

iTrust6G

**Final Course Work**

1ª Entrega Intercalar

**Student Name: Luisa Ferreira, a22209718, Licenciatura De Engenharia Informática**

**Supervisor's name:** Luis Campos

**Entidade Externa:** PDM

Departamento de Engenharia Informática e Sistemas de Informação

Universidade Lusófona, Centro Universitário de Lisboa

Final Course Work | Degree in Computer Science | 3/01/2025

**Direitos de cópia**

Intelligent Trust and Security Orchestration for 6G Distributed Cloud Environments, Copyright by Luisa Ferreira, Lusófona University.

The School of Communication, Architecture, Arts and Information Technologies (ECATI) and Lusófona University of Humanities and Technologies (ULHT) have the right, in perpetuity and without geographical limits, to archive and publish this dissertation in printed copies reproduced on paper or digitally, or by any other means known or invented, and to disseminate it through scientific repositories and to allow its copying and distribution for educational or research purposes, non-commercial, provided that credit is given to the author and publisher.

**Acknowledgments**

I would like to express my sincere gratitude to PDM for the opportunity to be part of this project and for trusting my work. Working with such experienced professionals has been an enriching experience that allowed me to learn and grow both personally and professionally.

A special thanks to Paulo Correia for his constant guidance, precise advice, and unwavering support, which helped me overcome the challenges throughout this journey. I would also like to mention Florian for the mutual support and collaboration that made this project even more meaningful.

Finally, I want to thank everyone who, directly or indirectly, contributed to the completion of this work, whether through teaching, sharing knowledge, preparing work environments, or providing the necessary materials for the development of the project.

Resumo

Este trabalho aborda os desafios de segurança associados às redes de telecomunicações de sexta geração (6G), que promovem a conectividade ubíqua e a convergência entre redes e sistemas de TI, essenciais para aplicações como eHealth, Indústria 5.0 e veículos autónomos. Dada a integração de equipamentos heterogéneos e multi-vendor, as redes 6G enfrentam riscos acrescidos, como a complexidade na gestão de vulnerabilidades e a necessidade de segurança contínua em ambientes dinâmicos. Este estudo propõe a implementação de uma arquitetura de "Zero-Trust", baseada em algoritmos de inteligência artificial e Machine Learning, para monitorizar e avaliar a postura de segurança em tempo real, mitigando ameaças. São também analisadas as implicações das regulamentações europeias, como o GDPR e a diretiva NIS2, na conformidade e gestão de cibersegurança dos operadores. A visão apresentada explora a utilização de ambientes programáveis para ampliar a visibilidade da rede e suportar avaliações contínuas de confiança.

Palavras-chave: Redes 6G; Segurança; Zero-Trust; Machine Learning; Infraestruturas Críticas

Abstract

This work addresses the security challenges associated with sixth-generation (6G) telecommunication networks, which enable ubiquitous connectivity and the convergence of networks and IT systems, essential for applications such as eHealth, Industry 5.0, and autonomous vehicles. With the integration of heterogeneous and multi-vendor equipment, 6G networks face increased risks, including complexity in vulnerability management and the need for continuous security in dynamic environments. This study proposes implementing a "Zero-Trust" architecture, leveraging artificial intelligence and machine learning algorithms to monitor and evaluate security posture in real time, mitigating threats. It also analyzes the implications of European regulations, such as GDPR and the NIS2 directive, on compliance and cybersecurity management for operators. The presented vision explores the use of programmable environments to enhance network visibility and support continuous trust assessments.

Keywords: 6G Networks; Security; Zero-Trust; Machine Learning; Critical Infrastructures

Table of Content

[Acknowledgments iii](#_Toc182436104)

[Resumo iv](#_Toc182436105)

[Abstract v](#_Toc182436106)

[Índice vi](#_Toc182436107)

[Lista de Figuras viii](#_Toc182436108)

[Lista de Tabelas ix](#_Toc182436109)

[Lista de Siglas x](#_Toc182436110)

[1 Introdução 1](#_Toc182436111)

[1.1 Enquadramento 1](#_Toc182436112)

[1.2 Motivação e Identificação do Problema 1](#_Toc182436113)

[1.3 Objetivos 1](#_Toc182436114)

[1.4 Estrutura do Documento 1](#_Toc182436115)

[2 Pertinência e Viabilidade 1](#_Toc182436116)

[2.1 Pertinência 1](#_Toc182436117)

[2.2 Viabilidade 1](#_Toc182436118)

[3 Conceitos Fundamentais 2](#_Toc182436119)

[3.1 Conceitos Teóricos 2](#_Toc182436120)

[3.2 Modelos e Algoritmos Relevantes 2](#_Toc182436121)

[3.3 Tecnologias e Ferramentas Utilizadas 2](#_Toc182436122)

[4 Estado da Arte 3](#_Toc182436123)

[4.1 Estado da Arte 3](#_Toc182436124)

[4.2 Proposta de inovação e mais-valias 3](#_Toc182436125)

[4.3 Identificação de oportunidade de negócio 3](#_Toc182436126)

[5 Solução Proposta 4](#_Toc182436127)

[5.1 Introdução 4](#_Toc182436128)

[5.2 Metodologia 4](#_Toc182436129)

[5.3 Recolha de Dados 4](#_Toc182436130)

[5.4 Descrição dos Dados 4](#_Toc182436131)

[5.5 Pré-processamento dos dados 4](#_Toc182436132)

[5.6 Análise Exploratória dos Dados 4](#_Toc182436133)

[5.7 Modelos e Algoritmos Escolhidos 4](#_Toc182436134)

[5.8 Abrangência 4](#_Toc182436135)

[6 Método e Planeamento 5](#_Toc182436136)

[6.1 Planeamento inicial 5](#_Toc182436137)

[6.2 Análise Crítica ao Planeamento 5](#_Toc182436138)

[7 Resultados e Discussão 6](#_Toc182436139)

[7.1 Resultados das Análises 6](#_Toc182436140)

[7.2 Comparação de Modelos e Abordagens 6](#_Toc182436141)

[7.3 Interpretação dos Resultados 6](#_Toc182436142)

[7.4 Limitações da Análise 6](#_Toc182436143)

[8 Implementação 7](#_Toc182436144)

[8.1 Recursos e Infraestrutura 7](#_Toc182436145)

[8.2 Processo de Implantação 7](#_Toc182436146)

[8.3 Testes de Validação e Desafios 7](#_Toc182436147)

[9 Conclusão 8](#_Toc182436148)

[9.1 Conclusão 8](#_Toc182436149)

[9.2 Trabalhos Futuros 8](#_Toc182436150)

[Bibliografia 9](#_Toc182436151)

[Anexo 1 – Recomendações para formatação de um relatório 10](#_Toc182436152)

Lista de Figuras

[Figura 1 – Processo de carregamento de uma página HTML. 10](#_Toc181747618)

Lista de Tabelas

[Tabela 1 - Calendarização de conteúdos do relatório 1](#_Toc181747619)

[Tabela 2 – Tipos de Selectores existentes. 10](#_Toc181747620)

Lista de Siglas

API Interface de Programação de Aplicações

HTML Linguagem de Marcação de Hipertexto

# Introdução

The problem under analysis is based on real circumstances related to the need to improve security and trust in 6G network platforms, a critical challenge in an era of widespread and integrated connectivity. The integration of heterogeneous and multi-vendor devices in 6G infrastructures, along with the increasing cybersecurity threats, has made the implementation of robust solutions essential. This work is based on external contributions, particularly from stakeholders and end-users, to define use case requirements, conduct a detailed threat surface analysis, and establish trust-related key performance indicators (KPIs). The study relies on thorough scientific analysis and a threat portfolio that guides the development of intelligence and security modules. This approach represents a significant step toward mitigating vulnerabilities, implementing "Zero-Trust" principles, and ensuring the resilience of critical telecommunication platforms.

## Enquadramento

The present work is set in the context of sixth-generation (6G) telecommunication networks, whose implementation is expected in the next decade. 6G networks represent a significant evolution in the telecommunications sector, being essential to support connectivity in critical sectors such as energy, transport, and public administration. These sectors, recognized by the European legislative framework NIS2 [NIS2, 2023], rely on robust infrastructures to ensure the resilience and security of their services.  
With increasing digitalization and the integration of multiple providers and heterogeneous technologies, security challenges arise, particularly in establishing trust between different administrative domains and protecting against cyber threats. In this scenario, the "Zero-Trust" (ZT) concept gains relevance. ZT is an architecture that continuously evaluates the security of entities before granting access to resources, promoting reliable end-to-end connectivity [ZT Architecture, 2020]. This paradigm is particularly suited for 6G networks, which demand adaptive security due to the dynamic nature of services and the absence of clear perimeters.  
The iTrust6G project is based on these principles and proposes an end-to-end security platform that combines threat analysis, the definition of trust-related key performance indicators (KPIs), and the use of explainable security modules. These modules enable transparent audits and foster trust among operators. Furthermore, the project is grounded in regulations such as GDPR [GDPR, 2016] and NIS2 to ensure compliance and strengthen the security of critical infrastructures.  
By aligning Zero-Trust principles with a detailed threat analysis and the definition of reliable metrics, this work addresses practical and scientific challenges, contributing to the security and resilience of 6G networks.

## Motivação e Identificação do Problema

### Motivation

The motivation for this work arises from the growing importance of sixth-generation (6G) networks as critical infrastructure supporting essential services such as autonomous vehicles, remote healthcare, and industrial automation. These networks, by integrating multiple providers and heterogeneous technologies, present new challenges related to security and trust, requiring robust and innovative solutions.  
The need to protect these networks against advanced cyber threats and ensure service resilience is reinforced by regulations such as GDPR and NIS2, which highlight the importance of compliance and security in critical infrastructures. Additionally, implementing the "Zero-Trust" concept represents a significant opportunity to redefine traditional security models, ensuring reliable and secure end-to-end connectivity. This work is motivated by the ambition to develop a platform that not only addresses technical challenges but also contributes to increasing operators' and users' trust in 6G networks.

**1.2.2 Problem Identification**

## The evolution towards 6G networks brings several specific challenges:

## Integration of multiple providers: The involvement of different operators and technologies complicates trust and security models.

## Network openness: Exposing capabilities through APIs to third-party services increases vulnerability to attacks and security breaches.

## Service cloudification: The continuous disaggregation of services into edge and cloud environments makes defining clear security perimeters difficult.

## Dynamic security orchestration: Establishing trust between administrative domains requires an adaptive approach that considers the diversity and volatility of interactions among domains.

These difficulties compromise the integrity and resilience of 6G networks, making it essential to implement a solution that combines continuous threat assessment, key performance indicators (KPIs), and explainable mechanisms for audits and decision-making.

## Objetivos

**1.3.1 General Objective**

Develop a 6G service management platform based on "Zero-Trust" principles, capable of ensuring trust and security for critical infrastructures in multi-provider networks.

**1.3.2 Specific Objectives**

* Design an end-to-end security architecture that enables continuous trust assessment and real-time threat management.
* Integrate artificial intelligence to detect novel threats and generate cyber threat intelligence to support proactive and reactive actions.
* Develop trust algorithms that continuously reassess the security posture of services operated in 6G environments.
* Implement intelligent solutions for security orchestration across the cloud continuum, encompassing edge, extreme edge, and public cloud.
* Specify and implement intent-based security policies to support automated and explainable orchestration.
* Create dynamic and configurable solutions for the secure placement of network functions in slices, ensuring isolation and security in service delivery.

## Document Structure

This report is organized as follows:

* **Section 1 - Introduction:** Presents the analysis of the feasibility and relevance of the work developed, including the framework, motivation, problem identification, and project objectives.
* **Section 2 - Relevance and Feasibility:** Evaluates the relevance and feasibility of the proposed solution, analyzing how the project meets the needs of 6G networks. This section includes a comparative analysis with existing concepts, identifies innovative elements, and highlights the advantages and benefits of the solution.
* **Section 3 - Specification and Modeling:** Details the characteristics of the developed solution, based on requirements identification, description of key elements, and exploration of real-world usage scenarios. It includes requirements analysis, enumeration, and detailed description of the main requirements, as well as interaction models of the solution.
* **Section 4 - Proposed Solution:** Presents the functional description of the developed solution, the technical architecture, the technologies and tools used, and the mechanisms implemented to support security and trust in 6G networks.
* **Section 5 - Testing and Validation:** Details the validation methods adopted in the project, including test scenarios, obtained results, and performance evaluation.
* **Section 6 - Methodology and Planning:** Describes the methodological approach adopted in the project, including the timeline, task distribution, and project management methods.
* **Section 7 - Conclusion:** Summarizes the main results achieved, discusses the impact of the work performed, and provides suggestions for future work.

TODO

A Tabela 1 é indicativa de entregáveis para cada momento de avaliação, assumindo abordagem sequencial do desenvolvimento de TFC. Podendo ser adotadas outras abordagens metodológicas (e.g.: metodologias ágeis), serão aceites outras organizações de entregas. Deve-se, no entanto, observar duas condições: (i) a 1ª entrega deverá manter os conteúdos indicados no quadro, por forma a permitir ao júri avaliar a pertinência do tema e a taxa de esforço esperada; (ii) a organização de conteúdos em cada entrega deve ter atenção aos critérios de avaliação de modo a garantir a uniformidade da avaliação

Tabela 1 - Calendarização de conteúdos do relatório

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Avaliação** | **Tipo** | **Introdução** | **Pertinência e Viabilidade** | **Conceitos Fundamentais** | **Estado da Arte** | **Solução desenvolvida** | **Resultados** | **Discussão** | **Implantação** | **Método e Planeamento** | **Conclusão** |
| 1ª entrega Intercalar | Qualitativa;  Júri cego | Incluir | Incluir | Incluir | incluir | incluir | N/D | N/D | N/D | Inicial | incluir |
| 2ª Entrega Intercalar | Qualitativa;  Júri cego | revisto | revisto | revisto | revisto | revisto | N/D | N/D | N/D | revisto | revisto |
| Final[[1]](#footnote-1) | Quantitativa;  Presencial | Final | Final | Final | Final | Solução Proposta | Incluir | Incluir | Incluir | Final[[2]](#footnote-2) | Final |

Legenda:

* Incluir/revisto: A inclusão dos conteúdos é obrigatória, podendo ser alterada face às entregas anteriores
* N/A: A entrega é facultativa, não sendo necessária caso não haja alterações face à entrega anterior
* De notar que a inclusão se torna obrigatória caso a avaliação anterior sugerir correcções
* N/D: Assume-se a inexistência de elementos para entrega

# Pertinência e Viabilidade

## Pertinência

A pertinência do trabalho em desenvolvimento é evidenciada pela sua contribuição para resolver desafios críticos associados à segurança operacional e à confiança em redes de sexta geração (6G). Estas redes, que suportarão aplicações essenciais como veículos autónomos, cuidados de saúde remotos e automação industrial, apresentam arquiteturas complexas que requerem soluções de segurança mais avançadas para proteger contra ciberameaças sofisticadas.

**2.1.1 Validação por Terceiros**

A relevância do iTrust6G foi validada por especialistas da área, incluindo operadores de telecomunicações e administradores de infraestruturas críticas, que destacaram a necessidade de soluções robustas para mitigar ataques cibernéticos e reforçar a confiança em serviços 6G. Além disso, end-users demonstraram interesse em serviços mais seguros e confiáveis proporcionados por esta plataforma.

**2.1.2 Impacto Positivo Esperado**

* **Para Operadores de Telecomunicações:** Integração de uma plataforma de confiança que permite monitorização contínua, resposta em tempo real e reavaliação da confiança em serviços críticos.
* **Para Infraestruturas Críticas:** Reforço da segurança e resiliência, garantindo operações ininterruptas mesmo sob ataques distribuídos.
* **Para Administradores de Segurança:** Ferramentas avançadas para deteção de ameaças, análise forense e mitigação proativa de riscos.
* **Para Utilizadores Finais:** Aumento da confiança em serviços 6G com proteção aprimorada contra ciberameaças.

### Discussão de Resultados

Os principais resultados foram validados através de um inquérito de pertinência realizado junto às partes interessadas, cujos gráficos e análises detalhadas estão apresentados no Anexo X. Estes resultados confirmam a relevância e necessidade da solução proposta, destacando a sua contribuição para a confiança e segurança em ambientes multi-fornecedor.

## Viabilidade

Viabilidade é a medida em que uma solução pode ser implementada e sustentada com sucesso. A viabilidade deverá ser avaliada por critérios econométricos, demonstrando-se que a solução proposta terá características para poder ser continuada após conclusão do TFC, não se esgotando enquanto projeto académico. Depende de vários fatores que devem ser avaliados: técnicos, económicos, sociais, ambientais. Deve ser feita uma reflexão e avaliação destes:

* Alinhamento com os Objetivos de Desenvolvimento Sustentável, identificando os ODS que o projeto pretende abordar e como se alinha com as metas específicas de cada ODS. Avaliar o impacto esperado do projeto nos ODS escolhidos.
* A viabilidade técnica refere-se à disponibilidade e adequação de ferramentas para executar a solução. Pode ser avaliada através de teste com um protótipo interativo (primeira entrega), ou um protótipo funcional e testes de aceitação (relatório final).
* A viabilidade económica refere-se aos custos e benefícios da solução, se é acessível, lucrativa e sustentável. Pode ser avaliada através de uma análise de custo-benefício, e retorno do investimento.
* A viabilidade social refere-se á aceitação e ao apoio da solução pelas partes interessadas, utilizadores e beneficiários envolvidos ou afetados pelo problema, avaliando se atende as necessidades, espectativas e preferências. Pode ser avaliada através de inquéritos e entrevistas e inquéritos de satisfação.

# Conceitos Fundamentais

## Conceitos Teóricos

Esta secção deverá apresentar uma descrição dos conceitos fundamentais teóricos para desenvolver o presente trabalho. Deverá apresentar ao leitor a descrição dos conceitos necessários para a compreensão da utilização dos mesmos nos capítulos seguintes. Criar sub-secções para separar tópicos.

## Modelos e Algoritmos Relevantes

Descreve as técnicas e algoritmos que serão considerados ou comparados no trabalho, fundamentando teoricamente a escolha de cada um.

## Tecnologias e Ferramentas Utilizadas

Descrição das várias tecnologias. Fundamentar as opções tecnológicas para a construção da solução. Listar as ferramentas usadas, com descrição sucinta e justificação do uso.

# Estado da Arte

## Estado da Arte

O Estado da Arte deverá referenciar trabalhos de outros autores, diretamente relacionados com o relatório e que apresentam outras alternativas para a solução do problema identificado, descrevendo-os brevemente e abordando as diferenças para o trabalho realizado, nomeadamente identificando os aspetos abordados no trabalho que não foram tratados pelos outros trabalhos. Se os conteúdos forem diferenciados, deve estar organizado em sub-secções. Cada trabalho referenciado deve conter pelo menos um parágrafo, e pelo menos uma referência bibliográfica para um artigo que detalhe o trabalho referido.

## Proposta de inovação e mais-valias

Identificar o que torna a solução inovadora e os principais elementos que diferencia das abordagens existentes. Referir as vantagens e benefícios que a proposta traz (melhoria eficiência, acessibilidade, impacto social, sustentabilidade).

Sendo o trabalho de cariz científico, a mais-valia poderá ser apresentada como o acréscimo que o trabalho se propões oferecer ao conhecimento

## Identificação de oportunidade de negócio

Com vista a fomentar o empreendedorismo tecnológico, se for pertinente, sugere-se que se realize uma proposta de negócio para exploração comercial do projeto desenvolvido ou sucedâneos.

# Solução Proposta

Na entrega final o título deverá passar a **Solução Desenvolvida**, apresentando-se resultado final do trabalho em vez de perspectiva a desenvolver em fases posteriores

A cada entrega, deve-se realçar eventuais alterações face a proposta anteriores

## Introdução

Nesta secção deve incluir uma descrição da solução desenvolvida. Deverá incluir:

* link para vídeo demonstrativo da solução desenvolvida.
* link para repositório Git com o código desenvolvido e eventualmente os dados caso sejam públicos.

## Metodologia

Descrição sumária da metodologia desenvolvida para implementar a solução. Criar uma ilustração que represente os vários passos que a constituem (e são detalhados nas secções seguintes), descrevendo cada passo sumariamente num par de linhas.

## Recolha de Dados

Descrição da fonte dos dados, seu formato e conteúdo. Se for mais adequado, e alguma das secções ficar excessivamente pequena, esta secção pode ficar junta com a seguinte.

## Descrição dos Dados

Define as variáveis, tipos de dados e características principais. Se for mais adequado, esta secção pode ficar junta com a anterior.

## Pré-processamento dos dados

Aborda a limpeza e preparação dos dados necessária, incluindo remoção de valores em falta ou normalização, necessários para uma boa análise.

## Análise Exploratória dos Dados

Uma vez os dados prontos, é apresentada uma análise para identificar eventuais padrões e características importantes.

## Modelos e Algoritmos Escolhidos

Explica o processo de escolha dos modelos e algoritmos, incluindo as razões para as seleções feitas. Detalha a configuração inicial dos modelos.

## Abrangência

Indicar unidades curriculares e as áreas científicas do curso aplicadas na solução proposta, descrevendo sumariamente que aspectos aprendidos serão utilizados e como.

# Método e Planeamento

## Planeamento inicial

Descrição do método de trabalho seguido no desenvolvimento do projecto. Ao elaborar este capítulo os alunos devem ter como referência o calendário proposto nos relatórios.

Deve ser incluído um plano de trabalho e cronograma (gantt-chart) orientado à gestão de projeto. No último relatório, aconselha-se que o calendário seja construindo tendo como orientação uma hipotética disponibilização publica da solução construída, focando na realização de testes, qualidade e aceitação, e eventual implementação.

## Análise Crítica ao Planeamento

Aconselha-se uma análise critica sobre o cumprimento do calendário e indicações do progresso do trabalho, onde se refira tarefas realizadas, dificuldades mais marcantes e alterações que tenham sido introduzidas ao plano e objectivos iniciais.

Esta secção é aconselhada na segunda entrega e indispensável na final

# Resultados e Discussão

Apresenta os resultados obtidos a partir das análises realizadas, incluindo uma discussão sobre o desempenho dos modelos e a relevância dos resultados encontrados. Deve comparar os resultados com os objetivos definidos e discutir possíveis interpretações dos dados. **Apresentam-se propostas de secções que podem ser adotadas ou agregadas**.

## Resultados das Análises

Apresenta os principais resultados das análises, como padrões identificados, insights obtidos e previsões realizadas. Deve incluir gráficos, tabelas e outras visualizações para facilitar a interpretação.

## Comparação de Modelos e Abordagens

Descreve e compara o desempenho dos diferentes modelos, destacando vantagens e limitações de cada abordagem. Pode incluir uma tabela comparativa para resumir métricas de desempenho.

## Interpretação dos Resultados

Análise crítica dos resultados, comparando-os com os objetivos estabelecidos. Discute as interpretações possíveis para os dados e os resultados obtidos, contextualizando com a literatura e hipóteses iniciais. Explora a relevância dos conhecimentos obtidos e as implicações das conclusões do estudo.

## Limitações da Análise

Identifica e discute as limitações do estudo em termos de dados, metodologias e modelos aplicados. Discute como estas limitações podem ter impactado os resultados.

# Implementação

## Recursos e Infraestrutura

Descrição dos requisitos de hardware e software para a execução da solução, incluindo ambiente de servidor, bases de dados, e dependências de software.

## Processo de Implantação

Passo-a-passo da instalação e configuração da solução no ambiente de produção, com destaque para o fluxo de trabalho, permissões e eventuais adaptações. Deve ser incluído referencia ao repositório git onde o código se encontra disponível.

## Testes de Validação e Desafios

Explicação dos testes de validação executados após a implantação, os problemas encontrados e as soluções implementadas para garantir a robustez da solução.

# Conclusão

## Conclusão

Esta secção deverá ter os principais resultados do trabalho. Deve começar formulando o problema abordados no trabalho, após os quais as principais ideias e conclusões de cada um dos capítulos devem ser apresentadas.

## Trabalhos Futuros

Nesta secção devem ser indicadas possíveis direções para trabalhos futuros.

Assumindo que o trabalho pudesse ser continuados, quais os próximos passos? Como se pode melhorar a solução

Tendo em vista a vertente de inovação e empreendedorismo, o que se pode fazer para aumentar o potencial da solução?

# Bibliografia

Exemplifica-se em baixo o formato de vários tipos de referências bibliográficas (livro, relatório, website, etc.). Deve estar ordenado alfabeticamente pela referência. As referências devem conter 4 carateres e 2 dígitos: os primeiros carateres dos nomes dos autores; e os dígitos do ano de publicação.

[TaWe20] A. Tanenbaum e D. Wetherall, *Computer Networks*, 6ª Edição, Prentice Hall, USA, 2020. (livro)

[ToBe24] S. Tomic e M. Beko, A min-max optimization-based approach for secure localization in wireless networks, IEEE Transactions on Vehicular Technology, Vol. 73, No. 4, mar. 2024 (artigo revista)

[CiAl24] B.P. Cipriano e P. Alves, *Seven Years Later: Lessons Learned in Automated Assessment*, 5th International Computer Programming Education Conference, ICPEC 2024, Lisboa, Portugal, jun. 2024 (https://drops.dagstuhl.de/entities/document/10.4230/OASIcs.ICPEC.2024.3). (artigo conferência)

[SaSi23] G. Santos e B. Silva, *Aplicação móvel para rotas de bicicletas*, Trabalho Final de Curso, DEISI, Universidade Lusófona, Lisboa, Portugal, 2023. (relatório)

[ULHT21] Universidade Lusófona de Humanidades e Tecnologia, [www.ulusofona.pt](http://www.ulusofona.pt), Out. 2021. (website)

[DEISI21] DEISI, *Regulamento de Trabalho Final de Curso*, Set. 2024.

# Anexo 1 – Recomendações para formatação de um relatório

A escrita do relatório deve seguir o presente template, não mudando nada em termos de formatação (fontes, espaçamentos, tamanhos, etc). **Este anexo exemplificativo deverá ser removido antes de submeter o seu relatório**. Antes de entregar o relatório, exercite a sua capacidade de auto-crítica lendo-o e verificando se está adequadamente redigido.

Na Tabela 2 exemplifica-se uma tabela e a forma como esta deve ser referenciada. Como poderá ver, se passar com o rato por cima da palavra “Tabela 1”, neste parágrafo, aparece o hiperlink. Tal é possível se for incluída uma referência da forma que se explica a seguir. As tabelas devem ser apresentadas sempre depois de referenciadas. A legenda da tabela deve ser inserida através da opção do menu *References\Insert caption* (no menu em cima do MS Word), sempre no topo da tabela. A referência a uma tabela insere-se através do comando *References*\*cross-reference*, sendo a sua numeração automática.

Tabela 2 – Tipos de Selectores existentes.

|  |  |
| --- | --- |
| **Tipo** | h1, p |
| **Universal** | \* |
| **Classe** | .class1 |
| **ID** | #element |
| **Atributo** | [target=\_blank] |
| **Pseudo-classe** | div:hover |
| **Pseudo-elemento** | p::first-letter |

O processo de carregamento de uma página HTML está representado na Figura 1 para exemplificar como se deve inserir uma legenda a uma figura assim como uma referência a esta mesma. Para inserir uma Figura, seleccione *References\Insert Caption* e indique que quer inserir uma Figura. A figura deve sempre aparecer depois de ser referida no texto. Para inserir uma referência a uma figura, utilizar *References\Cross-reference*. O índice e listas de tabelas e figuras (mas páginas iii a v) actualizam-se automaticamente se inseridas desta forma. Para actualizar basta selecionar todo o texto e premir F9.

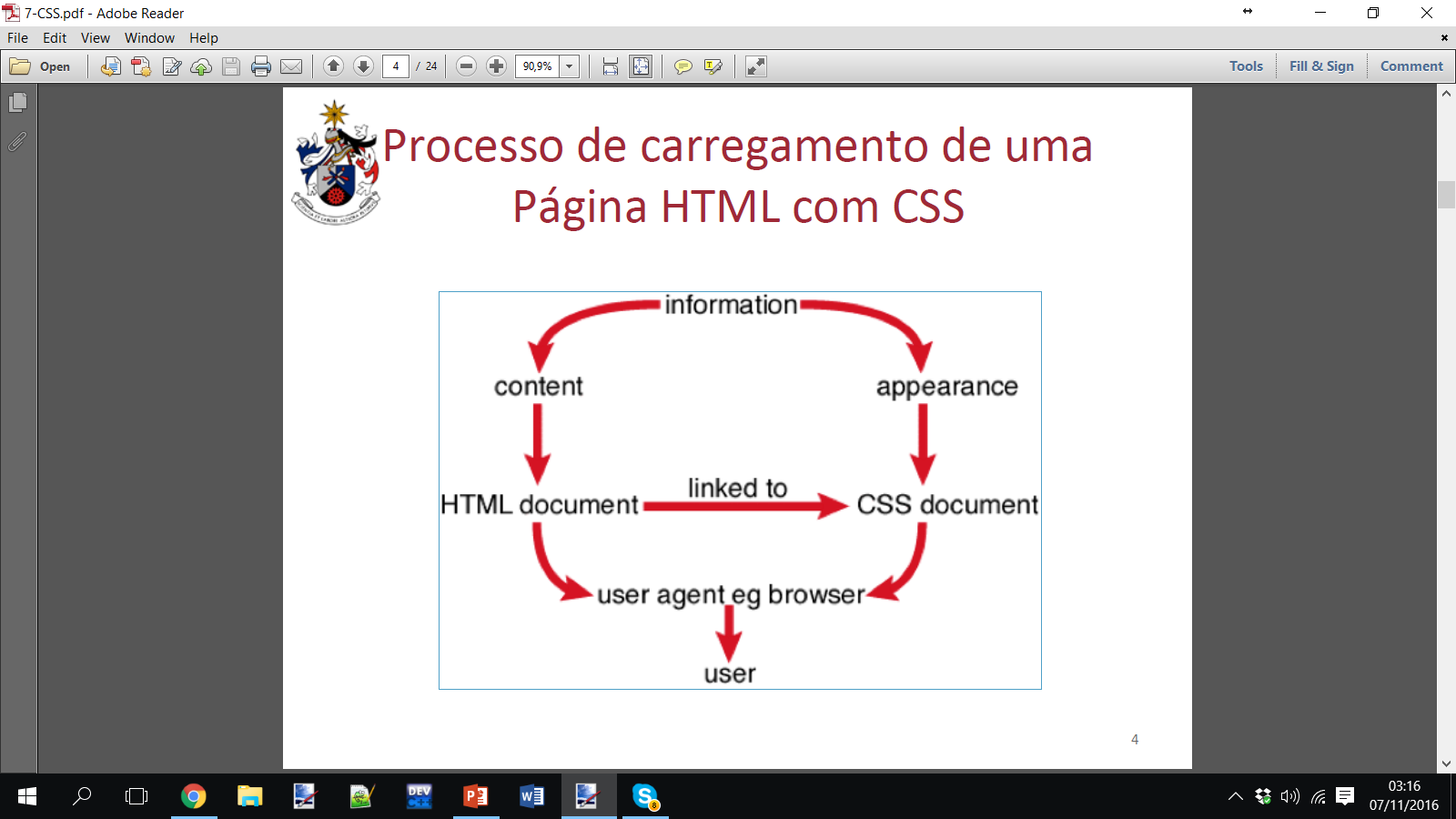


Figura 1 – Processo de carregamento de uma página HTML.

Explica-se de seguida a inserção de referências bibliográficas. Qualquer texto ou ideia que venha de uma referencia bibliográfica deve ser indicada com uma referência. Por exemplo, podemos referir que este trabalho se enquadra dentro do regulamento do Trabalho Final de Curso [DEISI21]. O hyperlink aponta para a referencia bibliográfica inserida relativa ao regulamento de TFC. Para sua criação deve:

1. escrever o texto que pretende na bibliografia
2. usar uma numeração adequada [], de forma a que respeite a ordem de aparecimento da referencia no texto.
3. selecionar a referencia inserida com o rato (por exemplo [2]) e escolher em Insert\Bookmark, criando um nome associado à referencia.

Depois, no texto onde pretender pode inserir a referencia através de Insert\Cross-reference.

1. O relatório final deverá incluir todos os conteúdos desenvolvidos ao longo do TFC [↑](#footnote-ref-1)
2. Para a entrega final sugere-se a inclusão, em anexo, de todo os planos de trabalho anteriores com apreciação de progresso e avaliação das dificuldades encontradas na elaboração e cumprimento do planeamento [↑](#footnote-ref-2)