

# Universidade de Aveiro

## DETI

---

# Aspetos Profissionais e Sociais para Engenharia Informática

TRABALHO 4

PROJETO FINAL

2023-2024

---

### **Docentes:**

Professor Rui L. Aguiar

### **Alunos:**

Daniel Madureira - 107603

Diogo Falcão - 108712

João Luís - 107403

José Gameiro - 108840

Pedro Ramos - 107348

Rodrigo Aguiar - 108969

Maio de 2024

# Conteúdos

---

<b>1. Contexto</b>	<b>2</b>
1. Introdução . . . . .	2
2. Projeto em Informática . . . . .	2
<b>2. Ecosistema</b>	<b>4</b>
1. Introdução e Clientes esperados . . . . .	4
2. Empresas fornecedoras . . . . .	4
3. Competição e fatores diferenciadores . . . . .	5
4. Enquadramento regulatório associado . . . . .	6
5. Efeito de escala e os seus resultados . . . . .	8
<b>3. Propriedade Intelectual</b>	<b>9</b>
1. Introdução . . . . .	9
2. Direitos de Autor . . . . .	9
3. Marcas Registadas . . . . .	10
3. Patentes . . . . .	10
<b>4. Software Open Source</b>	<b>12</b>
1. Uso no Projeto . . . . .	12
2. Licenciamento . . . . .	14
3. Impacto no produto . . . . .	15
<b>5. Cibersegurança</b>	<b>16</b>
1. Ataques . . . . .	16
2. Implementação da defesa . . . . .	17
3. Planos de recuperação . . . . .	18
4. Legislação de cibersegurança . . . . .	19
<b>6. Privacidade</b>	<b>20</b>
1. Efeitos no projeto . . . . .	20
2. Minimizar os problemas de privacidade . . . . .	21
3. Soluções técnicas . . . . .	22
4. Implementação de um serviço de resposta a pedidos legais . . . . .	23
<b>7. Aspetos éticos</b>	<b>24</b>
1. Aspetos éticos a considerar . . . . .	24
2. Regulações a cumprir . . . . .	25
<b>8. Aspetos de Inteligência Artificial</b>	<b>26</b>
1. Integração no serviço . . . . .	26
<b>9. Hyperscalers</b>	<b>27</b>
1. Relações com Hyperscalers . . . . .	27
2. Efeitos da legislação europeia sobre estes serviços . . . . .	28
<b>10. Efeitos no sistema</b>	<b>29</b>
1. Introdução . . . . .	29
2. Efeitos do sistema na rede onde foi integrado . . . . .	31
3. Ações para aumentar o sucesso do sistema . . . . .	32
4. Efeitos negativos da rede . . . . .	33
<b>Referências</b>	<b>34</b>

# 1. Contexto

---

## 1.1 Introdução

No âmbito do quarto trabalho da cadeira Aspectos Profissionais Sobre Engenharia Informática (APSEI), analisamos o nosso Projeto em Informática (PI) tendo em conta as diversas valências dos tópicos abordados durante as aulas. Assim, passamos a apresentar brevemente o projeto, considerando que este seria comercializado em grande escala, que incide sobre uma reformulação da plataforma Distribuição de Serviço Docente (DSD).

## 1.2 Projeto em Informática

O nosso PI focou-se numa renovação complexa da plataforma Distribuição de Serviço Docente (DSD), plataforma utilizada pelo Departamento de Elettónica, Telemática e Informática (DETI) para gerir o processo de publicação e escolha de dissertações, projetos e estágios, entre outras funcionalidades que caíram em desuso ao longo dos anos.

Para além disso, o nosso projeto visou resolver lacunas, apresentando novas funcionalidades que não existiam na plataforma antiga, evitando ter que fazer alterações diretas no código, e apresentando ainda um novo ator interveniente, o Diretor de Curso.

Simultaneamente, o sistema foi desenvolvido em tecnologias mais recentes, sendo a manutenibilidade do código um dos aspetos mais importantes do projeto.

Desta forma, através de um processo de levantamento de requisitos detalhado e contínuo, foi desenvolvido um sistema totalmente novo, acompanhado por uma interface moderna adaptada aos dias de hoje e otimizada para dispositivos móveis, sem perder sua plasticidade para alunos e professores.

A arquitetura geral do sistema é composta pelos seguintes módulos :

- Web Application ( React + Vite )
- Reverse Proxy and Web Server ( NGINX )
- Backend API ( FastAPI, python )
- Storage Layer ( MongoDB + MariaDB + File Storage )
- Serviços Externos ( IDP UA + Mail Server )

Um diagrama da arquitetura do sistema poderá ser visto na figura abaixo.

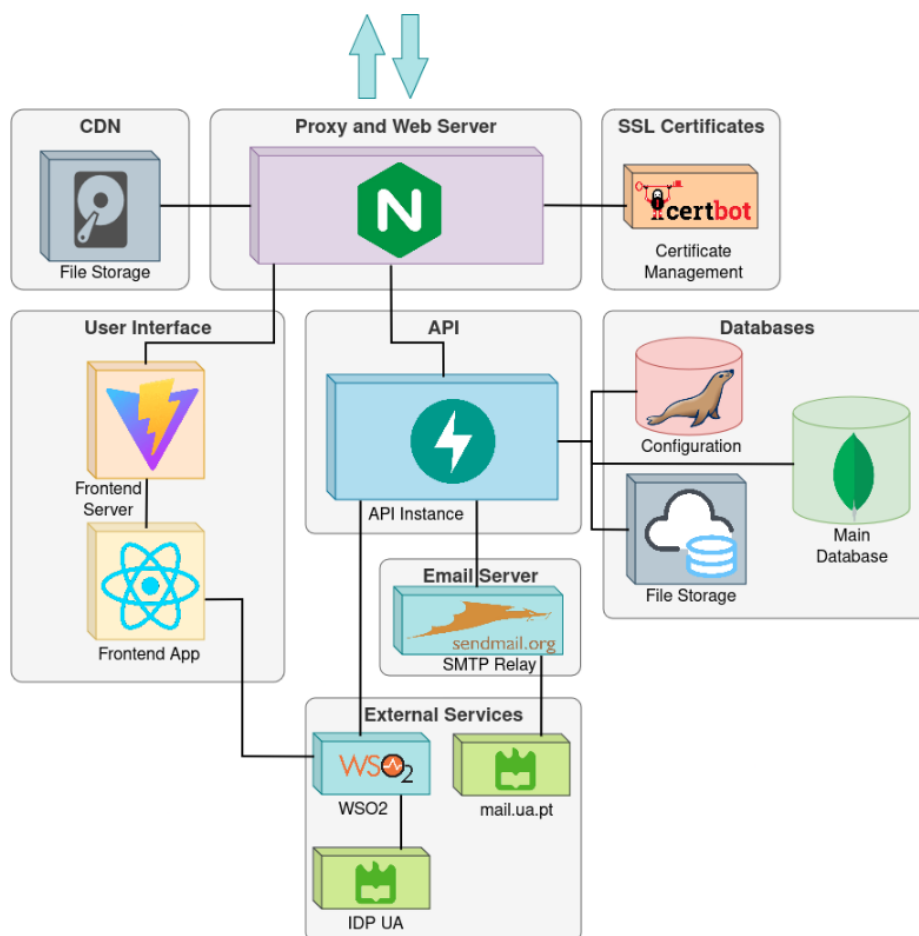


Figura 1: Arquitetura do sistema

Ao utilizar a nossa aplicação, um utilizador interage com a camada de User Interface através de um Reverse Proxy, que media também a interação da mesma com a API.

A API por sua vez comunica de volta com a User Interface, obtendo os dados necessários para as respostas através da interação com a camada de persistência, constituída por duas bases de dados e o sistema de ficheiros local.

A base de dados MongoDB armazena a maioria da informação necessária para o funcionamento da aplicação, tal como informações sobre os utilizadores ou sobre as dissertações publicadas, enquanto a base de dados MariaDB é utilizada para guardar configurações e variáveis secretas da aplicação.

O sistema de ficheiros locais é utilizado para guardar os documentos enviados ( pdf's de dissertações submetidas , imagens, entre outros documentos ).

Para autenticação, é utilizado o Identity Provider (IDP) da Universidade de Aveiro (UA), utilizando o WSO2 de forma a ter uma interface OAuth 2.0 sobre o IDP, para uma autenticação mais segura e uniforme, uma vez que o protocolo OAuth é um dos mais utilizados atualmente.

Por último, é ainda utilizado o serviço de emails da UA para notificar os utilizadores de situações importantes no sistema e que requerem a ação do utilizador, com a conexão ao serviço sendo feita pelo servidor Sendmail.

Esta arquitetura foi elaborada tendo em mente principalmente a performance e a manutenibilidade da solução, utilizando frameworks atuais e de alto nível para que possa ser mantida futuramente.

## 2. Ecossistema

---

### 2.1 Introdução e Clientes esperados

A comercialização do nosso projeto, posiciona-se num ecossistema educacional dinâmico.

Inicialmente, a plataforma está implementada no DETI, havendo uma possibilidade futura de expansão para outros departamentos da Universidade de Aveiro, como sistema único para gerir dissertações da Universidade.

Uma vez consolidada a plataforma dentro da universidade, o próximo passo é expandir este sistema para outras universidades.

Dadas as especificidades no processo de publicação e escolha de dissertações em cada universidade ou instituição de ensino superior e também a curta duração desta época, é necessário que este serviço se mostre flexível, podendo ser adaptado às necessidades específicas da instituição onde vai ser aplicado, e também altamente escalável, funcionando com alta performance tanto para uso num departamento como numa universidade com dezenas de milhares de alunos.

A nossa estratégia de comercialização dar-se-á através de um modelo de licenciamento, permitindo que instituições de educação superior adotem a nossa aplicação, fornecendo serviços de manutenção e suporte técnico. Também estaria incluído no serviço uma taxa inicial, calculada conforme as adaptações que fossem necessárias ser feitas para adaptar o serviço às especificações da instituição de ensino em questão.

### 2.2 Empresas fornecedoras

Dado toda a funcionalidade suportada pela aplicação, é necessário o uso de serviços de **fornecedores externos**, tanto de software como de infraestrutura.

A aplicação atual corre num servidor localizado no Instituto de Telecomunicações (IT), correndo instâncias locais de todos os serviços necessários, mostrando-se mais que necessário para servir as necessidades do DETI. Porém, uma expansão deste serviço sugeria a migração destes serviços para a cloud.

A utilização de soluções de armazenamento remotas facilitaria a integração do serviço em várias instituições e também permitiria ter uma solução de armazenamento mais fiável e tolerante a falhas.

Para isto, poderíamos recorrer a serviços externos como por exemplo instâncias de AWS EC2.

Este serviço fornece instâncias de máquinas virtuais que podem ser acedidas remotamente, com especificações personalizáveis, que poderiam ser ajustadas conforme as necessidades de espaço e de capacidade de processamento necessários.

Com uma infraestrutura escalável, confiável e segura, sendo a AWS a maior fornecedora de cloud services do mercado externo, poderíamos escalar a solução de armazenamento da aplicação para universidades com centenas de milhares de estudantes sem que tivéssemos de recorrer a armazenamento local, o que poderia ser custoso tanto em termos de hardware como de manutenção.

Migrar o serviço inteiro em si para a cloud também seria uma opção viável e necessária caso a instituição em questão não estivesse disposta a fornecer um servidor para hospedar o serviço ou caso um servidor local não conseguisse suportar todos os alunos com uma performance razoável.

Nestes casos, o custo destes serviços e infraestrutura seria repassado às instituições que utilizarem o nosso serviço. Enquanto que isto traria custos acrescidos, removeria a necessidade de criação e manutenção de infraestrutura local para suportar a aplicação, mostrando-se uma forma mais viável e potencialmente mais barata, tanto para a instituição em si como para a equipa de manutenção designada, dado que a integração com serviços externos removeria a necessidade de configuração local para cada instituição em que a aplicação fosse utilizada.

## 2.3 Competição e fatores diferenciadores

O **fator diferenciador** do nosso serviço consiste na capacidade de gestão de todo o processo de publicação e atribuição de dissertações numa só plataforma, uma vez que grande parte das instituições de ensino superior em Portugal ainda recorre a folhas de Excel ou emails para o mesmo processo.

Acompanhado de uma interface de utilizador moderna, responsiva e acessível, o nosso produto facilitaria o trabalho de vários tipos de utilizadores:

- Professores

Professores podem adicionar dissertações no website através de poucos cliques, disponibilizando a sua proposta para ser vista por qualquer aluno interessado.

Os professores também podem ver todas as dissertações que já submeteram e o estado das mesmas (alunos que mostraram interesse, se já foi estabelecido um acordo, etc...)

- Alunos

Alunos podem consultar rapidamente e numa interface apelativa todas as propostas de dissertações submetidas por professores, realizando todo o processo desde mostrar interesse numa dissertação até ao acordo final dentro da própria aplicação web.

- Funcionários das Secretarias

A plataforma eliminaria a necessidade de gestão manual das várias propostas e interesse nas mesmas através do uso de emails ou então através da consulta manual em ficheiros. A funcionalidade de exportar o estado das dissertações atual para um ficheiro Excel foi desenvolvida com este problema em mente, facilitando bastante o processo de trabalho por parte de funcionários de secretarias dos departamentos.

## 2.4 Enquadramento regulatório associado

Constituindo uma aplicação que lida com dados pessoais e académicos, a mesma cai sobre um **enquadramento regulamentar** restrito.

O uso e tratamento de dados pessoais exige o cumprimento das regulamentações locais, como por exemplo o Regulamento Geral de Proteção de dados Europeu.

Sendo assim, é necessário ter em considerações várias regras e leis na operação do serviço:

- Normas Internas da Instituição

É necessário garantir que o serviço cumpre as normas e leis internas da instituição em que está a ser utilizado, pelo que poderá ser necessário adaptar os processos existentes de submissão, aprovação e armazenamento das dissertações.

- Propriedade Intelectual

É necessário garantir que as dissertações submetidas não infringem algum contrato ou Propriedade Intelectual, ou que existe a opção de remoção nas mesmas nestes casos, quer seja pelo próprio orientador ou por um administrador da aplicação.

- Privacidade e Segurança

O sistema implementa um processo de autorização baseado em roles ( Role Based Access Control ) fornecidas através do IDP da UA que nos permitem limitar funcionalidades e dados apenas aos utilizadores que as devem poder aceder. Desta forma garantimos que não existe fuga de dados desnecessária ou roubos de informação. Sendo limitada à UA, é necessário garantir que a obtenção de dados dos utilizadores cumpre os requisitos de privacidade e segurança impostos pela regulamentação local, independentemente de qual é o serviço de autenticação utilizado.

- Consentimento Informado

Segundo o RGPD, é necessário o consentimento informado do utilizador para o tratamento dos seus dados pessoais. O IDP da UA garante-nos o consentimento do utilizador, informando o mesmo sobre quais dados serão partilhados com a aplicação e possíveis políticas de revogação dos mesmos (remover permissões de partilha, perguntar novamente se os dados mudarem).

O mesmo pode ser visto na imagem abaixo:

Está a aceder ao serviço:  
**wso2-is.ua.pt**

**Informação a ser fornecida ao serviço**

(clique para mostrar ou esconder)

UA-AD-FullName

**Rodrigo Silva Aguiar**

UA-AD-IUPI

**76811e8b-42bc-4e1d-adcc-6239f7d4e8d3**

UA-AD-Mail

**rodrigoaguiar96@ua.pt**

UA-AD-PrintUsers

**Access Denied**

UA-AD-Surname

**Aguiar**

UA-AD-Username

**rodrigoaguiar96@ua.pt**

UA-AD-Username\_as\_eduPersonPrincipalName

**rodrigoaguiar96@ua.pt**

UA-AD-displayName

**Rodrigo Aguiar**

UA-AD-givenName

**Rodrigo**

UA-RCU\_GURU-NumMecAluno

**108969**

UA-RCU\_GURU-TipoVinculo

**Aluno (Formação Inicial)**

UA-RCU\_GURU-Unidade

**Departamento de Electrónica,  
Telecomunicações e Informática**

Figura 2: Consentimento de dados no IDP da UA

É necessário garantir que noutras instituições o utilizador sabe quais dados estará a fornecer ao sistema e tenha o direito de dar o seu consentimento ou retirar o mesmo.



## 2.5 Efeito de escala e os seus resultados

A extensão da aplicação para uma implementação comercial de grande escala faria com que vários processos pudessem ser uniformizados e automatizados, beneficiando de **efeito de escala**.

À medida que mais instituições de ensino adotam o nosso serviço, os custos de desenvolvimento, manutenção e atualização do software serão reduzidos para cada uma das instituições, através da uniformização destes processos.

Isto poderia traduzir-se por exemplo em *updates* com uma frequência diária ou semanal que eram *shipped* e *deployed* automaticamente em todas as instituições de ensino, sem requerer trabalho manual.

Estando estabelecido este processo de gestão de qualidade e de *deploy* do serviço, poderia ser implementada apenas uma única equipa de monitorização, com conhecimento profundo deste processo, que garantia que o processo ocorria de forma correta.

O desenvolvimento de interfaces comuns para as várias instituições, mesmo que apresentem requisitos ou restrições diferentes, permite reduzir o custo de desenvolvimento e manutenção, sendo que não é preciso uma equipa especializada para cada instituição de ensino específica.

Através disto, também poderia ser implementada uma única equipa de *Customer Support*, que não teria de se preocupar com nuances ou detalhes específicos de cada implementação do serviço. Neste caso, o(s) cliente(s) também beneficiariam de um suporte técnico mais especializado, dado apenas ser necessário treinar uma equipa de especialistas num único sistema.

O custo de desenvolvimento de adaptações para as várias instituições de ensino poderia ser também diluído através de processos de standardização, sendo o decréscimo de custo repassado também ao cliente, fazendo o serviço ser mais apetecível em favor a alternativas desenvolvidas internamente ou a outros competidores.

Por exemplo, o processo de aceitação das propostas por parte de um administrador seria algo que poderia ser aplicado em grande parte das instituições de ensino, reduzindo a necessidade de fabricar código novo para esta funcionalidade.

Uma menor necessidade por parte da equipa técnica de desenvolver novo código levaria a que esta equipa pudesse ter um tamanho reduzido ou que se pudesse focar mais em suporte técnico, ultimamente levando tanto a menores custos para os clientes como a maior lucro proveniente deste serviço.

## 3. Propriedade Intelectual

---

### 3.1 Introdução

A propriedade intelectual é um direito único, que protege juridicamente as criações feitas a partir do conhecimento humano e fornece direitos exclusivos aos seus criadores. Estes direitos referem-se à sua integridade moral, à concessão de licenças para a disposição da obra e princípios que lhes estão garantidos. Os direitos de autor são um direito exclusivo em que terceiros só poderão utilizar o nome da obra mediante autorização prévia do seu autor.

A Propriedade Industrial tem características semelhantes ao Direito de Autor, pois trata-se de um direito constitutivo, exclusivo e tem como objetivo proteger objetos originais que estimulam o desenvolvimento da sociedade.

A regulação dos softwares é feita principalmente por meio da Lei n.º 9.609/98 (Lei do Software), a qual incorpora o entendimento de que programas de computador devem ser protegidos tais como os direitos de autor. Assim, aplicam-se também aos softwares as proteções conferidas pela Lei n.º 9.610/98 (Lei de Direitos de Autor), com pequenas diferenças. Nesta secção iremos abordar os direitos de autor sobre a plataforma "Dissertações", patentes e outros aspetos de propriedade individual sobre o trabalho base.

### 3.2 Direitos de autor

O software beneficia de uma proteção especial análoga à proteção conferida pelos direitos de autor. A proteção dos programas de computador na União Europeia e em Portugal é hoje estabelecida ao nível do direito de autor, por referência à Diretiva 2009/24/CE e ao Decreto-Lei n.º 252/94, de 20 de outubro. Para efetuar o registo, este poderá ser efetuado na Inspeção-Geral das Atividades Culturais (IGAC).

A regra será que, quando os programas de computador criados no âmbito de uma empresa ou de uma sociedade tenham origem em contrato de trabalho ou numa encomenda de obra, os direitos sobre os mesmos pertencerão à empresa e não ao seu criador intelectual. Desta forma, os direitos de autor no trabalho base são da própria Universidade de Aveiro.

### 3.3 Marcas Registadas

Uma marca é um sinal que se regista para distinguir um produto ou um serviço no comércio. O nosso site "Dissertações", teria que se registar junto do INPI e incorrer aos aspetos listados abaixo.

- Nome

Para o nome da marca "Dissertações", tivemos primeiro de observar se não existem nomes iguais de outras marcas dentro da mesma categoria. Recorrendo ao site do INPI, é possível notar que não existe nenhuma empresa atualmente em Portugal registada como "Dissertações" e consequentemente, nenhuma empresa com o mesmo nome na mesma categoria "serviços científicos e tecnológicos de pesquisa; conceção e programação de computadores".

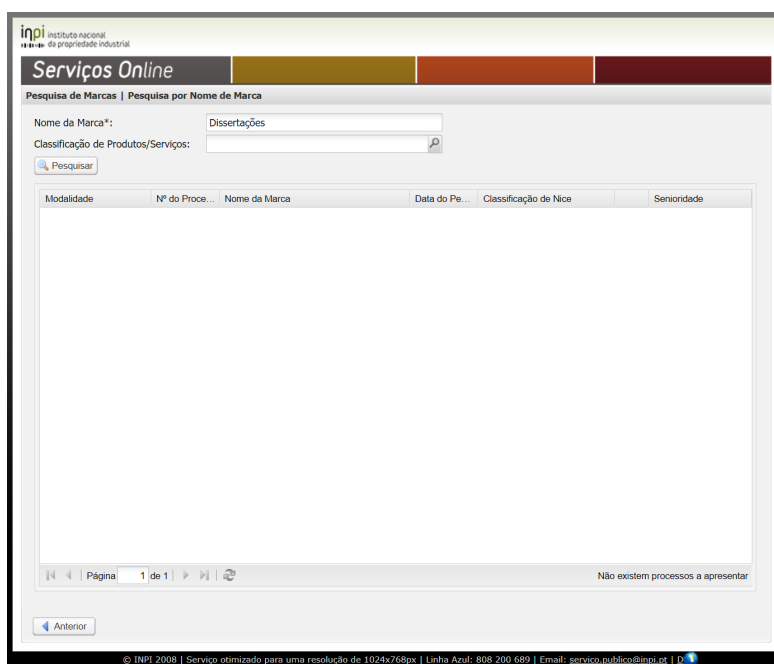


Figura 3: Base de dados da INPI

- Logótipo

O logótipo serve para identificar e diferenciar no mercado a própria entidade (pessoa singular ou coletiva) que presta os serviços ou comercializa os produtos.



Figura 4: Logótipo com texto



Figura 5: Logótipo

Este logótipo permite aos consumidores identificar e distinguir a empresa ou organização das outras existentes no mercado. O logótipo registado não pode ser igual nem semelhante a outro que já esteja registado, não pode conter elementos que sejam proibidos ou que violem a lei e a ordem pública, não induzir em erro o consumidor e ainda não pode ser unicamente composta por elementos usuais no comércio ou palavras que descrevam o produto ou serviço em questão, comparecendo às regras impostas pelo Serviços da Justiça português.

### 3.3 Patentes

A proteção por patente é frequentemente vista como uma forma de garantir o controlo do conceito subjacente a uma invenção.

No entanto, após a análise cuidadosa, concluímos que esta forma de proteção não se aplica ao nosso trabalho no web site "Dissertações", dado que a mesma não possui nenhuma característica técnica nova ou constitui uma ideia nova (dado que a plataforma antiga já implementava os mesmos workflows).

Embora as patentes possam oferecer benefícios como a valorização da empresa, fortalecimento do marketing, e royalties, impedem de terceiros de comercializar um produto baseado na tecnologia, no nosso caso, a patente não é a solução adequada.

Após uma pesquisa no sistema online do Instituto Online da Propriedade Industrial, não encontramos patentes registadas relacionadas a web sites de escolha e gestão de projetos e dissertações, o que reforça nossa conclusão de que a abordagem por patente não é viável para este projeto.

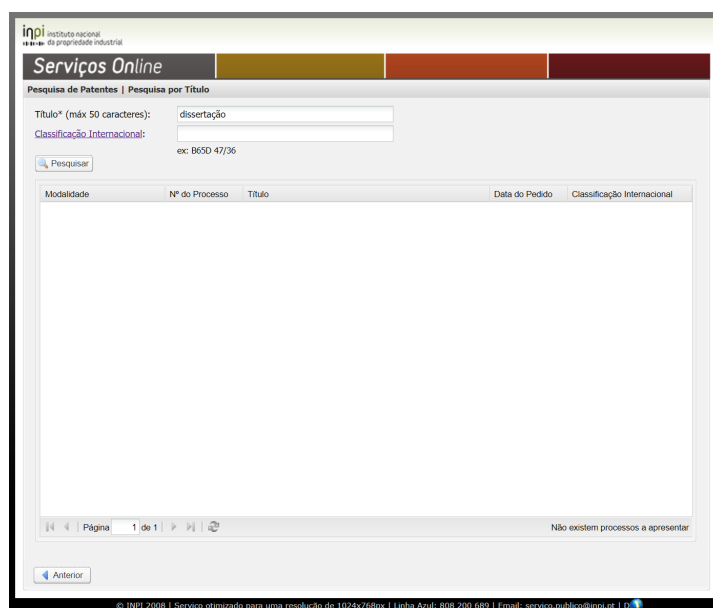


Figura 6: Patentes na base de dados da INPI

## 4. Software Open Source

### 4.1 Uso no Projeto

Open Source Software ou OSS é um software em que o seu código fonte encontra-se disponível para o público, para que qualquer pessoa possa visualizar, modificar ou distribuir [12].

Para este projeto, utilizamos múltiplos softwares que são considerados open source, como por exemplo: o sistema de bases de dados MongoDB, a linguagem de programação Python (para o desenvolvimento do backend), a framework React para o o desenvolvimento de aplicações web, uma grande parte das bibliotecas usadas quer para complementar o desenvolvimento do backend quer para o desenvolvimento do frontend.

Compatible	Package	License(s)
✓	Jinja2	BSD LICENSE
✓	MarkupSafe	BSD LICENSE
✓	aiofiles	APACHE SOFTWARE LICENSE
✓	aiohttp	MIT LICENSE
✓	annotated-types	MIT LICENSE
✓	blinker	MIT LICENSE
✗	certifi	MOZILLA PUBLIC LICENSE 2.0 (MPL 2.0)
✓	charset-normalizer	MIT LICENSE
✓	click	BSD LICENSE
✓	dataclasses	APACHE SOFTWARE LICENSE
✓	email-validator	THE UNLICENSE (UNLICENSE)
✓	et-xmlfile	MIT LICENSE
✓	fastapi	MIT LICENSE
✓	fastapi-cli	MIT LICENSE
✓	fastapi-mail	MIT LICENSE
✓	h11	MIT LICENSE
✓	httpx	BSD LICENSE
✓	idna	BSD LICENSE
✓	mariadb	GNU LESSER GENERAL PUBLIC LICENSE V2 OR LATER (LGPLV2+)
✓	motor	APACHE SOFTWARE LICENSE
✓	openpyxl	MIT LICENSE
✓	orjson	APACHE SOFTWARE LICENSE;; MIT LICENSE
✓	packaging	APACHE SOFTWARE LICENSE;; BSD LICENSE
✓	pillow	HISTORICAL PERMISSION NOTICE AND DISCLAIMER (HPND)
✓	pydantic	MIT LICENSE
✓	pydantic-core	MIT LICENSE
✓	pydantic-settings	MIT LICENSE
✓	pymongo	APACHE SOFTWARE LICENSE
✓	pypdf	BSD LICENSE
✓	python-multipart	APACHE SOFTWARE LICENSE
✓	requests	APACHE SOFTWARE LICENSE
✓	starlette	BSD LICENSE
✓	typing_extensions	PYTHON SOFTWARE FOUNDATION LICENSE
✓	ujson	BSD LICENSE
✓	urllib3	MIT LICENSE
✓	uvicorn	BSD LICENSE

Figura 7: Algumas licenças de softwares usados no backend do projeto

Package	License	Package	License
type-fest	(MIT OR CC0-1.0)	@humanwhocodes/object-schema (dev)	BSD-3-Clause
@ampproject/remapping (dev)	Apache-2.0	esquery (dev)	BSD-3-Clause
@humanwhocodes/config-array (dev)	Apache-2.0	hoist-non-react-statics	BSD-3-Clause
@humanwhocodes/module-importer (dev)	Apache-2.0	react-transition-group	BSD-3-Clause
before-after-hook (dev)	Apache-2.0	source-map	BSD-3-Clause
didyoumean (dev)	Apache-2.0	react	MIT
doctrine (dev)	Apache-2.0	react-cookie	MIT
eslint-visitor-keys (dev)	Apache-2.0	react-dom	MIT
ts-interface-checker (dev)	Apache-2.0	react-error-boundary	MIT
jackspeak (dev)	BlueOak-1.0.0	react-hook-form	MIT
path-scurry (dev)	BlueOak-1.0.0	react-icons	MIT
eslint-scope (dev)	BSD-2-Clause	react-is	MIT
esprez (dev)	BSD-2-Clause	react-refresh (dev)	MIT
esrecurse (dev)	BSD-2-Clause	react-router	MIT
estaverse (dev)	BSD-2-Clause	react-router-dom	MIT
esutils (dev)	BSD-2-Clause	read-cache (dev)	MIT
uri-js (dev)	BSD-2-Clause		

Figura 8: Algumas licenças de softwares usados no frontend do projeto

## 4.2 Licenciamento

Existem diversos tipos de licenças para OSS, cada uma destas possui as suas próprias regras e restrições. Uma das mais conhecidas é a Licença MIT, que permite, praticamente, a utilização de um software para uma qualquer finalidade, como por exemplo para fins comerciais, modificá-lo, distribuí-lo, entre outros. Isto tudo claro, sem a exigência de pagamento de taxas.

Para o nosso software, nós decidimos usar a licença Apache 2.0, que é uma licença semelhante à MIT, só que com a adição de cláusulas relativas a patentes, ou seja, exige que os desenvolvedores do software concedam uma licença para qualquer patente que detenham ou que seja pertinente para o software original.

Escolhemos utilizar a licença Apache 2.0 [6], visto que possibilita a utilização de outros softwares, que possuam diferentes tipos de licenças. No entanto nem todas apresentam compatibilidade com a Apache 2.0, como por exemplo a licença GPL (General Public License), em que softwares que tenham a licença Apache 2.0 podem ser incluídos e utilizados noutros que apresentem a licença GPL, mas o contrário não é possível, caso o software com a licença Apache 2.0 seja identificado como um trabalho derivativo de um software GPLv3 ou GPLv2.

No nosso projeto, maior parte dos softwares que escolhemos apresentam licenças que são compatíveis com a Apache License 2.0 e que são consideradas mais permissivas, como o React com a licença MIT, ou o Nginx com a licença BSD (Berkley Software Distribution) ou a biblioteca TailwindCSS com também a licença MIT. Mas também integramos alguns softwares que apresentam com licenças classificadas como copyleft e que podem entrar em conflito com outras, como é o caso do MongoDB que atualmente apresenta a licença SSPL (Server Side Public License) com características mais proprietárias e o da MariaDB que está licenciada sob a GPLv3.

## 4.3 Impacto no produto

A utilização de OSS pode reduzir significativamente os custos do desenvolvimento, pois uma grande parte dos softwares utilizados são gratuitos ou com custos baixos. No entanto, a manutenção do nosso software pode trazer mais gastos consigo, caso existam novas atualizações nos OSS's utilizados.

Oferece também a capacidade de aceder e modificar o código-fonte permite uma enorme flexibilidade na personalização do nosso sistema.

Com o software disponível para toda a sociedade, alguns riscos de segurança são geralmente menores, pois a identificação e correção de possíveis vulnerabilidades torna-se um processo mais rápido de realizar.

Como foi referido anteriormente, no nosso sistema, apresentamos softwares com licenças que não podem ser utilizadas em projetos com a licença Apache v2.0, caso a utilização destes seja considerado trabalho derivativo, como o MongoDB [10] e o MariaDB [9]. Porém, nós usufruímos destes apenas como sistema de bases de dados, ou seja, utilizamos estes 2 sistemas apenas para guardar dados, não alterámos nenhum código fonte de ambos os softwares, nem adicionámos novas funcionalidades, ou seja, o nosso projeto não é considerado um trabalho derivativo quer do MongoDB, quer do MariaDB.

Assim, a utilização do MongoDB e do MariaDB como sistemas de armazenamento de dados, sem uma alteração direta no código fonte ou a adição de novas funcionalidades, garante que o nosso projeto permaneça alinhado com as políticas de licenciamento destes softwares. Desta forma, evitamos potenciais questões de incompatibilidade de licença, estando em conformidade com o regulamento sobre a utilização de open source software.

No entanto, caso de alguma forma, o nosso sistema fosse considerado um trabalho derivativo dos softwares MongoDB ou MariaDB, então iríamos ter uma incompatibilidade com a licença GPL e portanto teríamos duas soluções para resolver esta incompatibilidade. Ou alterávamos a licença do nosso projeto inteiro para a licença GPLv3, o que poderia trazer ainda mais incompatibilidades com outras licenças de outros softwares utilizados, ou então substituir estes 2 open source softwares, por outros com licenças mais permissivas, como por exemplo substituíamos o MariaDB pelo PostGreSQL [7], que apresenta uma licença mais permissiva e parecida com as licenças MIT e BSD. Esta modificação não seria algo muito difícil e com custos elevados de realizar, visto que encontram-se poucos dados armazenados nesta BD, que são apenas relativos a configurações. No caso de substituir o MongoDB já seria algo mais difícil e, talvez, com algumas despesas elevadas associadas, visto que todos os dados mais importantes encontram-se lá guardados. No entanto seria possível substituí-lo pelo CouchDB [14], pois é também uma BD orientada a documentos e apresenta a licença Apache v2.0.



## 5. Cibersegurança

---

### 5.1 Ataques

Do ponto de vista de cibersegurança, existem diferentes tipos de ataques que tanto o nosso sistema como a nossa empresa podem sofrer, nomeadamente:

- Mass-Scale Phishing, Spear-Phishing ou Whaling são métodos que visam o roubo de identidade, através do roubo de credenciais. Esta ação é mais gravosa quanto maior for a hierarquia do roubado, podendo haver no caso de professores no sistema lugar a atribuição de uma proposta de dissertação/estágio a um aluno que não a deseja. No caso do administrador, poderia haver lugar a criação de cursos e áreas inexistentes, ou substituição dos Diretores de Curso por outra conta roubada, que poderia levar a problemas como o anteriormente referido. Além disso, o administrador, como atualmente tem acesso ao código, conseguiria criar, mudar ou eliminar qualquer dado ou até funcionalidade do sistema;
- Cross Site Scripting : Cross Site Scripting consiste numa vulnerabilidade de segurança que permite que atacantes executem código (localmente ou remotamente) através da manipulação de elementos HTML. Para a nossa aplicação web utilizamos React, que automaticamente faz a sanitização de todos os inputs dados pelo utilizador, não havendo forma de executar código JavaScript dentro do browser. É importante garantir que caso vulnerabilidades deste tipo aconteçam sejam resolvidas rapidamente e eficientemente para não causarem danos graves.
- Ataque de força bruta se o Identity Provider (IdP) da Universidade em questão for vulnerável a este tipo de ataques, resultando na fuga de passwords dos utilizadores, que podem depois ser vendidas em mercados/fóruns ilegais;
- Ataques de negação de serviço (DOS), em que há uma tentativa de usar os recursos de um sistema de forma massiva, tornando-os indisponíveis para os seus utilizadores;
- Rogue Employees, tanto na nossa empresa como nas próprias Universidades. Neste caso, pode haver eliminação da máquina virtual onde o sistema se encontra, ou até fuga dos dados armazenados ou outra informação sensível;
- Vulnerabilidades de dia zero - Havendo uso de algumas bibliotecas e pacotes tanto no frontend como backend, existe sempre a possibilidade de uma destas conter alguma vulnerabilidade que possa comprometer, com algum update, a nossa aplicação;

## 5.2 Implementação da defesa

Estes ataques podem ser praticamente anulados ou prevenidos se as seguintes medidas forem tomadas:

- Autenticação de 2 fatores: Este tipo de autenticação permite reforçar bastante o processo de autenticação, tornando o sistema mais seguro;

Estando dependentes das soluções de autenticação da universidade/instituição em questão, esta opção poderá nem sempre ser implementada.

Caso possível, uma solução de 2FA com recurso a códigos TOTP (Time-Based One-Time Password) enviados para o telemóvel do utilizador preveniria grande parte das situações de roubo de dados, sendo que o atacante também teria de ter acesso ao telemóvel do utilizador para se autenticar com o mesmo.

- Monitorização: Identificando e analisando o ambiente de segurança para as áreas de risco através da observação do tráfego da rede, logs, chamadas aos endpoints, etc, podemos tornar a nossa plataforma mais proativa em termos de segurança. Esta medida poderia eliminar ou minimizar os efeitos de ataques de DDoS [1] acima mencionados introduzindo *rate limiting* aos endpoints da nossa API, ou ainda *anycast network diffusion* [2] se a nossa solução se encontrar em vários servidores distribuídos, já que o número de pedidos vai ser distribuído pelos vários servidores.
- Formação contínua dos colaboradores da empresa para estarem a par das normas de segurança mais recentes, assim como pressionar as Instituições de Ensino Superior que usam o nosso sistema a formarem alunos, docentes e secretarias para a problemática de palavras-passe fracas.

É necessário garantir também que tanto os empregados da nossa empresa como os da universidade/instituição em questão tenham noção que não podem revelar detalhes da implementação do produto ou falar sobre o mesmo fora do local de trabalho.

- Acesso por parte do administrador

O nível de poder do administrador na aplicação dependerá bastante das regras impostas pela instituição em questão. Enquanto que na implementação atual, o administrador tem acesso a todos os dados guardados na base de dados, esta implementação não seria viável em larga escala.

Para resolver este problema, seria necessário a distribuição do poder entre várias entidades/pessoas, sendo que apenas uma pessoa não deveria poder aceder a todos os dados da aplicação.

- ASVS Standards e outras normas

Dada a natureza do nosso sistema, cumprir com o nível 2 do Standard de OWASP Application Security Verification Standard (ASVS) [13] é o recomendado para termos uma plataforma mais robusta. Além disso, a nossa própria empresa cumprir com normas como o ISO27001 assim como ter uma comunicação permanente e ativa com as equipas dedicadas na área de segurança das Universidades, ajudam a prevenir problemas de segurança.

## 5.3 Planos de recuperação

Dado que o serviço se integraria num mercado B2B (Business to Business), a reputação é bastante importante. Sendo assim, o profissionalismo com que oferecemos o serviço e a satisfação do cliente são bastante importantes para garantir o futuro e escalabilidade do serviço.

Recuperar de um ciberataque publicitado na Internet constituiria uma importante medida na gestão da reputação do serviço, pelo que é necessário a implementação de processos de como lidar com o mesmo.

Sendo assim, seriam estabelecidos os seguintes passos:

- Identificação do Incidente : Uma equipa de cibersegurança dedicada monitoriza o serviço constantemente para detetar fugas de informação ou falhas de segurança, detetando e confirmando ataques em caso da ocorrência dos mesmos.
- Contenção do Ataque: Os serviços identificados como atacados seriam isolados do resto do sistema para evitar a propagação do ataque, por exemplo, desconectando os serviços necessários ou desacoplando-os do resto da aplicação. Num último caso, um shutdown geral do sistema podia ser indiciado.
- Comunicação e Notificação: Informar a instituição em questão ou os utilizadores afetados da existência de um ataque e as possíveis medidas a tomar, de modo a restringir ao máximo o efeito do mesmo.
- Análise e Avaliação do Impacto: Avaliação dos danos causados pelo ciberataque, incluindo possíveis perdas de dados ou falhas de disponibilidade do sistema.
- Recuperação do ataque: Identificação das vulnerabilidades exploradas pelo(s) atacante(s) e correção das mesmas, seguida pela recuperação de possíveis dados perdidos e finalmente o reestabelecimento dos serviços afetados.
- Comunicação pós-incidente: Após a recuperação do incidente, proceder à elaboração de um relatório descrevendo o incidente e medidas tomadas para a prevenção de futuros ataques.

Nesta fase procederia-se também à elaboração de declarações públicas, que poderiam ser entregues aos órgãos de comunicação social ou outras organizações externas, de modo a gerir a reputação do sistema e da organização em si.

Em geral, é importante ter processos eficazes de recuperação de ataques sendo que, para além da reputação do nosso sistema, estaríamos a por em causa a reputação de uma instituição de ensino pública, que poderia ter várias consequências, de entre elas legais, por negligência ou falta de cuidado no tratamento de dados.

## 5.4 Legislação de cibersegurança

A nossa empresa, estando dentro da União Europeia, tem de seguir alguma legislação relacionada com a área da cibersegurança:

- Desde 2023, começou a ser feita a transição para o cumprimento de um nível comum de Cibersegurança em toda a União Europeia, a diretiva SRI 2 [\[15\]](#). Esta destina-se aos setores mais críticos da sociedade, incluindo organizações de investigação, como as Universidades.
- O RGPD está também relacionado com a cibersegurança, nomeadamente ter o princípio de segurança por design para novas funcionalidades que venham a ser desenvolvidas. Além disso, temos também o consentimento informado aos utilizadores, através do IdP, e ainda consultar os DPO's das diferentes Instituições acerca do processamento dos dados daquela organização.

## 6. Privacidade

---

### 6.1 Efeitos no projeto

Na plataforma disponibilizada a cada cliente, os dados privados podem ser separados em duas categorias: as propriedades de cada utilizador (email, número mecanográfico, identificador interno, número de ECTs obtidos, etc) e os registos das ações tomadas pelo mesmo na plataforma (dissertações escolhidas, ficheiros submetidos, tempos de login, etc).

Ao considerar o contexto de integração do sistema, a solução escolhida para obter as informações académicas relevantes de cada utilizador é preferencialmente através do uso dos serviços de identificação próprios de cada universidade, isto é, a autenticação e atribuição das propriedades de cada utilizador deve ser feita com recurso aos sistemas de IdP (Identity Provider) implementados por cada cliente.

Um IdP base tem de ser desenvolvido no caso de não existir nenhum serviço semelhante na universidade em questão, ou o sistema recorrer a métodos mais arcaicos para obter os dados de cada utilizador. No entanto, é de salientar que a maior parte das Instituições já tem este tipo de serviços nos dias de hoje.

No caso do desenvolvimento de um IdP novo para aquela universidade, esta situação seria indesejada, pois teria de ser realizado um levantamento da informação relevante de cada utilizador, tal como as suas credenciais de login na plataforma, que terão de por sua vez ser inseridas neste IDP base.

Antes deste processo ser iniciado, tem de ser identificado um Encarregado da Proteção de Dados (DPO). Esta entidade vai ser responsável por controlar a conformidade das operações de tratamento dos dados pessoais e de determinar a sua relevância para o funcionamento base do sistema.

No caso dos dados das ações tomadas, visto que estas são gerados pelo sistema em si, não necessitam de integração com sistemas externos.

Grande parte destes dados são habitualmente de cariz público, mas esta escolha é feita pelo próprio cliente e, caso estas dados sejam obrigados a serem mantidos privados, irá obrigatoriamente influenciar o cuidado com que os mesmos terão de ser processados e disponibilizados.

## 6.2 Minimizar os problemas de privacidade

Considerando os dados que se identifiquem como de caráter privado, a sua disseminação quer seja pela plataforma em si, quer seja por acessos externos não autorizados ou imprevistos (como por exemplo, em casos de data leaks ou breaches), é altamente perigosa e todas as ações possíveis devem ser tomadas para evitar e minimizar os problemas causados por tais eventos.

Visto que a plataforma não trata só de dados de indivíduos singulares, mas também dados gerados pelas ações mútuas de dois ou mais utilizadores, como por exemplo, a divulgação de que uma dissertação de um certo docente foi escolhida por um certo aluno, temos de considerar que qualquer eventual perda de informação vai afetar ambos os indivíduos envolvidos.

Para minimizar estes problemas de privacidade, cada implementação da plataforma terá de ser modificada para cumprir com os requisitos de tratamento e exposição de dados de cada Instituição cliente.

Assumindo que as mesmas têm regras estritas para o uso e divulgação dos dados dos seus membros, cabe à nossa implementação técnica assegurar o cumprimento das mesmas.

É preciso, no entanto, considerar a possibilidade de certas universidades não terem estes requisitos completamente definidos. Neste caso, a construção de uma proposta que defina exatamente a categoria dos diversos dados requisitados para o bom funcionamento da aplicação e a garantia da aprovação desta proposta pelos membros relevantes na instituição ficaria a cargo do anteriormente mencionado Encarregado da Proteção de Dados.

## 6.3 Soluções técnicas

Como mencionado na secção anterior, a real proteção dos dados e da privacidade dos utilizadores ficará a cargo das soluções técnicas implementadas.

Considerando agora apenas os dados classificados como privados, quaisquer que estes sejam dependendo das regras faladas no ponto anterior, cabe à plataforma obter, processar e persistir os mesmos de forma segura e resiliente, garantindo a sua integridade.

Para tal, iremos tirar proveito tanto de soluções já desenvolvidas para os restantes sistemas operacionais em cada universidade, como de funcionalidades de privacidade desenvolvidas especificamente para a nossa plataforma.

Para começar, a plataforma terá de ser hospedada completamente ao abrigo da rede do cliente, de forma a garantir que tráfego alheio à mesma não irá causar ações indesejadas em nenhum componente do serviço. Isto permite à aplicação usufruir das firewalls, bloqueios de portas, sistemas contra "Distributed Denial Of Service Attacks", entre outros, que estejam implementados pela rede da universidade em si. Caso estes componentes não existam, uma implementação base dos mesmos terá de ser realizada antes da plataforma entrar em uso, ou por um serviço contratado ou pelos nossos desenvolvedores.

Igualmente, o uso da rede interna diminui a probabilidade de um atacante externo realizar um ataque de interceção de mensagens ("sniffing") ou semelhante, uma vez que o acesso à rede em si é mais controlado.

Para o processamento e exposição de dados, é necessário que a aplicação consiga distinguir sobre quais dados pode ou não publicar, sendo que dados privados de cada utilizador apenas podem ser vistos pelo mesmo e pelas entidades consideradas como relevantes, como por exemplo, o docente com qual assinou acordo e com o diretor do curso em que a dissertação está inserida.

Esta funcionalidade apenas é possível caso um sistema de autenticação robusto seja implementado, uma vez que a partilha ou não destes dados para um certo utilizador vai ser baseada na sua identificação pelo sistema.

Quanto à persistência de dados, a mesma pode ser feita através de sistemas de armazenamento internos da universidade onde o sistema se encontra, preferencialmente dentro da mesma rede, ou através de um contrato externo para uso de um sistema de armazenamento "cloud".

Em ambas as opções, os dados devem sempre ser cifrados pelo sistema de forma a que perdas de informação por parte do sistema de armazenamento não comprometam a privacidade dos dados lá persistidos. Este processo não é complicado visto que as chaves de decifra não precisam de ser partilhadas, sendo a nossa plataforma o único sistema que precisa de obter os dados "plain text" originais e decifrados.

Finalmente, o uso de serviços de armazenamento externos implica uma discussão com os fornecedores dos mesmos para garantir que as funcionalidades dos mesmos garantem o nível de segurança, privacidade e contingência expectáveis no uso do nosso sistema.

## 6.4 Implementação de um serviço de resposta a pedidos legais

Considerando que a grande parte dos dados pessoais são obtidos por outros sistemas da universidade em que a plataforma está inserida, não é de prever que estes dados nos sejam requisitados por instituições legais, em vez de serem pedidos diretamente à fonte dos mesmos, ou seja, os serviços de onde o nosso sistema também os obtém.

Ao contrário destes dados, as informações geradas internamente pela plataforma e de caráter privado podem ser pedidas tanto por organizações jurídicas e legais como pelos próprios serviços de secretaria e gestão da universidade em si.

Na eventualidade destes dados serem pedidos por uma organização jurídica, cabe ao nosso Encarregado da Proteção de Dados analisar a sua relevância para o caso apresentado pela mesma.

É de notar que, uma vez mais, as políticas de privacidade e de resposta a pedidos legais da universidade em questão entram em consideração neste processo, visto que os dados são gerados por membros da mesma para fins académicos.

Sendo assim, a resposta a pedidos legais tem de ser avaliada em parceria com os membros relevantes da organização académica e a obtenção dos dados tem de ser realizada de forma altamente supervisionada e o mais automatizada possível, de forma a evitar a perda ou publicação dos mesmos. Isto significa que a própria plataforma deve ser capaz de obter, processar e exportar seguramente estes dados em caso destes serem considerados relevantes para o decorrer de uma investigação jurídica.

Também é preciso acentuar que a plataforma em si não opera sobre dados altamente críticos ou sensíveis, visto que em grande parte das universidades, a escolha de dissertações, os endereços eletrónicos, os nomes dos alunos e até as informações sobre os docentes são consideradas de caráter público, e a plataforma não precisa de dados extremamente detalhados sobre os seus utilizadores para realizar com sucesso as suas funcionalidades, sendo assim a probabilidade de pedidos legais altamente reduzida.



## 7. Aspectos éticos

---

### 7.1 Aspectos éticos a considerar

Para o nosso projeto, é necessário considerar diversos aspectos éticos para garantir a igualdade, privacidade e integridade de todas as partes envolvidas, como por exemplo:

- **Privacidade e Proteções de Dados Pessoais:** Os dados pessoais dos estudantes e docentes devem de ser protegidos contra acessos não autorizados e os dados relativos às dissertações devem também estar devidamente protegidos para não existirem fugas de informação indevidas. Também é necessário obter o consentimento explícito dos utilizadores para a recolha, o armazenamento e a utilização dos seus dados pessoais. Para estarmos em conformidade com este ponto, o mecanismo de autenticação deverá pedir o consentimento do utilizador para o tratamento dos seus dados pessoais, dando a conhecer algumas políticas sobre a revogação dos mesmos e a partilha dos dados com outras aplicações, identificando-as devidamente.
- **Igualdade e transparência:** A plataforma deve assegurar que o processo de atribuição de dissertações a estudantes é um processo justo e transparente, evitando favoritismos ou discriminações. No entanto, como no nosso sistema o processo de escolha e depois atribuição não é um processo automático, mas sim feita pelos docentes proponentes do tema, estes é que escolhem o aluno a atribuir a partir dos que mostraram interesse nas suas propostas, pelo que cabe a estes decidir de forma justa qual o estudante mais apropriado para a sua proposta.

Também é necessário garantir que o sistema seja acessível não só a todos os estudantes que se encontrem no ano em que devem de escolher a dissertação/estágio/projeto que quer realizar e docentes e também restringir as funcionalidades de submeter dissertações a utilizadores com os cargos necessários para tal e, consequentemente, permitir a esses utilizadores serem orientadores/coorientadores.

- **Integridade Académica:** Também é importante assegurar que todas as dissertações /estágios/projetos passam por uma avaliação por parte de um administrador, antes de serem publicadas para toda a comunidade académica. Nesta avaliação, cabe ao administrador analisar todas as informações de uma nova proposta submetida, e consoante isto aceitar ou recusar cada uma. Adicionalmente, cada proposta tem também de passar por uma validação por parte dos diretores de curso, para verificar se a proposta se adequa para os cursos selecionados pelo orientador.

## 7.2 Regulações a cumprir

Existem múltiplos regulamentos que devemos de seguir para podermos ter um sistema legal e que protege os direitos dos seus utilizadores

- **Regulamento Geral de Proteção de Dados (RGPD):** Como já foi referido neste relatório, deve garantir-se que os dados pessoais de cada utilizador sejam armazenados de forma segura e apenas pelo tempo necessário e que os utilizadores têm o direito de aceder, alterar e apagar os seus dados pessoais, bem como de recusar o seu tratamento.
- **Lei Proteção de Dados Pessoais (Lei n.º 58/2019):** Adotar mecanismos técnicos adequados para proteger os dados pessoais contra a destruição, perda, alteração sem consentimento, divulgação ou acesso não autorizado.
- **Regulamentos Académicos:** Como o sistema irá englobar englobar diversas universidades é necessário que, para cada universidade, o sistema siga os regulamentos de cada uma definidos relativamente à submissão, aprovação/recusa, escolha e atribuição de propostas de dissertações/projetos/estágios. É importante também assegurar também que todas as práticas e procedimentos adotados estejam alinhados com o código de ética e conduta da instituição.

## 8. Aspectos de Inteligência Artificial

---

### 8.1 Integração no serviço

De momento, o TB não possui qualquer tipo de sistema de Inteligência Artificial nem existe ideias de implementação dos mesmos.

Assumindo a expansão do projeto para uma larga escala, seria de esperar que uma equipa de Customer Support tivesse de ser estabelecida para fornecer ajuda a utilizadores que não saibam utilizar o serviço corretamente ou necessitem de ajuda.

Dado que a interface de utilizador teria de ser mudada de instituição para instituição (para cumprir as normas da gráficas de cada instituição), poderia ser necessário uma equipa de Customer Support para cada uma das instituições, o que resultaria em custos acrescidos, tanto para a instituição em si, como para a organização, com o recrutamento e treino de profissionais em sistemas específicos.

Sendo assim, a implementação de um modelo de Inteligência Artificial, um chatbot, que serviria como uma primeira linha de customer support, capaz de responder às perguntas de utilizadores, como por exemplo, como se mostra interesse numa dissertação, aliviaria a equipa de Customer Support designada, reduzindo os custos de operação.

Um sistema deste tipo teria de ser treinado e implementado de acordo com a regulação do AI ACT, caindo este sistema sobre a categoria de **Limited Risk**, pelo que o utilizador final teria de ser informado que se encontra a interagir com um sistema de inteligência Artificial.

Este sistema seria apenas treinado com dados locais ou da instituição em questão, garantindo que não tem acesso a dados pessoais.

Sendo assim, seria necessário a comunicação com a instituição em questão e o fornecimento de dados por parte da mesma para o treino deste modelo, havendo a garantia que estes não fornecem dados pessoais ou sensíveis.

## 9. Hyperscalers

---

### 9.1 Relações com Hyperscalers

Como mencionado anteriormente, a boa separação do processamento necessário para a realização rápida e consistente das funcionalidades da plataforma e do local de persistência dos dados utilizados, leva a uma facilidade de integração de uma ou ambas estas facetas da aplicação num serviço de "cloud computing" ou "cloud storage", sendo que os óbvios fornecedores de tais sistemas são os "Hyperscalers" do mundo da informática.

Para o "hosting" do serviço em si, seria beneficiário hospedar o mesmo dentro de servidores privados dentro da própria rede da instituição que adquiriu o nosso serviço, de forma a providenciar um acesso mais seguro de dentro da própria e uma integração mais fácil com os restantes serviços (IDP, correio eletrónico, etc) da mesma.

Mas, tal como em muitos dos tópicos anteriormente falados, é possível que um cliente não disponha dos meios para criar e gerir uma máquina suficientemente capaz de hospedar o nosso sistema internamente, sendo assim necessário implementar a plataforma num serviço de "cloud computing" através de um serviço externo à universidade e à nossa empresa.

Para tal, seria necessário chegar a um acordo sobre os parâmetros do serviço providenciado e testar se as implementações com os restantes sistemas da universidade são plausíveis, tecnologicamente e em termos da privacidade dos dados transmitidos entre as redes envolvidas.

Já na persistência de dados, a nossa solução compreende que, uma vez que os dados são cifrados apenas localmente, a utilização de serviços externos de armazenamento não só é esperada, como também é considerada a solução ótima para o problema.

Sendo assim, será uma vez mais preciso obter um acordo com uma empresa que disponibilize um serviço de armazenamento de dados que conforme com as expectativas e características necessárias para o bom funcionamento da nossa aplicação e para a segurança dos dados persistidos.

Concluindo, o uso de serviços de "Hyperscalers" é esperado e por vezes até benéfico face às alternativas propostas, considerando que os critérios de aceitação do serviço são cumpridos pelo serviço a contratar.

## 9.2 Efeitos da legislação europeia sobre estes serviços

Para alcançar os parâmetros legais e de privacidade esperados pelo nosso serviço, o uso de sistemas de "cloud computing" ou "cloud storage" tem de garantir que um nível equivalente de proteção de dados pessoais é alcançado comparativamente ao processamento e persistência de dados localmente.

Dentro da União Europeia, vários estudos foram realizados a pedido da mesma para avaliar e definir um conjunto de medidas de segurança e transparência no uso de serviços "cloud".

Resultando destes estudos, foram identificados que os contratos habituais destes serviços excluía ou altamente removiam a culpa dos fornecedores do serviço em casos em que os dados são perdidos ou corrompidos [4].

Após esta análise, o uso de serviços "cloud" por empresas e indivíduos privados foi altamente regulada para beneficiar os mesmos.

No contexto da nossa aplicação, os efeitos destes regulamentos garantem que as perdas de informação por parte destes serviços sub-contratados não culpabiliza a nossa empresa e a utilização destas plataformas para complementar a nossa aplicação não está proibida por nenhuma lei.

Concluindo, o uso de serviços "cloud" como parte do nosso sistema não carece de uma grande alteração no paradigma legal, visto que as considerações a tomar já foram analisadas dentro da União Europeia e as legislações foram alteradas para que empresas privadas facilmente consigam tirar proveito dos benefícios que a "cloud computing" trás sem necessitar de processos e contratos legais extensos.

## 10. Efeitos no sistema

### 10.1 Introdução

Efeitos de rede referem-se ao fenómeno no qual o valor de um produto, serviço ou plataforma aumenta conforme o número de utilizadores dos mesmos aumentam. Este conceito é portanto crítico para entender o crescimento de um produto.

No caso da nossa plataforma, o aumento do número de utilizadores da mesma vai estar relacionado principalmente com dois grupos - o número de universidades que vai aderir ao nosso sistema e o universo de estudantes e docentes dessas universidades que prosseguem para mestrado ou estão na condição de propor temas para dissertações.

Assim, faz sentido analisar o quão valiosa a nossa plataforma pode vir a ser de acordo com esta perspetiva. Tendo em conta dados recolhidos pelo Observatório das Desigualdades, o número de estudantes inscritos no ensino superior tem vindo a subir, tendo aumentado em cerca de 5% desde 2015 em Portugal [11]. Mesmo no grupo PIIGS (Portugal, Itália, Irlanda, Grécia e Espanha) esta tendência mantém-se, como se pode ver na figura abaixo:

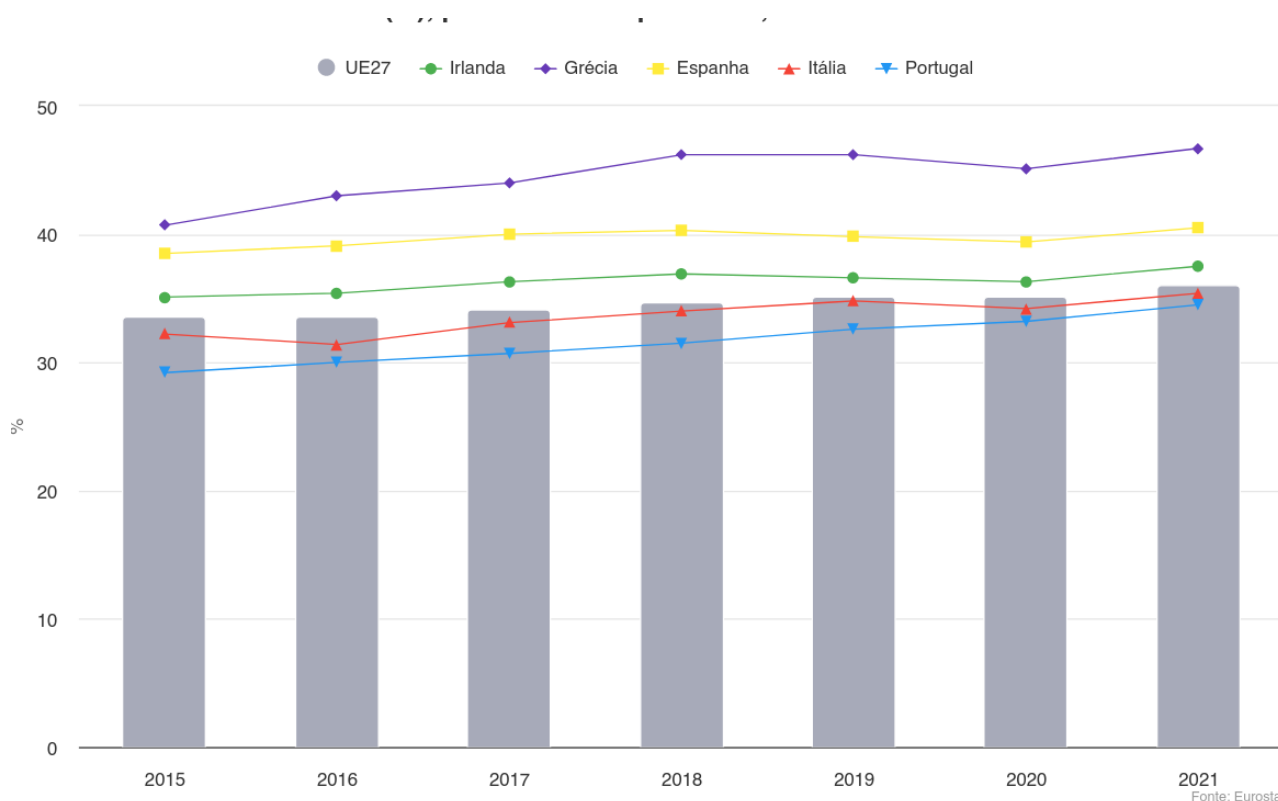


Figura 9: Alunos inscritos no ensino superior/terciário, por população 20-24 anos de idade (%), países da Europa do Sul, 2015-2021

Em Portugal, dados da Direção Geral de Estatísticas da Educação e Ciência (DGEEC) mostram que o número de estudantes que prosseguem para mestrado aumentou cerca de 4% entre 2017/18 e 2021/22[5] como mostra a figura abaixo:

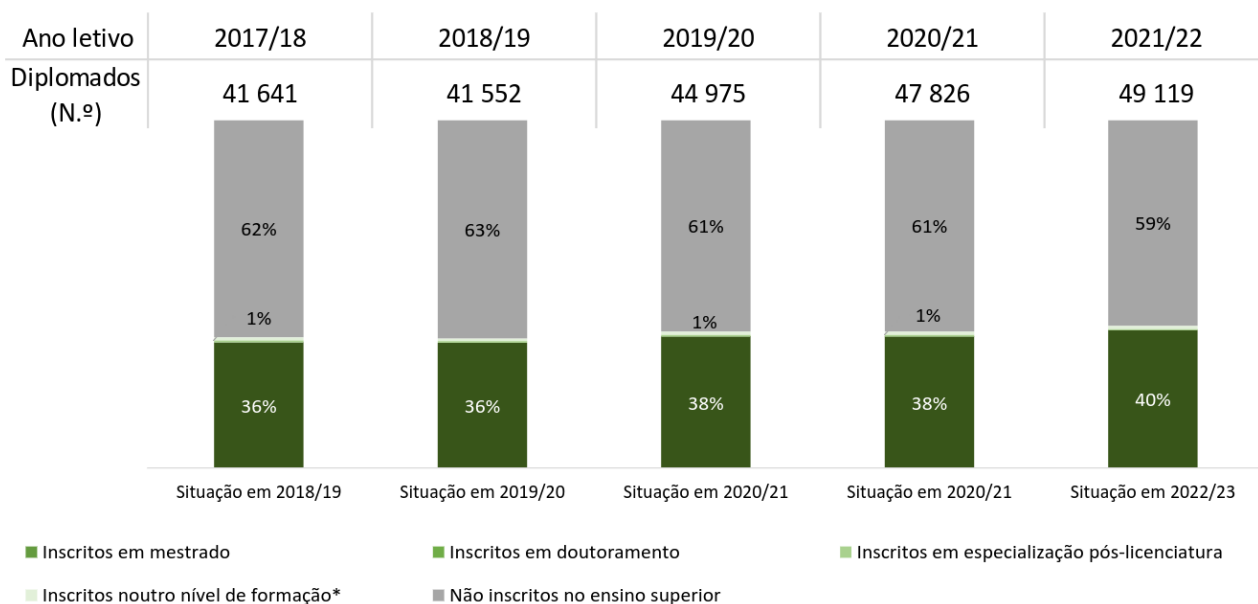


Figura 10: Situação no ano letivo seguinte dos diplomados de licenciatura 2017/18 a 2021/22

Analisando as estatísticas, podemos verificar que a tendência é que o número de estudantes que avançam para mestrado aumente, e que consequentemente o número de dissertações, projetos ou estágios também aumenta. Assim, quer pela lei de Sarnoff, lei de Metcalfe, ou lei de Reed o valor da rede está destinado a aumentar.

## 10.2 Efeitos do sistema na rede onde foi integrado

A integração deste sistema numa rede universitária traria vários efeitos positivos:

Ao facilitar o acesso e administração dos temas relativos às dissertações, a plataforma promove uma maior eficiência no que toca à eficiência operacional e na comunicação entre os estudantes e orientadores. Assim, os estudantes podem facilmente navegar pelas dissertações e escolher as que mais se alinham com os seus interesses. Por outro lado, os docentes ganham uma plataforma centralizada para gerir as suas dissertações e tudo relacionada às mesmas, desde ver os alunos interessados até assinar o acordo com eles.

Esta plataforma pode trazer uma padronização do processo que é a submissão e escolha das dissertações. Para além de uniformizar este processo a nível institucional, isto permite que os vários departamentos da mesma universidade possam colaborar e encontrar sinergias e oportunidades de orientação em diversas dissertações, visto que há vários temas que são multidisciplinares. Isto tem valor porque não só une mais a oferta formativa dos diversos departamentos, mas também expande o universo de temas a que os estudantes estão expostos, o que enriquece a qualidade da pesquisa e alarga os horizontes dos estudantes. Esta uniformização abre também portas à colaboração entre estudantes para uma mesma dissertação, o que aumenta a cooperação inter-estudantes.

Ao oferecer uma oferta mais diversificada, e como referido anteriormente, a qualidade da pesquisa aumenta. Isto dá-se uma vez que os interesses pessoais dos estudantes se alinham com o tema da pesquisa, o que gera mais motivação para o desenvolvimento da mesma. Ao mesmo tempo, os orientadores podem dedicar mais tempo às suas atividades de investigação ao invés de se preocuparem com questões administrativas.

Seria possível também obter dados valiosos para as universidades, departamentos e docentes. Dados como as áreas de interesse por departamento, tendências de pesquisa, preferências de temas, etc, poderiam ser analisadas de modo a auxiliar na tomada de decisões estratégicas, desde alocação de recursos, mudanças de planos curriculares ou até investimento em novos cursos.

Caso o numero de universidades na rede seja suficiente, efeitos de maior impacto podem começar a surgir. No caso da unificação do processo de dissertações entre as universidades aderentes, a partilha de temas de dissertações pode romper a barreira dos departamentos e alastrar-se para o que seria uma rede inter-universitária de temas de dissertações, aumento ainda mais o repertório de temas disponíveis para os alunos e ainda mais a exposição a novas ideias e horizontes. Desta forma seria possível gerar uma maior identificação entre os alunos e os temas propostos, assim como criar uma rede de partilha para a investigação académica de tamanho considerável, ao mesmo tempo que a cooperação entre instituições alcançaria um nível mais elevado que abriria portas e facilitaria a troca de recursos, quer a nível de docentes quer a nível curricular, entre os estabelecimentos de Ensino.



## 10.3 Ações para aumentar o sucesso do sistema

De forma a garantir o sucesso do sistema é necessário pôr em prática várias ações estratégicas que promovam tanto a adesão do sistema quanto o benefício percebido pelos utilizadores ao usar a plataforma.

Assim, numa primeira fase seria necessário garantir um suporte contínuo à comunidade que aderiu à plataforma, ao mesmo tempo que é fornecido o treino necessário para o uso correto do sistema em si. Desta forma é possível suavizar a transição entre os processos antigos e o processo proposto pelo nosso sistema, ao passo que se maximiza a adesão ao sistema em si. Ao adotar esta prática é possível endereçar problemas que possam surgir durante o uso comum da plataforma e resolvê-las de forma rápida.

Para além de um suporte contínuo, é crucial ser possível medir o desempenho do sistema e monitorizar continuamente o seu uso e carga. Assim, o *feedback* dos utilizadores do serviço através de inquéritos, pesquisas de satisfação e de alcance torna-se uma medida necessária para conseguir extrair estes *insights* valiosos. Com base nestes *insights* é possível identificar áreas de melhoria que podem ser corrigidas ou melhoradas em versões futuras do serviço.

No entanto, para além da parte de assistência técnica, seria vital ter uma vertente de comunicação fortíssima. Esta será responsável por comunicar claramente os benefícios e pontos fortes do sistema em vigor. Através de campanhas de consciencialização, sessões de demonstração e presença em eventos seria possível destacar como o sistema facilita a gestão das dissertações e melhora a experiência académica.

Desta forma seria possível criar uma comunidade à volta da plataforma. Esta comunidade é na verdade uma mais valia, uma vez que fomenta a troca de experiências, informações e práticas que agregam à plataforma. Esta partilha por parte da comunidade inter-universitária incentiva uma cultura de melhoria constante, o que é claramente benéfico para o sistema.

Estas práticas culminam no que é talvez o maior fator para o sucesso da nossa plataforma, que é na verdade a dependência do mesmo. Uma vez que quando os processos de uma parte tão crucial e comum de uma fase indispensável do percurso de mestrado passam a ser processados pela plataforma, tanto o recuar a métodos menos eficientes e mais trabalhosos, como o recurso a folhas de Excel ou plataformas desatualizadas, tanto o trabalho que daria mudar de serviço fazem com que este sistema passe a fazer parte do que é dissertação em si. Assim, a partir do momento que uma instituição incorpore este sistema o sucesso do mesmo torna-se uma questão de tempo.

Da mesma forma, ao ganhar uma comunidade à volta do mesmo, e ao ser aderido por várias universidades, a opção de não dispor tanto da facilidade adquirida com o sistema ou de não estar dentro da norma imposta pelo mesmo faz com que seja "necessário" adquirir a nossa plataforma. Neste ponto é atingida a massa crítica, e o sucesso do sistema é assegurado.

## 10.4 Efeitos negativos da rede

Apesar dos benefícios que a nossa plataforma trás para a rede, há que reconhecer que um sistema deste tipo pode trazer malefícios, principalmente para uma rede universitária. Estes efeitos podem limitar a eficácia do sistema e gerar desafios adicionais para as instituições.

A segregação dos sistemas por universidade pode levar a que haja um isolamento das mesmas, limitando severamente as oportunidades de cooperação entre as instituições. Uma vez que cada universidade pode estar a um sistema diferente para processar as dissertações, a introdução de outro sistema que aumenta ainda mais a segregação pode fechar portas e limitar a troca de conhecimentos entre as instituições. Assim, os docentes deixam de ter fácil acesso a temas de dissertações ou recursos de pesquisas que poderiam ser convertidas em temas para alunos.

Por outro lado, a personalização extrema de forma a que os sistemas implementados em cada universidade pode levar a inconsistências entre os mesmos. Uma vez que os utilizadores e contextos diferem, o rumo que as alterações seguem podem ser bastante diferentes. Assim, alunos ou docentes que mudem de universidade ou colaborem com múltiplas instituições vão ter dificuldade em interagir com um sistema em específico, deteriorando a eficiência do sistema. Para além disso, estas diferenças podem gerar uma perceção de falta de qualidade e desconfiança na plataforma, impactando de forma negativa a adesão ao sistema e a satisfação dos utilizadores em relação ao sistema.

Outro risco deste sistema prende-se com a dependência tecnológica do mesmo. Em caso de falha da plataforma, e no cenário de uma dependência semi-total da universidade do sistema, pode haver uma paralisação ou interrupção nas atividades académicas, o que pode levar a atrasos e a alterações indesejadas de processos internos. Num cenário de não haver backups ou processos alternativos, pode ainda ser necessário recomeçar a época de escolha de dissertações devido à perda da informação. Isto pode limitar ainda mais a cooperação com outras instituições pois no caso de partilha de temas e um cenário de falha, esta situação pode também gerar complicações na outra instituição.

# Referências

---

- [1] CloudFlare. URL: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> (acedido em 25/05/2024).
- [2] CloudFlare. *What is Anycast?* URL: <https://www.cloudflare.com/learning/cdn/glossary/anycast-network/> (acedido em 25/05/2024).
- [3] CNCS. *Contexto Atual*. URL: <https://www.cncs.gov.pt/pt/contexto/> (acedido em 25/05/2024).
- [4] European Comission. *European Comission*. URL: [https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/cloud-computing-contracts\\_en](https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/cloud-computing-contracts_en) (acedido em 26/05/2024).
- [5] Direção-Geral de Estatísticas da Educação e ciência. *Prosseguimento de estudos dos diplomados de licenciatura 2017/18 a 2021/22*. Abr. de 2024. URL: <https://www.dgeec.medu.pt/art/ensino-superior/estudos/areas-de-estudo/64f855f0d128bc76d4fba91e#artigo-657c86e518230137b6bbdab3> (acedido em 24/05/2024).
- [6] Apache Software Foundation. *Apache License v2.0 and GPL compatibility*. URL: <https://www.apache.org/licenses/GPL-compatibility.html> (acedido em 24/05/2024).
- [7] The PostgreSQL Global Development Group. *PostgreSQL License*. URL: <https://www.postgresql.org/about/licence/> (acedido em 24/05/2024).
- [8] Faculdade de Letras da Universidade do Porto. URL: [https://sigarra.up.pt/flup/en/web\\_base.gera\\_pagina?p\\_pagina=diSSERTacoes\\_teses](https://sigarra.up.pt/flup/en/web_base.gera_pagina?p_pagina=diSSERTacoes_teses).
- [9] *MariaDB Licenses*. URL: <https://mariadb.com/kb/en/mariadb-licenses/> (acedido em 24/05/2024).
- [10] *MongoDB Licensing*. URL: <https://www.mongodb.com/legal/licensing/community-edition> (acedido em 24/05/2024).
- [11] ObservatorioDesigualdades. *Alunos inscritos no ensino superior - observatório das desigualdades*. Jan. de 2024. URL: <https://www.observatorio-das-desigualdades.com/2024/01/01/alunos-inscritos-no-ensino-superior/> (acedido em 24/05/2024).
- [12] Opensource.com. *What is open source*. URL: <https://opensource.com/resources/what-open-source> (acedido em 24/05/2024).
- [13] OWASP. *Owasp Application Security Verification Standard*. URL: <https://owasp.org/www-project-application-security-verification-standard/> (acedido em 25/05/2024).
- [14] CouchDB PMC. *CouchDB Bylaws*. Jul. de 2014. URL: <https://couchdb.apache.org/bylaws.html> (acedido em 24/05/2024).
- [15] Europe Union. *Directive - 2022/2555 - en - EUR-lex*. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555> (acedido em 25/05/2024).
- [16] Europe Union. *Políticas de Cibersegurança*. URL: <https://digital-strategy.ec.europa.eu/pt/policies/cybersecurity-policies> (acedido em 25/05/2024).
- [17] Payal Wadhwa. *How to implement cybersecurity monitoring in 2024*. Abr. de 2024. URL: <https://sprinto.com/blog/cybersecurity-monitoring/> (acedido em 25/05/2024).