Caraterísticas do back-end de cada uma das soluções analisadas.

[a] Boris Kolpackov: https://cppcon.org/bonus-talk-cxx-in-ms-office-2014/ (2023-01-21)
[b] Adobe: https://developer.adobe.com/commerce/php/best-practices/extensions/faq/ (2023-01-21)
[c] Geoff van der Meer: https://engineering.atspotify.com/2013/03/how-we-use-python-at-spotify/ (2023-01-21)
[d] NextCloud: https://github.com/nextcloud/server (2023-01-21)
[e] Nextcloud: https://docs.nextcloud.com/server/latest/admin_manual/configuration_database/linux_database_configuration.html (2023-01-21)
[f] SuiteCRM: https://docs.suitecrm.com/8.x/developer/installation-guide/ (2023-01-21)
[g] Mautic: https://developer.mautic.org/?php#introduction (2023-01-21)
[h] Ermin Trevisan: https://www.odoo.com/pt_BR/forum/ajuda-1/technical-architecture-for-odoo-12-149657 (2023-01-21)

Observa-se que são utilizadas as tecnologias standard para o desenvolvimento backend, nomeadamente PHP e Javascript, incluindo também algumas referências a motores de bases de dados como MySQL e PostgreSQL.

Escalabilidade

Aplicação	Escalabilidade
Gmail	Sendo suportado pelo Bigtable[Chang et al., 2008], o GMail está preparado para escalar até petabytes de dados.
Microsoft Office	É suportado pela plataforma de computação em cloud Azure, pelo que está igualmente preparado para uma alta escalabilidade.
Adobe Creative Cloud	Utiliza os serviços da Amazon (AWS)[a] pelo que está preparado para uma alta escalabilidade.
Spotify	Utiliza os serviços da Google Cloud[b] pelo que está preparado para escalar para milhões de utilizadores simultâneos.
NextCloud	Trabalha com vários *providers*, oficiais[c] e não oficiais[d]. Também é possível optar por implementar uma instância do Nextcloud, logo cada solução irá ter os seus limites em termos de escalabilidade.
SuiteCRM	Tem uma lista de parcerias[e], cada uma com as suas caraterísticas em termos de escalabilidade; por exemplo, o parceiro Univention oferece várias opções de *hosting*, uma delas utilizando a AWS.
Mautic	Escalabilidade é muito dependente do hardware, mas existem *community partners* oficiais[f].
Odoo	Tal como as outras opções open-source, a sua escalabilidade é bastante dependente do hardware.

Tabela 15: Escalabilidade de cada uma das soluções analisadas.

[a] Amazon Web Services (AWS): https://aws.amazon.com/partners/adobe/ (2023-01-21)
[b] Google Cloud: https://cloud.google.com/customers/featured/spotify (2023-01-21)
[c] Nextcloud: https://nextcloud.com/partners/ (2023-01-22)
[d] Nextcloud: https://github.com/nextcloud/providers (2023-01-22)
[e] SuiteCRM: https://suitecrm.com/about/about-us/partners/ (2023-01-22)
[f] Mautic: https://www.mautic.org/mautic-community-partners (2023-01-22)

Apesar de depender também de outros fatores, como a eficiência do código responsável por *load balancing* do servidor, o tópico de escalabilidade é altamente dependente do poder do hardware onde a aplicação está a ser hospedada. É óbvio que aplicações desenvolvidas e hospedadas por gigantes da tecnologia como a Google, Microsoft e a Amazon, vão conseguir ter tempos de resposta mais curtos, e ter uma capacidade de utilizadores simultâneos também muito maior, quando comparados com empresas não tão globais.

Assim, para a plataforma eVoto, torna-se uma prioridade estudar motores responsáveis pelo serviço da aplicação online, ao cliente, para ser possível tirar o melhor partido possível dos servidores da Eurotux.

Foi observado um fenómeno interessante nesta tabela, Escalabilidade, e na tabela apresentada a seguir, Performance. Enquanto que na primeira tabela a informação mais facilmente obtida e com maior grau de certeza correspondia àquela das soluções closed-source, o oposto foi observado na segunda tabela.

Pensa-se que a razão para tal é que a informação pertinente às aplicações closed-source, pela sua própria natureza, são mais orientadas a um cliente não developer - mas não exclusivamente. Uma grande parte da informação mais prontamente disponível sobre aumento de desempenho para estas aplicações era dedicada a problemas apenas resolvíveis do lado do consumidor.

Já as soluções open-source tendem a apontar os seus esforços de marketing e documentação para um cliente developer, um cliente que irá implementar e modificar a aplicação para o seu uso customizado - mas não exclusivamente, pois como se pode cobservar todas as opções open-source aqui exploradas têm parcerias com *providers* que fornecem serviços ao cliente menos interessado em implementar e modificar a aplicação, e mais em apenas utilizá-la como qualquer outro serviço.

Performance

Aplicação	Performance
Gmail	Opções de limpeza de cache, front-end e back-end.
Microsoft Office	Opções para reduzir a quantidade de dados que são carregadors, assim como desativar add-ons e templates. Também permite limpar a cache.
Adobe Creative Cloud	Permite alterar uma série de fatores para permitir um tempo de carregamento menor e diminuir a carga na rede, assim como desativar add-ons, e limpar a cache[a].
Spotify	Permite limpar a cache, e a música é comprimida para diminuir o peso na rede.
NextCloud	Oferece recomendações para otimizar a instância, e informação sobre os métodos de melhoramento de performance incluídos[b]: ferramentas de diagnóstico do sistema, dicas para correr numa máquina virtual, cache, recomendações de motores de bases de dados devido a problemas de performance conhecidos, *file locking*, dicas sobre *offloading* de TLS (HTTPS) e en/decriptação, entre outros.
SuiteCRM	Oferece uma série de referências[c] para otimização de servidores, nomeadamente: instalação de uma *php oncode cache* para aumentar a performance de todos os ficheiros, alterações para otimizar o MySQL, indexação, e mudanças no *config*, entre outros.

Tabela 16: Soluções para performance em cada uma das soluções analisadas - parte 1.

[a] Lara Lee: https://www.laralee.design/slow-adobe/ (2023-01-22)
[b] Nextcloud: https://docs.nextcloud.com/server/latest/admin_manual/installation/server_tuning.html (2023-01-22)
[c] SuiteCRM: https://docs.suitecrm.com/developer/performance-tweaks/ (2023-01-22)

Aplicação	Performance
Mautic	Apresenta alguns pontos[a] para aumentar a performance: limpeza da cache, resolver o *schema* da base de dados, verificar os logs, entre outros.
Odoo	Olivier Dony for OpenERP[b] diz que devido ao PostgreSQL, é altamente escalável. Deve-se também evitar fazer o deployment do PostgreSQL numa VM, mas se for necessário, deve-se otimizar para operações I/O. Sugere também utilizar a ferramenta `munin` para monitorizar os tempos de resposta da aplicação. Fornece também quais deverão ser os tempos normais para os vários tipos de respostas, para comparação.

Tabela 17: Soluções para performance em cada uma das soluções analisadas - parte 2.

[a] Mautic: https://docs.mautic.org/en/troubleshooting (2023-01-22)

[b] Olivier Dony for OpenERP: https://www.slideshare.net/openobject/tips-on-how-to-improve-the-performance-of-your-custom-modules-for-high-volumes-deployment-olivier-dony-open-erp (2023-01-29)

Nesta secção é possível observar que é quase sempre oferecido ao cliente o mesmo conjunto de opções para melhoramento de performance, um padrão que é comum tanto a soluções closed-source como open-source. As opções são: limpeza de cache, desativar add-ons (quando aplicável) e redução da qualidade dos dados a ser enviados (compressão de dados).

Tal como era esperado, as soluções open-source oferecem métodos muito mais exaustivos, uma vez que é possível manipular o próprio código da aplicação. Salienta-se que observar o que as aplicações closed-source oferecem é importante para, mais tarde, avaliar que opções poderiam ser oferecidas aos clientes do eVoto, olhando para os exemplos aqui coletados.

Segurança

Aplicação	Segurança
Gmail	Uma caraterística interessante acerca de como a Google garante a segurança dos seus utilizadores no Gmail, é a da utilização de inteligência artificial para detetar e assinalar emails com tentativas de scam, phishing e malware. O Gmail também é protegido através de monitorização de logins suspeitos, e encriptação de emails.
Microsoft Office	Para além da proteção base oferecida de graça, a Microsoft vende a ferramenta Microsoft Defender [a], que cobre todos os serviços do Microsoft 365, e permite: gerir e assegurar a segurança de identidades, deteção de ameaças e falhas de segurança, ivestigação automatizada, opções de segurança para aplicações na nuvem, e também segurança orientada ao email, para impedir tentativas de phishing ou comprometimento de emails empresariais.
Adobe Creative Cloud	A Adobe adota o Secure Product Lifecycle (SPLC), que é uma política de desenvolvimento de produto que garante que existem normas de segurança a cumprir durante qualquer momento do ciclo de vida do produto [b].
Spotify	O Spotify criou a Kitsune [c], uma plataforma para gerir vulnerabilidades. Nesta plataforma, os *developers* recebem notificações de quando vulnerabilidades são encontradas e lhes são atribuídas; também permite escalar problemas para os *stakeholders* apropriados.

Tabela 18: Segurança de cada uma das soluções analisadas - parte 1.

[a] Microsoft: https://www.microsoft.com/pt-pt/security/business/siem-and-xdr/microsoft-365-defender (2023-02-23)

[b] Adobe: https://www.adobe.com/trust/security/adobe-splc.html (2023-02-23)

[c] Yukio Mizuta, Nurit Izrailov: https://engineering.atspotify.com/2022/11/spotifys-vulnerability-management-platform/ (2023-02-23)

Aplicação	Segurança
NextCloud	Existem várias caraterísticas [a] relacionadas com a segurança: ferramentas já incluídas para monitorização e criação de logs, administradores podem definir permissões de acesso e regras para retenção de dados, existe também controlo no acesso a ficheiros, e encriptação em várias camadas (utilizando o standard SSL/TLS na transferência de dados). Também detalha que princípios de segurança são seguidos para a autenticação, tais como SSO/SAML e 2FA.
SuiteCRM	Oferece uma suíte de funcionalidades aptamente chamada Security Suite [b], que permite a definição de grupos, cada um com as suas permissões específicas.
Mautic	O Mautic pratica uma política (Security Advisory) onde avios utilizadores quando são encontradas vulnerabilidades, e quais os passos que devem seguir [c].
Odoo	A equipa [d] aponta os maiores fatores que contribuem para um baixo nível de segurança, e apresenta soluções para fortalecer esses aspetos: injeção de código, erros de lógica durante autenticação, exposição de dados sensíveis, *parsing* de dados XML não confiáveis, validações incorretas de permissões de utilizadores, má configuração da segurança para *deployment*, entre outros.

Tabela 19: Segurança de cada uma das soluções analisadas - parte 2.

[a] Nextcloud: https://nextcloud.com/secure/ (2023-02-23)
[b] SuiteCRM: https://docs.suitecrm.com/user/security-suite-groups/ (2023-02-23)
[c] Mautic Security Team: https://www.mautic.org/mautic-security-team (2023-02-23)
[d] Odoo: https://www.slideshare.net/openobject/security-odoo-code-hardening (2023-02-23)

A informação sobre a segurança que é apresentada nesta secção é bastante variada, e oferece diferentes perspetivas, e todas devem ser consideradas durante a análise da plataforma eVotUM, não só quais as opções oferecidas aos clientes, mas também das políticas internas que devem ser adaptadas pela empresa criadora.

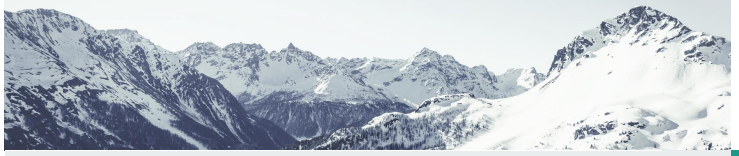
Apêndice B
Apresentação das Certificações

Este apêndice contém a apresentação feita acerca das conclusões tomadas depois da investigação aprofundada da certificação ISO/TS 54001:2019.

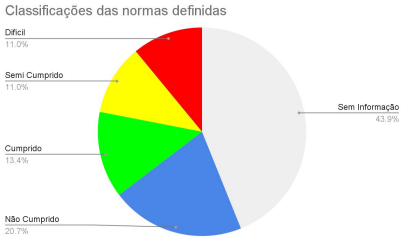
Também está disponível para consulta no link https://docs.google.com/presentation/d/1r-pj5RmFOSRt3V17ruumtdEwZqtQUnUP5ezecHoam8g/edit?usp=sharing.

Conclusões de Análise

Certificação ISO/TS 54001:2019



Resumo



Classificações

Sem Informação

Caso não exista informação adicional à do ISO 9001, ou caso a informação dada não seja relevante. Estes pontos podem ser contados como cumpridos.

Não Cumprido

São pontos que podem ser cumpridos. A esmagadora maioria dos pontos com esta classificação são referentes a documentação que deve ser criada.

Cumprido

Já cumprido pelo eVotUM.

Semi-Cumprido

Estes pontos já têm partes de si cumpridas, mas falta algum desenvolvimento ou documentação para cumprir na totalidade.

Dificil

A maior parte destes pontos têm referências explícitas a eleições físicas que, pela natureza do eVoto, são (quase) impossíveis de satisfazer.

Conclusão

A favor

- 89% das normas definidas estão ou podem ser satisfeitas

Contra

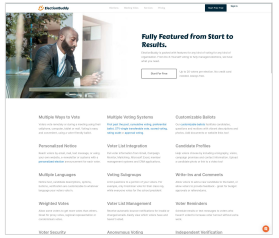
- 11% das normas são dificilmente cumpridas do modo definido pela norma

→ Solução Alternativa

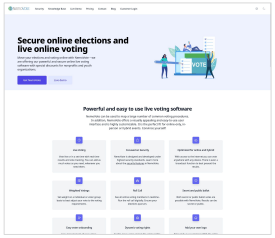
Solução Alternativa

Criar na homepage do eVoto uma lista de comparações entre o que o eVoto implementa e o que a certificação define.

- Sugestão: não diretamente, criar apenas uma lista de características.
  Fazer uma comparação direta à certificação mas não estarmos certificados nela pode causar desconfiança em potenciais clientes.

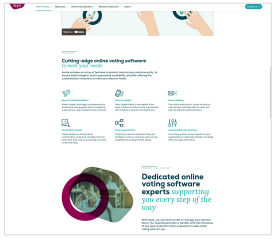


ElectionBuddy

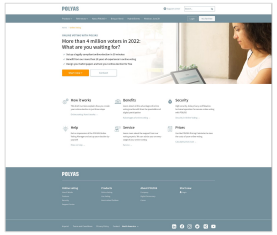


NemoVote

Em caixas

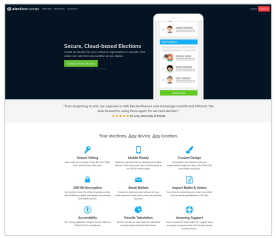


Scytl - InVote



Polyas

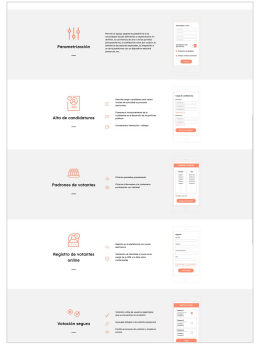
Em caixas



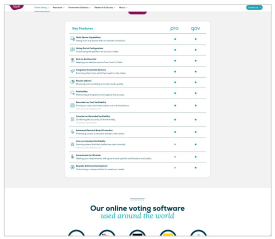
ElectionRunner

Em caixas

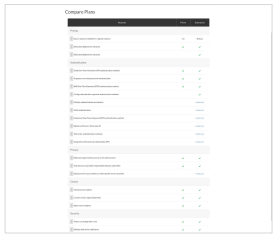
DemocraciaOS - Votación de Autoridades



Conjunto de ícones com tópicos

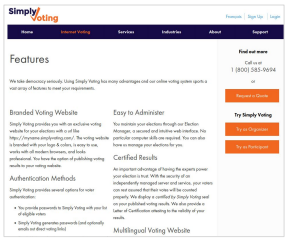


ScytI - InVote



NVotes

Em tabela - Características e comparação de planos



SimplyVoting

Descrição detalhada

Sugestões

- Acessibilidade
- Chatbot
- Levantamento de Opiniões

Acessibilidade

Logo após segurança, acessibilidade é a maior força motriz para o voto online.

Comercializar o eVoto como sendo uma opção altamente acessível poderia ser uma boa estratégia para o destacar no mercado.

Por exemplo:

- Pronto para leitores de ecrã
- Apto para destreza limitada
- Navegável por teclado
- Modo de alto contraste
- Modo para daltonismo
- Foco claro do cursor

Exemplo Voatz

Chatbot

Serviço de suporte já utilizado por muitas empresas.

Poderia ser interessante fornecer um serviço de suporte em formato de chatbot.

Existem soluções no mercado prontas a implementar.

Exemplos:

- Electionbuddy
- ERA
- ChatBot

Levantamento de Opiniões

Requerido por uma das cláusulas da norma ISO/TS 54001.

Por exemplo, um pop-up que apareceria a pedir para classificar a aplicação.

- Apenas a uma parte do corpo eleitoral
- Durante um intervalo de tempo depois do lançamento do eVoto
- Ou apenas para as primeiras eleições de um dado utilizador

Conclusões de Análise

Certificação ISO/TS 54001:2019

Apêndice C
CRA - Informações e Instruções Destinadas ao Utilizador

Este apêndice é um excerto do Regulamento de Resiliência Cibernética [Comissão Europeia, 2022].

No mínimo, devem ser fornecidas com o produto com elementos digitais as seguintes indicações:

1. O nome, nome comercial registado ou marca registada do fabricante, bem como o seu endereço postal e endereço de correio eletrónico de contacto, apostos no produto ou, se tal não for possível, na embalagem ou num documento que o acompanhe;

2. O ponto de contacto por meio do qual se pode comunicar e receber informações sobre vulnerabilidades de cibersegurança do produto;

3. A identificação correta do tipo, lote, versão ou número de série ou outros elementos que permitam a identificação do produto e as respetivas instruções e informações destinadas ao utilizador;

4. A utilização prevista, incluindo o ambiente de segurança proporcionado pelo fabricante, bem como as funcionalidades essenciais do produto e informações sobre as propriedades de segurança;

5. Qualquer circunstância conhecida ou previsível, relacionada com a utilização do produto com elementos digitais de acordo com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsível que possam dar origem a riscos de cibersegurança significativos;

6. Se é possível aceder à lista de materiais do software e, se for caso disso, onde se pode fazê-lo;

7. Se for caso disso, o endereço Internet que permite aceder à declaração de conformidade UE;

8. O tipo de apoio técnico no domínio da segurança que o fabricante oferece e até quando será prestado ou, no mínimo, até quando os utilizadores podem esperar receber atualizações de segurança;

9. Instruções pormenorizadas ou um endereço Internet que remeta para tais instruções pormenorizadas e informações sobre:

(a) As medidas a tomar quando o produto é posto em funcionamento pela primeira vez e ao longo de toda a sua vida útil de modo a garantir uma utilização segura do mesmo;

(b) Como as alterações do produto podem afetar a segurança dos dados;

(c) Como podem ser instaladas atualizações relevantes em termos de segurança;

(d) A desativação segura do produto, incluindo informações sobre como se pode remover de forma segura os dados dos utilizadores.

Apêndice D
CRA - Produtos Críticos com Elementos Digitais

Este apêndice é um excerto do Regulamento de Resiliência Cibernética [Comissão Europeia, 2022].

Classe I

1. Software de sistemas de gestão de identidade e software de gestão de acesso privilegiado;
2. Navegadores autónomos e incorporados;
3. Gestores de senhas;
4. Software de pesquisa, remoção ou colocação em quarentena de software malicioso;
5. Produtos com elementos digitais com a função de rede privada virtual (VPN);
6. Sistemas de gestão de rede;
7. Ferramentas de gestão da configuração da rede;
8. Sistemas de monitorização do tráfego na rede;
9. Gestão de recursos de rede;
10. Sistemas de gestão de informações e eventos de segurança (SIEM);
11. Gestão de atualizações/atualizações corretivas, incluindo gestores de arranque;
12. Sistemas de gestão da configuração de aplicações;
13. Software de acesso remoto/partilha à distância;
14. Software de gestão de dispositivos móveis;
15. Interfaces físicas da rede;
16. Sistemas operativos não abrangidos pela classe II;

17. Barreiras de segurança, sistemas de deteção e/ou prevenção de intrusões não abrangidos pela classe II;
18. Encaminhadores, modems para ligação à Internet e comutadores não abrangidos pela classe II;
19. Microprocessadores não abrangidos pela classe II;
20. Microcontroladores;
21. Circuitos integrados de aplicação específica (ASIC) e redes de portas lógicas programáveis (FPGA) destinados a serem utilizados por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)];
22. Sistemas de controlo da automação industrial (IACS) não abrangidos pela classe II, tais como controladores lógicos programáveis (PLC), sistemas de controlo distribuído (DCS), controladores numéricos computorizados (CNC) para máquinas-ferramentas e sistemas de supervisão, controlo e aquisição de dados (SCADA);
23. Internet das coisas industrial não abrangida pela classe II.

Classe II

1. Sistemas operativos para servidores, computadores de secretária e dispositivos móveis;
2. Hipervisores e sistemas container runtime que permitam a execução virtualizada de sistemas operativos e ambientes semelhantes;
3. Infraestruturas de chaves públicas e emitentes de certificados digitais;
4. Barreiras de segurança, sistemas de deteção e/ou prevenção de intrusões destinados a utilização industrial;
5. Microprocessadores de uso geral;
6. Microprocessadores destinados a integração em controladores lógicos programáveis e em elementos seguros;
7. Encaminhadores, modems para ligação à Internet e comutadores destinados a utilização industrial;
8. Elementos seguros;

9. Módulos de segurança físicos (HSM);
10. Criptoprocessadores seguros;
11. Cartões inteligentes, leitores de cartões inteligentes e dispositivos de autenticação;
12. Sistemas de controlo da automação industrial (IACS) destinados a serem utilizados por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)], tais como controladores lógicos programáveis (PLC), sistemas de controlo distribuído (DCS), controladores numéricos computorizados (CNC) para máquinas-ferramentas e sistemas de supervisão, controlo e aquisição de dados (SCADA);
13. Dispositivos da Internet das coisas industrial destinados a serem utilizados por entidades essenciais do tipo referido no [anexo I da Diretiva XXX/XXXX (SRI 2)];
14. Componentes de sensores e acionadores de robôs e controladores de robôs;
15. Contadores inteligentes.

Apêndice E
Questionário eVotUM - 05/09/2023

Neste anexo estão as notas da reunião de 5 de setembro de 2023. As informações aqui contidas não representam uma transcrição exata do que foi dito, pois são notas pessoais escritas durante a reunião.

O interveniente nesta reunião é o *Senior Software Developer* Sandro Rodrigues.

1. Autorizas que o teu nome seja mencionado na minha tese como a fonte destas respostas?

   Sim.

2. Qual é a relação entre o eVoto e a Dipcode/Eurotux?

   A Universidade do Minho é em parte a detentora do eVotUM, no entanto o eVoto SaaS será um produto unicamente da Eurotux.

3. É a Dipcode/Eurotux que realiza a gestão técnica (suporte, infraestrutura)?

   Sim.

4. A Dipcode/Eurotux pode criar eleições e gerir todo o processo eleitoral associado? Ou seja, os clientes podem pedir que a empresa faça toda a parte de administração de uma eleição?

   Não, nem nos é possível, por uma questão de separação de responsabilidades.

5. É possível exportar os dados de uma eleição para um ficheiro csv/xls/txt?

   Não.

6. O eVotUM apresenta relatórios ou análises em tempo real? Por exemplo, quantos votos foram submetidos neste preciso momento, antes do fecho da eleição.

   Sim, a comissão eleitoral pode consultar votos já submetidos, algo que se chama uma "contagem parcial".

7. É automaticamente enviado um email/notificação ao eleitor quando um passo da eleição é dado (abertura, envio de voto, fecho, etc)?

   Sim, no fim da votação o utilizador recebe um email com a referência de voto, o resto é através da funcionalidade de mensagens do eVotUM.

8. Já foi realizado o plano de mensalidades/subscrições/pagamentos para o eVoto?

   Parcialmente. Apenas que vai ser mensal, ainda não foram definidos preços, nem possíveis categorias de subscrição.

Apêndice F
Análise Detalhada da certificação ISO/TS 54001:2019

Este documento detalha apenas os pontos mais importantes da análise ao ISO 54001 juntamente com algumas notas pessoais. É importante esclarecer que **algumas informações foram omitidas**, e que **todo o texto em português foi traduzido por mim** e pode, por isso, **apresentar incongruências com o texto original.**

Especificamente recomenda o ISO/IEC 27000.

Financiamento de campanha é um documento que especifica as atividades, responsabilidades e recursos para monitorizar as finanças de campanhas políticas.

Educação eleitoral é dar a conhecer ao eleitor o processo eleitoral.

F.1 4. Context of the organization

- Understanding the organization

  [9001] A organização deve determinar os problemas internos (cultura, conhecimento, valores, performance) e externos (legal, tecnológico, competitivo, cultural, social, etc) relevantes para o propósito.

  O corpo eleitoral deve determinar, como parte de problemas externos:

  1. Alterações a leis que influenciem o funcionamento de processos eleitorais
  2. Assuntos orçamentais que influenciem o desenvolvimento do serviço eleitoral
  3. Outros problemas considerados pertinentes

- Understanding the needs and expectations of interested parties

  [9001] A organização deve determinar: (1) as partes interessadas relevantes ao sistema de gestão de qualidade, (2) os requisitos destas partes interessadas que são relevantes para o sistema de gestão de qualidade.

  O corpo de gestão eleitoral deve identificar as necessidades e as expectativas das partes interessa-

das que sejam relevantes para o sistema de gestão de qualidade. Uma sugestão para definir estas partes interessadas é a utilização do ISO/TS 9002:2016.

  - O eVoto já tem estas entidades definidas: responsável institucional, comissão eleitoral, eleitor, público, administrador técnico.*

- Determining the scope of the quality management system

  A norma é aplicável a eleições em todos os níveis do governo.

  Os requisitos definidos neste documento aplicam-se a:

  1. registo de eleitor
  2. registo de organizações políticas e candidatos
  3. logística eleitoral
  4. lançamento de votos
  5. contagem de votos e declaração de resultados
  6. educação eleitoral
  7. supervisão de financiamento de campanha
  8. resolução de litígios eleitorais

  » O eVoto implementa todos os pontos exceto: educação eleitoral (6) e supervisão de financiamento de campanha (7).

- Quality management systems and its processes

  Devem ser asseguradas tanto justiça como imparcialidade nas eleições. O corpo eleitoral deve implementar ações para assegurar a integridade do serviço eleitoral, para assegurar a observação desimpedida do processo eleitoral por indivíduos acreditados, e para prevenir abuso.

  O corpo eleitoral deve determinar os limites e a aplicabilidade do sistema de gestão de qualidade eleitoral para definir o seu âmbito.

  Incluindo os processos para o sistema já definidos no 9001, adicionam-se: processos para atividades de gestão, provisão de recursos, execução, medição, análise e melhoramento.

F.2 5. Leadership

- Leadership and commitment - General

- Leadership and commitment - Customer focus

Para além de eleitores, candidatos, e organizações políticas, o corpo eleitoral pode identificar outras entidades como clientes eleitorais.

» O eVoto já define tal. Ver acima.

- Policy - Establishing the quality policy
- Policy - Communicating the quality policy

[9001] Definição de uma política de qualidade.

A política de qualidade eleitoral deve (1) estar disponível como informação documentada e (2) disponível para partes interessadas, quando apropriado.

» Por exemplo, basta ter a política de qualidade

- Organizational roles, responsibilities and authorities

[9001] A gestão deve assegurar que as responsabilidades e autoridades de diferentes cargos são definidos, comunicados, e percebidos.

Antes do processo eleitoral:

1. As responsabilidades e autoridades devem ser comunicadas dentro do corpo eleitoral
2. As responsabilidades devem ser implementadas
3. Os clientes eleitorais são informados da divisão de responsabilidades

» O eVoto já realiza isto automaticamente, através de perfis de utilizador e do registo correto de tais. Candidatos são registados como candidatos, eleitores como eleitores, etc, e automaticamente já detém das permissões e responsabilidades adequadas.

F.3 6. Planning

- Actions to address risks and opportunities

A gestão deve assegurar que (1) o planeamento do sistema de gestão de qualidade eleitoral inclui planeamento para todos os processos eleitorais e (2) todo o planeamento e todos os processos protegem os direitos fundamentais dos clientes eleitorais.

» Isto já está a ser feito automaticamente uma vez que é o próprio administrador que define o planeamento do processo eleitoral, por exemplo, ao definir as datas de cada uma das etapas e ao definir as caraterísticas de cada uma das eleições.

- Quality objectives and planning to achieve them
- Planning of changes

F.4 7. Support

- Resources - General
- Resources - People
- Resources - Infrastructure - General
- Resources - Infrastructure - Infrastructure for voter registration and registration of political organizations and candidates

  A gestão deve especificar os requisitos para o sistema de informação necessários para suportar os processos eleitorais de (1) registo de eleitores e (2) registo de organizações políticas e candidatos, incluindo:

  1. Integridade e disponibilidade de dados
  2. Segurança de informação
  3. Problemas de privacidade e confidencialidade
  4. Informação pessoal dos eleitores

  Sugere ver ISO/IEC 27000 para diretrizes sobre isto.

  » Analisar a arquitetura para confirmar que tal já está a acontecer.

- Resources - Infrastructure - Infrastructure for electoral logistics

  O plano de desenvolvimento deve especificar requisitos mínimos para (1) a segurança e neutralidade física do local de voto e (2) o equipamento do processo, incluindo o equipamento de voto.

  Caso o equipamento seja considerado não conforme, deve ser terminado de acordo com requisitos definidos numa outra secção.

  » Este é mais complicado, pois é difícil como é que se poderia adaptar esta cláusula a voto online considerando que não temos acesso aos dispositivos pessoais das pessoas que utilizam o eVoto.

- Resources - Infrastructure - Infrastructure for vote casting

  O corpo eleitoral deve tomar medidas razoáveis para assegurar que pessoas portadoras de deficiência e com necessidades especiais têm acesso ao equipamento de voto.

*» O facto de que o eVoto é online mais do que confirma este ponto uma vez que não há nada mais acessível do que um telemóvel pessoal já personalizado pela própria pessoa para as suas necessidades.

As minhas sugestões são: garantir que o eVoto (1) é acessível a screen readers, (2) não necessita de muita destreza (p.e. pessoas com tremores de mãos), (3) é acessível apenas por teclado, (5) possui modo de alto contraste, (6) possui modo para daltonismo, (7) indique o foco do cursor claramente. Também não se deve ignorar as traduções (já implementadas). Embora muito mais complicado, também poderia ser interessante fornecer um serviço de suporte em formato de chatbot (recomendo vivamente ver a implementação do chatbot do https://electionbuddy.com/). Isto podia eventualmente estar ligado a/ser um projeto-teste para uma implementação empresarial do ChatGPT que se tem vindo a falar.

Acho que tentar comercializar o eVoto como sendo um sistema de voto altamente acessível (acima do normal) podia ser uma mais valia, especialmente considerando que o voto é um direito humano básico. Também não se pode negar que é uma situação *win-win*: o maior número possível de pessoas tem acesso à plataforma, a empresa recebe boa publicidade, e os seus colaboradores melhoram as suas capacidades de garantir acessibilidade de software num mundo cada vez mais informatizado.*

- Resources - Infrastructure - Infrastructure for vote counting and declaration of results

  O corpo eleitoral deve definir os requisitos mínimos para (1) a segurança física e a neutralidade dos locais de contagem de votos, (2) a proteção dos materiais eleitorais (p.e. os boletins antes e depois do dia da eleição), (3) sistemas para comunicar os resultados.

  » Considero que estes 3 pontos são cumprido através das medidas de segurança e proteção do servidor (quer a sala de servidores da Eurotux, quer um serviço como a AWS ou a Google Cloud).

- Resources - Environment for the operation of processes

  O corpo eleitoral é responsável pelo cumprimento de normas de segurança de construção, saúde, segurança, ambientais, e protocolos de segurança física.

  para o ambiente de trabalho aplicável às localizações de voto, corpo eleitoral deve especificar no plano de desenvolvimento eleitoral os seguintes requisitos:

  1. Espaço de armazenamento para todo o material eleitoral
  2. A colocação e separação mínima de estações de voto

3. Infraestrutura física adequada a operação contínua e eficaz
4. Acesso a pessoas portadoras de deficiência
5. Saída e entrada do local de voto desimpedidos, para eleitores e para os trabalhadores
6. Sinalização adequada para identificar locais de voto

» Mais uma vez, esta cláusula aplica-se especificamente a voto físico e a sua interpretação precisa especial atenção. Uma conversa com alguém com experiência com a linguagem de certificações poderá ser benéfico, para perceber como é que esta cláusula pode ser cumprida no contexto do eVoto.

- Resources - Monitoring and measuring resources - General

- Resources - Monitoring and measuring resources - Measurement traceability

  O equipamento de voto deve (1) estar protegido de ajustes que possam invalidar o resultado do voto e (2) ser auditado por uma autoridade competente, independente, e apartidária.

  Quando é descoberto que o equipamento não está conforme, deve ser pensada e documentada a validade de resultados prévios. Devem ser tomadas as ações apropriadas em relação ao equipamento defeituoso.

  » Práticas padrão de cibersegurança asseguram o ponto (1), e o ponto (2) é assegurado através de auditorias ao sistema. Ambos já são feitos.

  Quando utilizado em equipamento de voto, deve ser confirmada a capacidade do software de satisfazer a sua tarefa pretendida. Esta confirmação deve ser feita antes do primeiro uso e re-confirmado conforme necessidade.

- Resources - Organizational knowledge

- Competence - General

- Competence - General for the electoral body

  Os trabalhadores do corpo eleitoral deve ter educação, treino ou experiência adequados e devem ser selecionados através de um processo de recrutamento competitivo público e baseado em competências.

  O corpo eleitoral deve definir os cargos e a educação, treino ou experiência adequados a cada cargo.

» Mesmo problema em relação a ser uma definição para eleições físicas. Se esta clausula for vista do ponto de vista de uma entidade como por exemplo a Universidade do Minho, já faz mais sentido.

- Competence - Education and training of poll workers

  Os trabalhadores devem ter concluído o treino para o seu cargo na sua totalidade, e a educação e treino devem ser regulares.

  » Ponto anterior.

- Awareness

  O corpo eleitoral deve ter um processo para monitorizar o quanto os trabalhadores estão cientes do que contribuem para atingir os objetivos de qualidade do processo eleitoral.

  » Ponto anterior.

- Communication

- Documented information - General

  [9001] A organização deve possuir a documentação pedida pelo International Standard e documentação necessária ao sistema de gestão de qualidade.

  O corpo deve criar e manter documentação que inclui:

  1. Uma declaração explícita do âmbito do sistema de gestão da qualidade eleitoral, incluindo uma declaração que identifique os processos eleitorais que estão no âmbito da implementação deste documento;
  2. A especificação para um plano de desenvolvimento do serviço eleitoral para controlar a criação, desenvolvimento e prestação do serviço eleitoral, ou referência ao mesmo.

  A extensão da documentação varia conforme o âmbito do sistema de qualidade.

- Documented information - Creating and updating

- Documented information - Control of documented information

  A informação documentada necessária pela gestão de qualidade eleitoral deve estar de acordo com ISO 9001/2015.

  » Certificar que a Eurotux cumpre a versão de 2015.

- Documented information - Minimum documentation requirements - General

  Os documentos da documentação eleitoral devem:

  1. Mostrar um identificador único e número de revisão
  2. Incluir um título
  3. Ser identificados com data de emissão
  4. Anexar assinaturas de aprovação ou autenticação equivalente
  5. Ser submetido a controlos que impeçam do seu uso de ser tornado obsoleto ou substituído, e ter identificação adequada caso sejam retidos por algum propósito.

- Documented information - Minimum documentation requirements - For voter registration

  Definição de um documento com:

  1. Os requisitos mínimos para o registo de um individual
  2. Os métodos de identificação que devem ser seguidos quando é feito o registo ou a atualização de um registo de um eleitor.

- Documented information - Minimum documentation requirements - For the registration of political organizations and candidates

  Definição de um documento que define os requisitos para:

  1. O formulário de candidatura oficial
  2. O registo de registos
  3. O instrumento e a documentação de apoio devem ser apresentados para registar um desafio
  4. As circunstâncias sob as quais um partido político pode ter o seu registo cancelado

  » Desafio é uma reclamação.

- Documented information - Minimum documentation requirements - For electoral logistics

  Criação de um documento que define as instruções de trabalho e provisionamento, staffing, e configuração do local de voto, incluindo:

  1. Configuração do local de voto
  2. Diretrizes para a compra transparente de materiais eleitorais
  3. Garantia dos materiais eleitorais antes da abertura do local de votação e durante e após a votação
  4. Instalação e teste de voto eletrónico

5. Criação e atualização de mapas eleitorais
6. Identificação, seleção e treino de autoridades eleitorais

» Novamente, o problema da eleição física.

- Documented information - Minimum documentation requirements - For vote casting

  Definição de um documento com instruções para:

  1. Confirmação de registo de voto antes da votação
  2. Monitorização do local de voto durante o período de votação
  3. Gravação de incidentes de voto

  » Mesmo problema da eleição física para o ponto 2. Os pontos 1 e 3 já são feitos pelo eVoto, através da consulta de cadernos eleitorais e através da existência de logs, respetivamente.

- Documented information - Minimum documentation requirements - For vote counting and the declaration of results

  Definição de um documento com instruções e critérios que assegurem a integridade da contagem, incluindo:

  1. Publicação pública dos resultados
  2. Declaração de disputas processuais-eleitorais observadas (documentos de desafio/contestação)
  3. Declaração de resultados

  » Levantam-se questões de privacidade considerando que vários serviços vão querer utilizar este serviço e podem não querer que as suas eleições sejam públicas para o público em geral.

- Documented information - Minimum documentation requirements - For electoral education

  Definição de um documento que especifica:

  1. Um plano de educação eleitoral que documenta o propósito, estratégia, audiência, abordagem, recursos, responsabilidades e agenda para o programa de educação eleitoral
  2. Quaisquer procedimentos e instruções necessárias à implementação do plano educacional

  » Educação eleitoral significa dar a conhecer aos cidadãos o sistema eleitoral e os seus processos.

- Documented information - Minimum documentation requirements - For the oversight of campaign financing

O corpo eleitoral deve estabelecer e manter um plano documentado para a supervisão de financiamento de campanha que define as responsabilidades e requisitos para planear e executar o financiamento da campanha, estabelecer registos, e reportar resultados.

» Investigar se isto é aplicável ao eVoto.

- Documented information - Minimum documentation requirements - For the dispute resolution

  Definir um documento que especifica os processos e instruções de trabalho necessários à resolução de uma disputa eleitoral. Os processos devem descrever o processo de criação de uma disputa e devem incluir a data, a localização e o tipo da disputa e as partes interessadas nela.

  Recomenda-se ISO 10003 que oferece firetrizes para a resolução de uma disputa.

  » A possibilidade de envio de reclamações e consequente resolução na Eurotux/no cliente deve satisfazer esta cláusula.

- Documented information - Control of records

  Todos os registos que suportem procedimentos legais devem ser identificados e controlados.

- Documented information - Minimum records requirements - General

  Todos os registos identificados na documentação eleitoral devem ter (1) um identificador único, (2) data de execução, (3) assinatura ou equivalente da entidade que executou o registo.

  » Todos os registos devem ter esta informação. É uma questão de implementar.

- Documented information - Minimum records requirements - For voter registration

  O registo de eleitor deve ter, no mínimo:

  1. Primeiro e último nome
  2. Data de nascimento
  3. Local de nascimento
  4. Morada
  5. Identificação válida
  6. Eleitorado onde é feito o voto
  7. Género
  8. (opcional) Data de registo
  9. (opcional) Estado civil

» Seria necessário adicionar esta informação aos registos do eVoto. Atualmente o eVoto tem: nome, username, endereço de email pré-definido, número de telemóvel pré-definido, endereço de email para notificações, número de telemóvel para notificações, método de envio de chave de segurança. Este tipo de informação seria necessário para qualquer eleição governamental, embora não seja necessário para eleições simples sem um verdadeiro vínculo legal.

- Documented information - Minimum records requirements - For the registration of political organizations and candidates

  O processo eleitoral para o registo de organizações políticas e candidatos deve gerar uma lista de registo oficial como output do registo desse processo. O registo de cada organização deve ter:

  1. Artigos de incorporação (estatuto de companhia?)
  2. Declaração de princípios políticos ou plataforma política (ou referência a)
  3. Estados, leis ou processos (ou referência a)
  4. Nomes de autoridades/representantes
  5. Morada ou detalhes de contacto dos representantes
  6. *Endorsements* (assinatues ou outro)

  Cada candidato registado deve também incluir:

  1. Uma carta ou documento de *endorsement* de uma organização política (exceto independentes) ou os resultados oficiais de uma eleição primária
  2. Nome completo
  3. Número de identificação governamental
  4. Morada
  5. Prova de que cumpre os pré-requisitos estabelecidos pela lei (exceto independentes)

  O corpo eleitoral deve também estabelecer os requisitos para:

  1. O formulário de candidatura oficial
  2. O registo de registo, incluindo:
     1. Declaração específica se há requisito legais para quotas de registo de candidatos à base do género
     2. Declaração da percentagem de candidatos masculinos e femininos, caso requisitos legais existam
     3. A certificação de que as percentagens são cumpridas, caso requisitos legais existam

3. A documentação instrumental e a documentação de suporte a ser preenchida para uma disputa

» Teriam de ser adicionados campos para toda esta informação ao eVoto. Não é feita menção a candidatos cujo género não seja masculino ou feminino.

- Documented information - Minimum records requirements - For the electoral logistics

  O processo de logísticas eleitorais deve produzir um registo que confirma que o local de voto foi completado. Deve incluir:

  1. Identificador único à estação de voto
  2. Localização do loca de voto
  3. Lista de trabalhadores do local de voto
  4. Número de eleitores registados por local de voto
  5. Número de estações de voto por localização de voto
  6. Referência à configuração de instruções de trabalho
  7. Uma declaração de que o local de voto foi executado conforme descrito

  Também deve declarar que todos os trabalhadores foram devidamente treinados, incluindo informação pessoal relativa ao trabalhador (nome, currículo, treino, data do treino, confirmação de treino).

  » Levanta-se novamente a questão da eleição online vs física.

- Documented information - Minimum records requirements - For vote casting

  O lançamento de voto deve assegurar o boletim secreto e deve produzir um registo de voto para cada localização de voto, com a seguinte informação por cada eleitor:

  1. Nome
  2. Identificador único de eleitor
  3. Data do lançamento do voto
  4. Assinatura do eleitor ou semelhante (por exemplo, fotos, ou dados biométricos)

  » Isto pode ser aplicado no contexto de um relatório de eleição, no entanto, não seria possível associar a localizações de voto.

- Documented information - Minimum records requirements - For vote counting and the declaration of results

A contagem de votos deve produzir um documento com a seguinte informação, para cada estação de voto e para cada proposta de boletim:

1. Identificador único da estação de contagem
2. Número de eleitores que votaram
3. Número de votos por organização/candidato
4. Número de boletins válidos
5. Número de boletins rejeitados
6. Número de boletins em branco
7. Número de boletins recebidos pela estação de contagem
8. Declaração oficial de que a contagem foi feita de modo legal
9. (opcional) Número de boletins não utilizados

» Mais uma vez, no eVoto não existem estações de contagem (nem de voto), no entanto pode ser possível emitir um relatório com esta informação, disponível ao responsável pelo respetivo processo eleitoral.

- Documented information - Minimum records requirements - For electoral education

  O processo da educação eleitoral deve produzir todos os registos especificados para o processo.

  » Conforme como se aplica a educação eleitoral no eVoto.

- Documented information - Minimum records requirements - For the oversight of campaign financing

  Mínimo: registos das auditorias e dos seus resultados.

  » Conforme se aplica (ou não) o financiamento de campanha no eVoto.

- Documented information - Minimum records requirements - For dispute resolution

  O processo de resolução de uma disputa deve produzir um documento que inclui, no mínimo:

  1. O pedido de resolução (com data, localização, tipo, e partes interessadas)
  2. A resolução adotada
  3. A razão para a decisão
  4. As provas oferecidas
  5. Aviso da resolução

  » Adaptar ao sistema de reclamações do eVoto.

F.5 8. Operation

- Operational planning and control

  A organização deve assegurar que os processos eleitorais que são *outsourced* estão controlados. Deve produzir um plano de desenvolvimento de serviço eleitoral de uma forma adequada ao modo de operações do corpo eleitoral.

- Requirements for products and services - Customer Communication

- Requirements for products and services - Determining the requirements for products and services

- Requirements for products and services - Review of the requirements for products and services

  Os recursos provenientes de avaliações de requisitos devem incluir (1) as questões abordadas durante a avaliação e (2) quaisquer decisões tomadas.

- Requirements for products and services - Changes to requirements for products and services

- Design and development for products and services - General

- Design and development for products and services - Design and development planning

  O corpo eleitoral deve documentar o plano de desenho e o desenvolvimento dentro do plano para o desenvolvimento do serviço eleitoral que especifica:

  1. As etapas de desenho e desenvolvimento e os respetivos documentos *inputs* e *outputs*
  2. Os processos de avaliação, verificação e validação necessários para cada etapa do desenvolvimento
  3. Recursos necessários ao desenho e desenvolvimento
  4. Agenda à base de atividades para o desenho e desenvolvimento

  » Considero que a Eurotux já faz isto com, por exemplo, os planeamentos de sprint.

- Design and development for products and services - Design and development inputs

- Design and development for products and services - Design and development controls

  Registos de avaliações de desenho e desenvolvimento devem incluir:

  1. Questões abordadas durante a avaliação do desenho e do desenvolvimento
  2. Todas as decisões tomadas para assegurar o cumprimento do desenho e desenvolvimento

Os registos dos resultados da avaliação devem incluir (1) questões identificadas durante a verificação e (2) as ações necessárias a tomar para resolver essas questões.

- Design and development for products and services - Design and development outputs
- Design and development for products and services - Design and development changes
- Control of externally provided processes, products and services - General
- Control of externally provided processes, products and services - Type and extent of control
- Control of externally provided processes, products and services - Information for external providers
- Production and service provision - Control of production and service provision

  O corpo eleitoral deve documentar os requisitos para os controlos do serviço de provisionamento no documento referente ao planeamento do serviço eleitoral.

  As condições de controlo incluem (se aplicável):

  1. A implementação de atividades de lançamento, entrega e seguimento do serviço eleitoral
  2. Monitorização de eleições por autoridades adequadas
  3. Acesso a todos os aspetos do processo eleitoral, contratualmente combinados.

  » É mais do que possível aplicar esta cláusula a eleições online.

- Production and service provision - Identification and traceability
- Production and service provision - Property belonging to customers or external providers
- Production and service provision - Preservation
- Production and service provision - Post-delivery activities
- Production and service provision - Control of changes
- Release of products and services
- Control of nonconforming outputs

  O corpo eleitoral deve assegurar que são identificadas e controladas quaisquer incongruências relativas ao serviço eleitoral, equipamento de voto, processo de voto, atividades relacionadas com o voto e materiais eleitorais.

O corpo eleitoral deve definir as autoridades e respetivas responsabilidades para lidar com incongruências.

» Enquanto que não haveria possibilidade de interagir com o equipamento de voto (dispositivo pessoal do eleitor) o resto parece ser atingível.

O corpo eleitoral deve sinalizar e invocar controlos físicos para prevenir o uso de materiais de eleição defeituosos.

» Não é possível invocar controlos "físicos" muito mais do que bloquear o voto a um eleitor que não tenha, por exemplo, um dispositivo funcional ou, um outro exemplo, bloquear uma eleição porque se suspeita de fraude, ou algum procedimento semelhante. Apenas uma sugestão para tentar cumprir esta cláusula.

F.6 9. Performance Evaluation

- Monitoring, measurement, analysis and evaluation - General
- Monitoring, measurement, analysis and evaluation - Customer satisfaction

  Recomendam obter informação do eleitor através de um levantamento de opiniões.

  » Seria interessante implementar, por exemplo, um pop-up que apareceria ao eleitor depois do lançamento e registo do voto a pedir para classificar a aplicação. Isto podia ser aplicado apenas a uma parte do corpo eleitoral, ou apenas durante um intervalo de tempo, ou apenas para a primeira eleição de uma dada conta.
- Monitoring, measurement, analysis and evaluation - Analysis and Evaluation
- Monitoring, measurement, analysis and evaluation - Internal audit

  O corpo eleitoral deve realizar várias auditorias internas para determinar se o sistema de gestão de qualidade eleitoral está conforme as obrigações legais para eleições democráticas.

  » Do que consegui pesquisar, não existem leis específicas para eleições online, para além de leis e regulamentos mais gerais como o GDPR e coisas mais óbvias, como os direitos humanos.
- Management review - General
- Management review - Management review inputs
- Management review - Management review outputs

F.7 10. Improvement

- General
- Nonconformity and corrective action
- Continual improvement

Apêndice G
Diagrama de estados do processo eleitoral no eVotUM

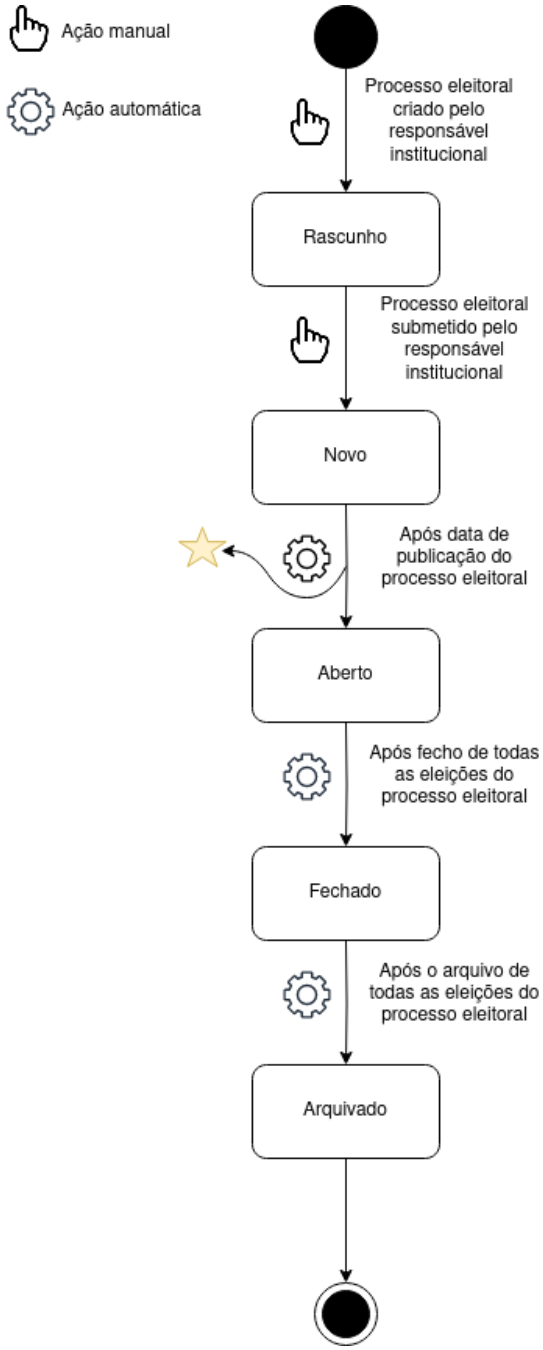


Figura 24: Diiagrama de estados do processo eleitoral.

Apêndice H
Diagrama de estados de uma eleição no eVotUM

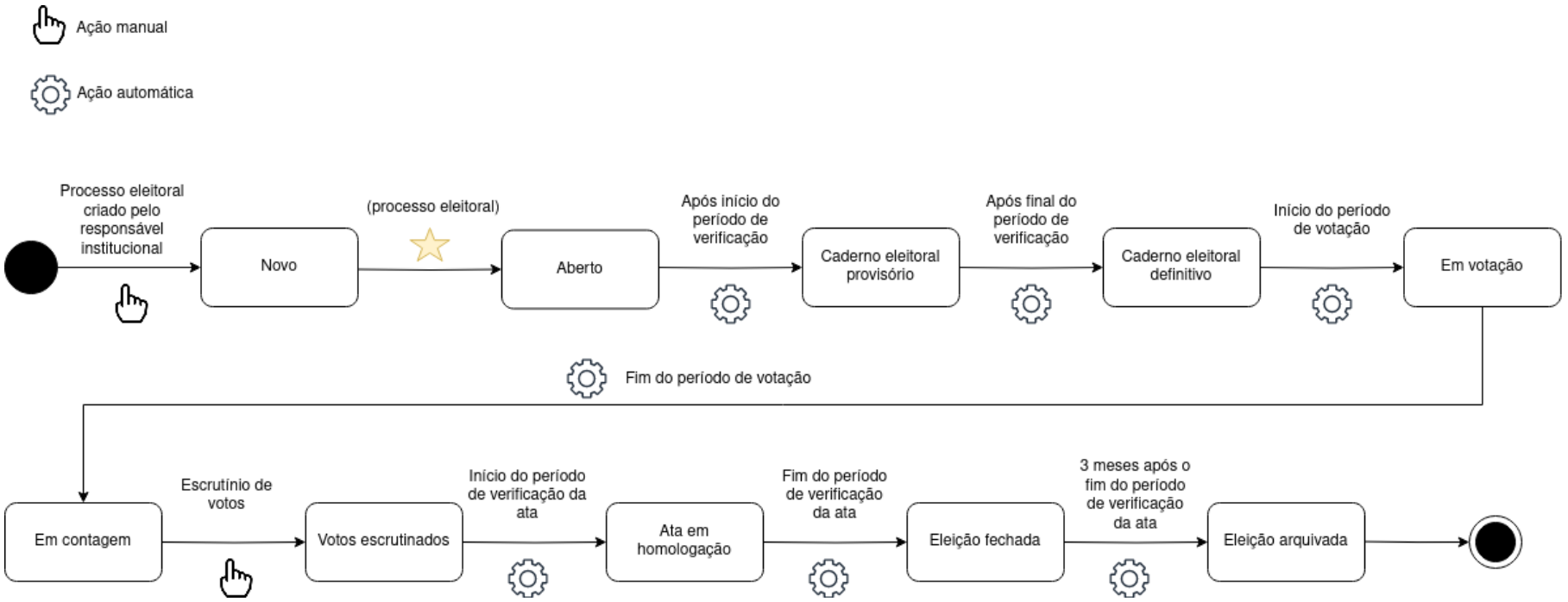


Figura 25: Diagrama de estados de uma eleição.

Apêndice I
CRA - Palestra FOSDEM 2024

Este apêndice contém o power-point apresentado pelos autores da Lei de Resiliência Cibernética, durante a palestra na FOSDEM 2024.

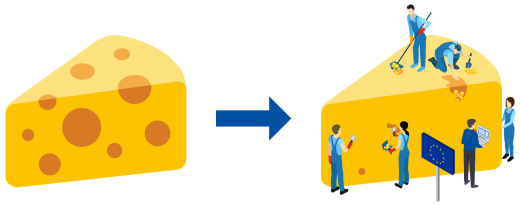
Os autores são: Simon Phipps, Enzo Ribagnac, Gaël Blondelle, Benjamin Bögel, e Omar Ennaji.

Também está disponível para consulta no link https://fosdem.org/2024/events/attachments/fosdem-2024-3683-the-regulators-are-coming-one-year-on/slides/22201/Slides_CRA_FOSDEM_v3_ukPnQUG.pdf.

Cyber Resilience Act

Benjamin Bögel
European Commission, DG CONNECT

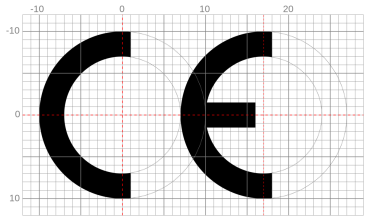
CRA in a nutshell



Main elements of the law

- **Cybersecurity rules** for the placing on the market of hardware and software
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Reporting** obligations
- **Market surveillance and enforcement**

CE marking



In scope: “products with digital elements”

✓ **Hardware products** (including components placed on the market)
(laptops, smart appliances, mobile phones, network equipment or CPUs…)

✓ **Software products** (including components placed on the market)
(operating systems, word processing, games or mobile apps, software libraries…)

…including their **remote data processing solutions**!

Outside the scope

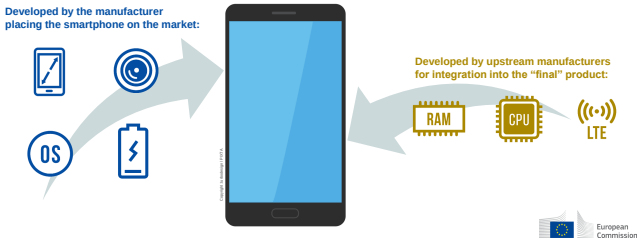
✗ **Non-commercial products**
(hobby products)

✗ **Services, in particular standalone SaaS** (covered by NIS2)
(websites, purely web-based offerings…)

✗ **Outright exclusions**
(cars, medical devices, in vitro, certified aeronautical equipment, marine equipment)

A simplified example of smartphones

*As a rule, whoever places on the market a **“final” product or a component** is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking.***



Conformity assessment – risk categorisation

Default category — self-assessment
(memory chips, mobile apps, smart speakers, computer games...)

Important products — application of standards/third-party assessment
(operating systems, anti-virus, routers, firewalls…)

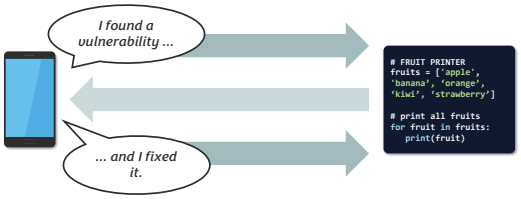
Critical products — in the future potentially certification
(smart cards, secure elements, smart meter gateways…)

FOSS — self-assessment (unless categorized as “critical products”)
(web development frameworks, operating systems, database management systems…)

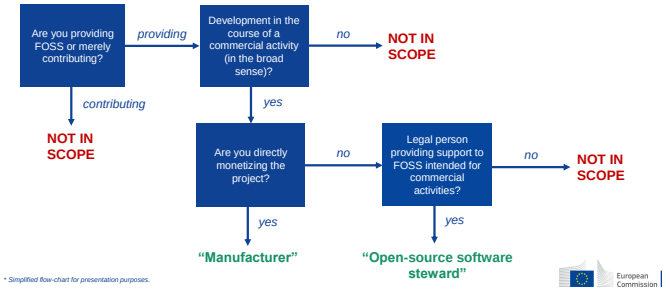
Sharing the responsibility

Sharing the responsibility

Sharing the responsibility



Is your open-source project covered?*



* Simplified flow-chart for presentation purposes.

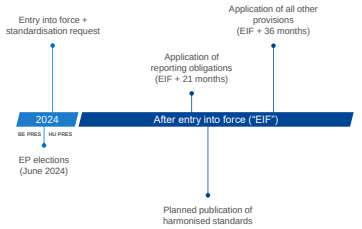
Open-source software steward

- **Light-touch approach** for legal persons that do not directly monetise but *"support on a sustained basis the development of specific [FOSS] products [..] intended for commercial activities"*.
- **Examples:**
  - Foundations supporting specific FOSS projects
  - Companies that build FOSS for their use but make it public
  - Not-for-profit entities that develop FOSS

Obligations of the stewards

- Put in place a **cybersecurity policy** taking into account the specific nature of the open-source software steward
- Cooperate with **market surveillance authorities**
- **Report incidents and vulnerabilities** to the extent that they are involved in the development

Tentative timeline



Thank you.

Coloque aqui informação sobre financiamento, projeto FCT, etc. em que o trabalho se enquadra. Deixe em branco caso contrário.