Extended Abstract

Sistema de Integração Segura e Análise Automática de CCTV com Câmaras em Redes Não Controladas

1 - INTRODUÇÃO E ENQUADRAMENTO:

No panorama atual dos sistemas de videovigilância verifica-se uma grande dependência de hardware, como NVRs [Network Video Recorders] para agregar várias câmaras e disponibilizar *streaming* da sua imagem. A maioria destes dispositivos também possibilita o *playback* e exportação de vídeos gravados, sendo que alguns controlam ainda os acessos de utilizadores. A detecção de movimentos ou objetos é uma *feature* de apenas alguns modelos apesar de que, ultimamente, se têm verificado um grande crescimento e aposta tecnológica nesta área [https://ieeexplore.ieee.org/abstract/document/6491471]**.** Assim, os NVRs, embora raramente reúnam individualmente todas estas funcionalidades num dispositivo só [https://univates.br/revistas/index.php/destaques/article/view/2389], são a peça central do processo de videovigilância dentro de uma rede controlada.

Em determinados cenários [https://www.sciencedirect.com/science/article/pii/S1439179124000458], existe a impossibilidade destas câmaras serem inseridas todas numa determinada LAN [Local Area Network] privada. Por este motivo e por estarem numa outra rede não controlada, é necessário aceder via Internet, que origina alguns problemas, tais como:

- Incompatibilidade entre câmaras de diferentes fornecedores, obrigando muitas vezes à utilização de mais do que um software, já que nem todas são totalmente compatíveis com a mesma aplicação.
- Falta de segurança e de privacidade dos dados, uma vez que muitas destas câmaras recorrem a conexões P2P [Peer-to-Peer] quando acedidas fora da LAN. Este mecanismo depende, geralmente, de servidores do fornecedor, sobre os quais não existe controlo nem garantia de proteção dos dados [https://www.nozominetworks.com/blog/new-reolink-p2p-vulnerabilities-show-iot-security-camera-risks]. Além disso, a comunicação entre a aplicação e a câmara é frequentemente pouco segura e não encriptada, expondo a *stream* de vídeo e as credenciais a potenciais ataques.
- Falta de controlo de acessos e gestão de utilizadores, pois a maior parte das aplicações de acesso remoto a CCTV [Closed Circuit Television] são desenvolvidas para cenários onde estas atividades não são a prioridade [https://www.mdpi.com/1424-8220/23/4/1805] , priorizando o acesso intuitivo e rápido.

Para além destas barreiras técnicas e de segurança, emerge um desafio operacional extremamente relevante, particularmente no contexto da segurança pública. Entidades como os OPCs [Órgão de Polícia Criminal] dependem de videovigilância para a obtenção de provas. O processo atual, contudo, assenta frequentemente na revisão humana através da visualização integral contínua das gravações efetuadas, distribuindo muitas vezes intervalos de tempo por vários agentes para que seja facilitada. Esta informação foi obtida através de um questionário/entrevista, realizado em conjunto com agentes da investigação criminal da GNR[Guarda Nacional Republicana] e da PSP[Polícia de Segurança Pública], no qual o objetivo principal seria a validação da existência deste problema. O mesmo pode ser consultado no **ANEXO A**. Ainda assim, este processo torna-se demorado e intensivo, recorrendo a uma enorme quantidade de recursos humanos e tempo, que são valiosos e, infelizmente, escassos[https://www.dn.pt/sociedade/falta-de-policias-e-de-viaturas-e-instalacoes-e-equipamentos-em-mau-estado-relatorio-aponta-as-falhas-da-psp-e-gnr].

Uma vez que estes problemas trazem insegurança e ineficiência, resolvê-los é uma preocupação do encarregado de segurança e CCTV de uma entidade pública ou privada, tal como dos agentes encarregues pela obtenção de prova sob videovigilância dentro das polícias de investigação criminal. É neste contexto de múltiplos desafios que surge a proposta deste trabalho: o desenvolvimento do FUSE [Flexible Universal Stream Engine]. O FUSE é idealizado como uma plataforma de software que centraliza e organiza sistemas de videovigilância heterogéneos e geograficamente dispersos, com um foco integrado na segurança dos dados, na automatização da análise de vídeo, e na manutenção de registos de auditoria e gestão de utilizadores.

Importa ressalvar que o presente trabalho decorre em contexto empresarial, sendo acolhido pela empresa StabilityBubble, Lda. O FUSE não se configura apenas como um exercício académico teórico, mas sim como a proposta de uma plataforma comercial destinada a responder a lacunas de mercado identificadas pela empresa. Assim, esta dissertação visa conciliar o

rigor da investigação científica com os requisitos práticos e operacionais de um produto de software real, tirando partido da infraestrutura e know-how da entidade de acolhimento.

2 - PERGUNTA DE INVESTIGAÇÃO:

A proposta desta plataforma levanta a seguinte pergunta principais de investigação:

> **RQ1:** De que forma pode ser desenhada/projetada uma solução de software que permita aceder seguramente a câmaras CCTV, localizadas em redes externas não controladas, caracterizadas por uma elevada diversidade de arquiteturas, padrões tecnológicos e origem de fabrico?

Decompondo esta pergunta para uma melhor e mais estruturada compreensão, a investigação será guiada pelas seguintes sub-perguntas operacionais:

> **RQ1.1:** Como pode ser desenhada uma camada de abstração de software que normalize as funcionalidades (visualização, controlo, gravação) de câmaras de diferentes interfaces e especificações técnicas distintas, garantindo a extensibilidade futura do sistema?
>
> **RQ1.2:** Que mecanismos de rede e protocolos de comunicação são mais eficazes para garantir a confidencialidade e integridade da comunicação com câmaras localizadas em redes não fidedignas, sem introduzir vulnerabilidades na rede de destino e agregação das várias streams?
>
> **RQ1.3:** Em que medida a integração de modelos de visão computacional para a automatização da deteção de eventos pode validar a utilização da plataforma proposta para otimização de processos de investigação criminal?

A resposta à questão central de investigação (RQ1) será materializada através da implementação e validação experimental da plataforma FUSE. Todo o processo encontra-se detalhado no capítulo 5 referente à Metodologia. No entanto, para fundamentar as decisões técnicas necessárias na implementação do MVP[Minimum Viable Product] analisar-se-ão as sub-questões operacionais, no capítulo 4 do Estudo do Estado da Arte.

3 - OBJETIVOS:

Foram definidos o seguintes objetivos para o desenvolvimento e validação do FUSE:

- Desenvolver uma arquitetura de software extensível que, através de uma camada de abstração, normalize a comunicação com câmaras de diferentes fornecedores. O sistema deverá suportar um protocolo base de *streaming* como o RTSP[Real Time Streaming Protocol] e centralizar as funcionalidades de visualização em tempo real, gravação, e *playback* numa interface unificada.
- Implementar um modelo de comunicação seguro, *Secured By Design,* que utilize túneis VPN [Virtual Private Network] para isolar e criptografar a comunicação entre as câmaras externas e o servidor de implementação da aplicação.
- Desenvolver um sistema de controlo de acessos baseado em ações (modelo ABAC [Action/Attribute Based Access Control]) para gerir as permissões de utilizadores de forma granular e garantir a auditoria das ações.
- Integrar um módulo de análise de vídeo para a deteção automatizada de eventos complexos, implementando um pipeline de processamento progressivo em três fases:
  - **Fase 1** (Deteção de Atividade): Identificação de movimento e atividade relevante nos streams de vídeo para filtrar segmentos de interesse.
  - **Fase 2** (Classificação de Objetos): Análise dos segmentos filtrados para detectar e classificar objetos de categorias pré-definidas (e.g., humanos, veículos, animais).
  - **Fase 3** (Extração de Atributos): Análise aprofundada dos objetos classificados para extrair características específicas e customizáveis, como matrículas e cores de veículos, ou atributos de vestuário e acessórios de pessoas, que servirão de base para a pesquisa de eventos complexos.
- Validar a viabilidade da arquitetura através de um protótipo funcional (MVP [Minimum Viable Product]) que demonstre a integração bem-sucedida de, no mínimo, duas/três **(DECIDIR AINDA)** câmaras tecnologicamente diferentes, a

segurança da comunicação e a eficácia da deteção de eventos num cenário simulado, pelo menos até à Fase 2 anteriormente mencionada.

Quanto aos principais contributos deste trabalho, espera-se que do ponto de vista técnico-científico surja uma arquitetura referência para integração segura e inteligente de sistemas CCTV distribuídos, principalmente quando há a presença de interoperabilidade entre redes não controladas e controladas. Por outro lado, do ponto de vista social e operacional, tenciona-se validar a ferramenta para que esta possa vir a aumentar significativamente a eficiência e eficácia da investigação criminal dos OPC, otimizando a alocação de recursos e reduzindo o tempo de análise manual do vídeo.

4 - ESTUDO DO ESTADO DA ARTE:

Este capítulo apresenta a revisão de literatura fundamentada no âmbito do projeto, analisando o estado atual das tecnologias críticas para o desenvolvimento do FUSE. O objetivo principal desta revisão é responder às sub-questões operacionais previamente identificadas, nomeadamente a RQ1.1 e a RQ1.2, estabelecendo uma base teórica sólida para as decisões de arquitetura e segurança.

Adicionalmente, e dada a natureza aplicada da RQ1.3, é conduzido um estudo técnico aprofundado sobre os paradigmas atuais de visão computacional. Este estudo visa não apenas identificar o estado da arte, mas também comparar padrões, *pipelines* de processamento e modelos de Inteligência Artificial (IA) passíveis de integração na plataforma.

4.1 - Processo de Investigação

O Processo de investigação foi guiado pelo mapeamento das duas primeiras sub-questões da presente dissertação em questões de pesquisa com foco na revisão literária, conforme descrito na tabela 1.

Tabela 1 - Questões de Pesquisa Orientadas à Revisão Literária

Research Question ID	Literature Review Research Question ID	Description	Tópicos e *Keywords* de pesquisa
RQ1.1	LRRQ1	Quais são as arquiteturas de referência e padrões de *design* de software descritos na literatura para a abstração e interoperabilidade de dispositivos IoT[Internet of Things] heterogéneos? **MUITO ABRANGENTE? DEFINO IOT AQUI PELA PRIMEIRA VEZ OU FALO ANTES?**	*IOT Interoperability, Hardware Abstraction Layer, Middleware patterns, ONVIF standardization, Heterogeneous device integration.*
RQ1.2	LRRQ2	Qual o estado da arte em protocolos de comunicação segura e VPNs para acesso remoto e *streaming*?	*Secure Tunneling Protocols , VPN performance analysis, Streaming encryption, NAT Traversal, Zero Trust Network Access.*

Cada questão de pesquisa será enquadrada de acordo com o modelo PICOCS[Population, Intervention, Comparison, Outcomes, Context, Study][https://dl.acm.org/doi/abs/10.1145/2830719.2830732], garantindo o rigor na seleção das fontes utilizadas. A informação será depois selecionada seguindo o fluxo PRISMA[Preferred Reporting Items fot Systematic reviews and Meta-Analysis][https://www.sciencedirect.com/science/article/pii/S1743919110000403]. O processo inclui a definição de keywords de pesquisa, a aplicação estrita de critérios de inclusão e exclusão, seguida de uma filtragem em etapas e, finalmente, uma discussão crítica sobre a aplicabilidade dos estudos selecionados para a arquitetura do FUSE. Como fator inclusivo de seleção, selecionou-se, por exemplo, a data de publicação posterior a 2018. A escolha deste intervalo visa garantir que as arquiteturas, *frameworks* e algoritmos analisados representam o atual estado da arte, evitando a adoção de paradigmas que, embora válidos no passado, não refletem as necessidades de desempenho e escalabilidade dos sistemas modernos. Foram privilegiados artigos revistos por pares, normas técnicas e literatura técnica amplamente reconhecida. Excluíram-se estudos puramente teóricos sem aplicação prática ao domínio da videovigilância ou da integração de dispositivos, tal como trabalhos relativos a soluções proprietárias fechadas sem documentação técnica pública suficiente.

4.2 - Estado da Arte em Visão Computacional

Relativamente à terceira sub-questão, a RQ1.3, referente à automatização da análise de vídeo, optou-se por uma abordagem de Revisão Narrativa e Exploratória, como descrita por Maria J. Grant e Andrew Booth em [https://onlinelibrary.wiley.com/doi/full/10.1111/j.1471-1842.2009.00848.x] como "*State-of-the-art review*" . Esta modalidade metodológica caracteriza-se pela sua flexibilidade na análise crítica da literatura atual, permitindo identificar conceitos-chave, padrões arquiteturais e soluções técnicas emergentes sem a rigidez protocolar de uma revisão sistemática e formal.

Esta opção justifica-se pela vertiginosa evolução dos modelos de IA (Inteligência Artificial) e pela necessidade de analisar não apenas literatura académica clássica, mas também documentação técnica de modelos recentes e *benchmarks* da indústria. A análise encontra-se segmentada em três domínios fundamentais que correspondem às fases da *pipeline* de processamento proposta para o FUSE:

- Deteção de Movimento (Fase 1)
- Deteção de Objetos (Fase 2)
- Visual-Language Models - VLMs (Fase 3)

Apesar da natureza exploratória, esta pesquisa manterá o rigor científico na seleção de fontes, priorizando publicações de menos de 1 ano, dado o exponencial e recente crescimento tecnológico da área, e repositórios *open-source* com forte validação comunitária. A pesquisa foi orientada pelas seguintes *keywords*, agrupadas por domínio:

- **Fase 1 (Pré-processamento):** *Background Subtraction*, *Motion Detection Algorithms*, *Frame Differencing efficiency*, *Video Activity Detection*.
- **Fase 2 (Classificação):** *Real-time Object Detection*, *YOLO architecture*, *One-stage detectors*, *CNN inference optimization*, *Edge AI*.
- **Fase 3 (Extração de Atributos):** *Vision-Language Models (VLMs)*, *Multimodal AI*, *Zero-Shot Learning*, *Open-vocabulary detection*, *Visual Question Answering*.

4.2.1 - Deteção de Movimento e Filtragem Temporal

A primeira etapa da revisão incidirá sobre métodos de pré-processamento e filtragem de vídeo, essenciais para a eficiência global do sistema. O estudo focará na comparação entre algoritmos clássicos de processamento de imagem (baseados em diferenças de pixéis e estatística de cena) e abordagens mais modernas de "lightweight AI". O objetivo principal será identificar técnicas capazes de filtrar eficazmente segmentos de vídeo sem atividade relevante, minimizando o uso de recursos computacionais (CPU/GPU) e garantindo robustez face a mudanças de iluminação ou ruído visual, sem descartar falsos negativos críticos. A literatura evidencia uma divisão clara entre abordagens clássicas de processamento de imagem, que privilegiam a eficiência computacional e simplicidade de implementação, e abordagens baseadas em modelos leves de IA, que oferecem maior robustez semântica à custa de maior complexidade. Esta tensão entre eficiência e capacidade de generalização constitui um dos principais trade-offs analisados nesta fase da *pipeline*.

4.2.2 - Deteção e Classificação de Objetos (Object Detection)

Neste domínio, a literatura será analisada com foco em arquiteturas de Redes Neuronais Convolucionais (CNNs) otimizadas para inferência em tempo real. Será dado destaque preponderante à análise da família de arquiteturas YOLO[*You Only Look Once]*[https://github.com/ultralytics/ultralytics], atualmente considerada o padrão de indústria para o equilíbrio entre velocidade e precisão[https://www.sciencedirect.com/science/article/abs/pii/S1568494624006951]. O estudo comparativo visará determinar qual a versão ou variação desta arquitetura melhor se adequa aos requisitos forenses do projeto, avaliando métricas como a capacidade de deteção de objetos pequenos ou distantes e o desempenho em *hardware* com recursos limitados. Os estudos analisados preliminarmente revelam um debate recorrente entre arquiteturas altamente precisas, mas computacionalmente exigentes, e modelos otimizados para inferência em tempo real.

4.2.3 - Modelos de Visão-Linguagem (Vision-Language Models)

Por fim, explora-se a fronteira mais recente da Inteligência Artificial: a integração entre visão computacional e processamento de linguagem natural. A revisão abordará o estado da arte dos VLMs, analisando arquiteturas multimodais recentes, como por exemplo a família Qwen-VL, entre outras emergentes. O foco da investigação será compreender como estes modelos permitem a extração de atributos complexos e a realização de pesquisas em linguagem natural, avaliando a sua viabilidade de integração num *pipeline* local em termos de latência e exigência de memória.

4.3 - Identificação da Lacuna Literária

Da análise preliminar da literatura resulta uma lacuna clara: embora existam estudos sólidos sobre integração de dispositivos IoT, protocolos de comunicação segura e modelos avançados de visão computacional, estes domínios são maioritariamente abordados de forma isolada. Verifica-se a ausência de uma arquitetura integrada que combine, de forma sistemática, a interoperabilidade segura de câmaras CCTV localizadas em redes não controladas com *pipelines* de análise automática de vídeo orientadas a contextos forenses. É precisamente nesta interseção, entre segurança de comunicação, abstração de *hardware* heterogéneo e inteligência analítica aplicada, que o presente trabalho se posiciona.

5 - METODOLOGIA :

A metodologia adotada para a realização deste trabalho académico baseia-se no modelo de "*Research Process*" proposto por B. J. Oates no Livro "Researching Information Systems and Computing" [https://dokumen.pub/researching-information-systems-and-computing-978-1-4129-0223-6.html] , ilustrado na Figura 1. A imagem foi retirada do documento original e editada, de forma a sublinhar os tópicos que se aplicam para este projeto.

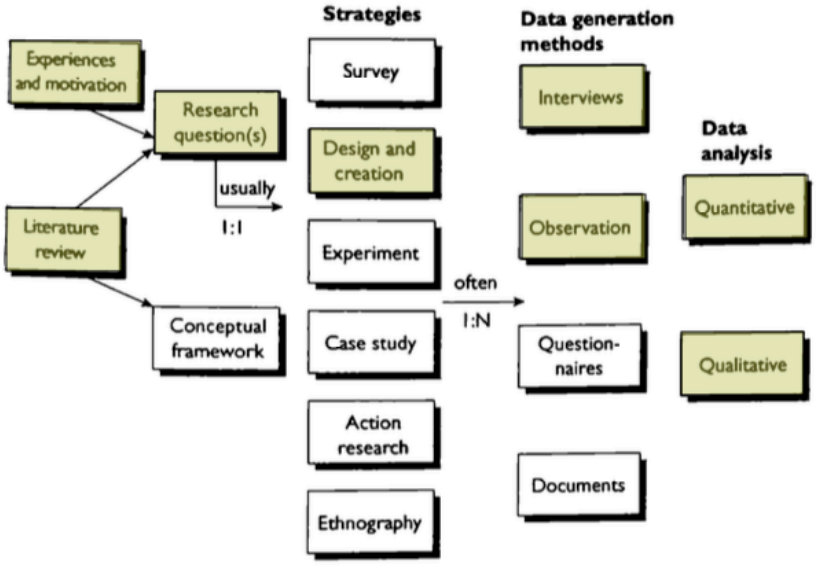

Figura 1 - Diagrama de "Research Process" de B. J. Oates, aplicado ao contexto do projeto

O ponto de partida da investigação enquadra-se em "***Experiences and motivation***", dado que a génese deste projeto deriva diretamente da observação da ineficiência e limitações técnicas enfrentadas pelos OPC e gestores de segurança a recolha de imagens de CCTV. Através de feedback adquirido através de questionários e entrevistas com Núcleos (GNR) e Esquadras (PSP) de Investigação Criminal (Anexo A), estes problemas são confirmados e registados. Complementarmente, é realizada uma *"Literature Review"* preliminar para compreender o estado da arte em protocolos de comunicação e visão computacional. Esta análise permitiu identificar a ausência de soluções integradas que garantam simultaneamente segurança em redes hostis e inteligência analítica avançada. A junção desta necessidade prática (experiência) com a identificação desta lacuna teórica (literatura) resultou na formalização das "***Research Questions***" apresentadas anteriormente.

A estratégia central adotada para este trabalho é a de "***Design and Creation***". Esta abordagem é a mais adequada para projetos de Engenharia de Software cujo objetivo primário é o desenvolvimento de um protótipo que visa resolver muitos dos problemas práticos observados e identificados em determinado cenário, como forma de validação de futura implementação ou desenvolvimento de algo mais avançado. Dentro desta estratégia inserem-se 4 principais passos, nomeadamente *Design*, Desenvolvimento, Testes e Conclusões. No ***Design***, o foco será a proposta de arquitetura a seguir no passo seguinte de **Desenvolvimento**, que terá como principal objetivo a implementação do protótipo (MVP) e da pipeline de análise de vídeo. Seguidamente procede-se aos **Testes**, que incluirão uma avaliação da consistência e

qualidade do código, tal como implementação em cenário real, que possibilitará a obtenção de resultados para que estes venham a ser interpretados na secção de **Conclusões**.

Relativamente aos resultados e à sua avaliação, será usado o método de "***Interviews***" com utilizadores finais, sendo estes OPCs ou encarregados de segurança de uma outra entidade, de modo a recolher feedback e validação do funcionamento do protótipo e respetiva utilidade do mesmo. Em adição, será também usado o método de "***Observation***", onde se poderá obter e quantificar resultados e taxas de correspondência na análise automática de eventos e objetos.

Quanto à análise de dados, optou-se por uma abordagem mista que integra os dois métodos disponíveis "***Quantitative***" e "***Qualitative***". A análise quantitativa incidirá sobre as métricas técnicas recolhidas durante os testes do protótipo, tais como as taxas de precisão e alerta na deteção e classificação de objetos (Fase 2 e 3 da *pipeline*), a latência do *streaming* via túnel VPN, os tempos de processamento da análise de vídeo, entre outros. Já a análise qualitativa será aplicada à interpretação do *feedback* dos utilizadores e das observações de cenário real, avaliando o impacto operacional da ferramenta, a eficácia percebida na redução do tempo de investigação e a adequação da interface aos processos de trabalho dos OPC.

6 - PLANEAMENTO DE TRABALHO:

Este capítulo descreve o planeamento deste projeto, que foi estruturado para garantir a exequibilidade dos objetivos propostos dentro do prazo académico estipulado. A organização das atividades divide-se entre a fase de preparação (unidade curricular de PREPD) e a fase de execução e escrita da dissertação (unidade curricular de DIMEI).

6.1 - Definição do Âmbito e Entregáveis

O âmbito deste projeto foi decomposto através de um WBS[Work Breakdown Structure]. Pelo mesmo, ilustrado na Figura 2, estão organizados os entregáveis previstos por cinco fases principais, sendo estas:

1. **Planeamento e Análise:** Focada na definição do problema e estado da arte. Inclui entregáveis como o *Project Charter*, o próprio WBS, um *Gantt Chart*, um questionário e respetivas respostas dos OPC, este *Extended Abstract e* a revisão da literatura incluída no mesmo.
2. **Design:** Dedicada à modelação da solução. Os principais entregáveis previstos são a documentação da Arquitetura de Software (Vistas 4+1) e o Modelo de Domínio, assegurando que a estrutura do FUSE é robusta antes da implementação.
3. **Desenvolvimento:** Fase central do projeto, onde será implementado o código da aplicação. Divide-se em três módulos críticos:
   - **Comunicações Seguras:** Escolha e implementação de protocolos e túneis VPN.
   - **Camada de Abstração:** Normalização dos diferentes fabricantes de câmaras.
   - **Módulo de Análise de Vídeo:** Desenvolvimento das *pipelines* de deteção (bifásica para o MVP e trifásica se o tempo permitir).

   Dos entregáveis previstos para esta fase fazem parte o código da aplicação, a *pipeline* bifásica e a documentação de procedimento de acesso e protocolos escolhidos na comunicação. Caso seja possível dentro do período previsto para o desenvolvimento e entrega do trabalho, ainda será entregue a *pipeline* trifásica.
4. **Testes:** Validação da solução através de testes unitários e funcionais, em conjunto com a validação do protótipo em ambiente controlado ou cenário-real que resultará na produção de um relatório de *feedback* adquirido.
5. **Conclusões:** Considerações finais do projeto. Os entregáveis que fazem parte da conclusão são a redação final da dissertação, a interpretação dos resultados e a apresentação final.

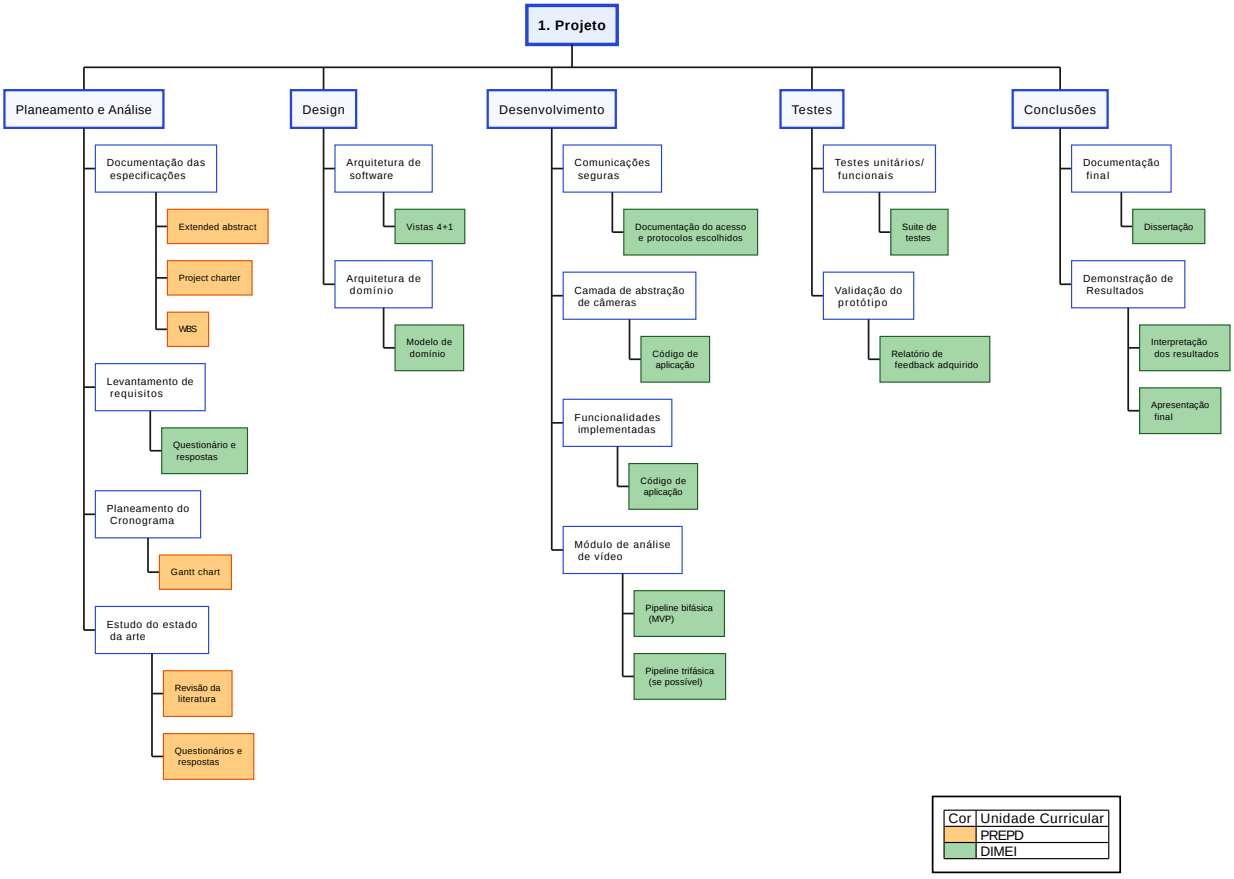

Figura 2 - WBS

6.2 - Plano de Trabalho

O objetivo desta secção é ilustrar e descrever a calendarização das entregas dos respetivos entregáveis mencionados anteriormente, garantindo um acompanhamento rigoroso do progresso do projeto. O planeamento temporal encontra-se representado no diagrama de Gantt, Figura 3, que estabelece a sequência lógica e as datas-alvo para a conclusão de cada artefacto, dividindo-se em dois grandes marcos temporais associados às unidades curriculares de PREPD e DIMEI.

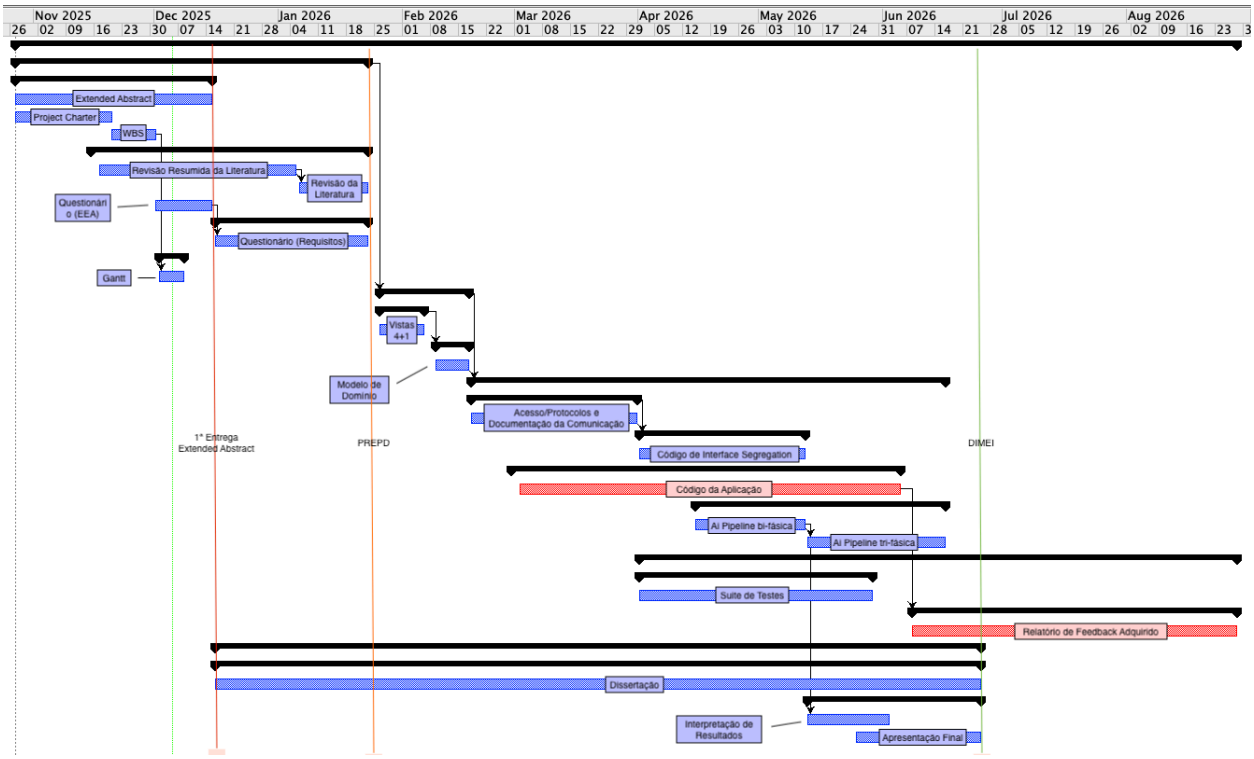

Figura 3 - Gantt Chart

A execução do cronograma inicia-se com um primeiro marco de controlo a 15 de dezembro de 2025. Para esta data, está prevista a entrega do conjunto documental de planeamento, que inclui este *Extended Abstract*, o WBS e o Planeamento Temporal (Gantt). Adicionalmente, será submetida uma revisão resumida da literatura, incluída no *Extended Abstract* e os resultados preliminares do questionário, focados especificamente na validação da necessidade do projeto junto do público-alvo.

O encerramento da fase de planeamento (PREPD) está estipulado para 7 de janeiro de 2026. Esta entrega consolidará toda a etapa de "Planeamento e Análise", incluindo a versão final e completa da Revisão da Literatura e o levantamento de requisitos detalhado, resultante do adicional preenchimento dos questionários. A nível de estrutura documental, prevê-se que a dissertação esteja redigida até à fase de pré-Design, estabelecendo a fronteira académica para o início do desenvolvimento técnico.

O segundo grande bloco temporal, referente à unidade curricular de DIMEI, tem como data-alvo de entrega final o dia 22 de junho de 2026 [**CONFIRMAR**]. Este período compreende a execução integral das fases de "Design", "Desenvolvimento", "Testes" e "Conclusões". Até esta data, espera-se a conclusão da arquitetura, a implementação do protótipo FUSE e a respetiva bateria de testes técnicos, que possibilitará a obtenção de resultados e interpretação dos mesmos de modo a validar e avaliar a solução final.

Importa ressalvar uma exceção prevista no planeamento referente à validação em cenário real. Dada a dependência de terceiros e a complexidade logística de implementação em ambiente operacional, admite-se que esta componente específica da fase de testes possa estender-se para além da data limite de entrega académica (22 de junho), funcionando como uma etapa de validação contínua e recolha de métricas pós-entrega da dissertação.

6.3 - *Project Charter* e Gestão de Riscos

O *Project Charter* constituiu o artefacto inicial deste projeto, servindo como primeiro documento para a formalização da proposta de dissertação junto da empresa acolhedora e da instituição académica. Dada a sua natureza preliminar, este documento apresentou uma visão inicial do problema e dos objetivos que, embora alinhados com a missão do FUSE, se revelaram amplos, tendo sido posteriormente refinados e concretizados no WBS e no plano de trabalhos detalhado anteriormente. As datas e entregáveis originais constantes no *Charter* foram, por conseguinte, ajustados para refletir um mais correto e detalhado planeamento. Apesar destes ajustes, o *Project Charter* mantém-se como a referência central para

a identificação das partes interessadas (*Stakeholders*). A Tabela 2 apresenta o mapeamento atualizado dos *Stakeholders*, classificando-os quanto ao seu poder de influência e nível de interesse no sucesso do projeto. Destaca-se a inclusão da *StabilityBubble*, cuja posição estratégica evolui para fornecedor potencial do *software* pós-desenvolvimento, e a exclusão de entusiastas de *Home Automation*, inicialmente projetados como possível público-alvo. Esta exclusão dá-se devido à grande apropriação do FUSE a entidades e OPCS, dado que se torna uma solução demasiado desenvolvida para projetos caseiros e pequenos.

Para a classificação dos *Stakeholders*, utilizou-se como base a "Mendelow's Matrix" [https://aisel.aisnet.org/icis1981/20/]. A atribuição dos níveis ('Alto', 'Médio', 'Baixo') obedeceu aos seguintes critérios:

- **Poder:** Capacidade da entidade em influenciar decisões, alocar recursos ou bloquear o andamento do projeto.
- **Interesse:** Grau de impacto que os resultados do projeto terão nas operações ou estratégia da entidade.

Tabela 2 - Stakeholders identificados

Nome	Poder	Interesse	Justificação
StabilityBubble / NovaForensic	Alto	Alto	Entidade promotora e futura fornecedora/exploradora comercial da solução FUSE.
Órgãos de Polícia Criminal (OPC)	Alto	Alto	Utilizadores finais críticos; o seu *feedback* valida a utilidade operacional e requisitos forenses.
Paulo Baltarejo Sousa (Orientador)	Alto	Médio	Orientação académica e validação científica da metodologia e resultados.
Francisco Loureiro (Supervisor)	Alto	Alto	Supervisão empresarial e alinhamento do produto com a estratégia de mercado.
Gestores de Segurança	Médio	Médio	Potenciais clientes empresariais que beneficiam da centralização de sistemas CCTV.
Fornecedores de Câmaras	Baixo	Baixo	O FUSE visa a eliminar a dependência de um só fornecedor, que tanto pode ser um novo fator decisivo para a escolha do fabricante.

Relativamente à gestão de riscos, trata-se de um processo contínuo que se iniciou com o levantamento preliminar no *Project Charter*. Embora a análise inicial focasse riscos mais genéricos (e.g., dependência de *hardware*), o planeamento aprofundado permitiu identificar ameaças mais específicas e definir estratégias de mitigação concretas. A Tabela 3 consolida os riscos, atribuindo-lhes uma probabilidade e um impacto, combinando alguns identificados na fase inicial com novos riscos técnicos decorrentes da complexidade da análise de vídeo e integração de redes. A quantificação do risco segue uma matriz de probabilidade e impacto (P×I), onde ambas as variáveis são classificadas numa escala de Likert[https://psycnet.apa.org/record/1933-01885-001] de 1 a 5. Esta escala foi definida da seguinte forma:

- Probabilidade (P): 1 representando um acontecimento raro ou extremamente improvável, e 5 algo que seja extremamente provável acontecer, possivelmente previsto.
- Impacto (I): 1 compreende uma insignificância ou ligeiro atraso, enquanto que 5 impacta criticamente, possivelmente impossibilitando o projeto ou condicionando o resultado do mesmo.

A multiplicação destes fatores resulta no Risco Quantificado, permitindo priorizar as estratégias de mitigação para as ameaças com pontuação mais elevada, conforme demonstrado na Tabela 3.

Tabela 3 - Identificação e gestão de riscos associados ao projeto

ID	Descrição	Causa	Probabilidade (P)	Impacto (I)	Risco Quantificado (P*I)	Resposta
1	**Indisponibilidade de Hardware (GPU)**	A análise de vídeo requer *hardware* gráfico potente, que é escasso ou não disponível	3	4	12	**Mitigar:** Garantir que a integração com a *pipeline* de análise automática é feita

		durante o decorrer do trabalho				de forma modular e desacoplada, permitindo a flexibilidade da escolha do modelo de AI utilizado conforme o hardware disponível no momento.
2	**Incompatibilidade de Protocolos**	Determinada câmara não suporta o protocolo RTSP, impossibilitando a integração prevista.	2	2	4	**Aceitar:** Focar o MVP na compatibilidade estrita com RTSP, Excluindo câmaras que não suportem.
3	**Falsos Positivos na Deteção**	Pipeline de IA gera demasiados alertas falsos em condições adversas (chuva, noite).	3	3	9	**Mitigar:** Implementar um sistema de ajuste de sensibilidade configurável pelo utilizador (ex: segundos necessários de deteção do objeto antes do alerta)
4	**Atraso no Cronograma**	A complexidade da integração de múltiplos sistemas excede o tempo previsto para o semestre letivo.	3	5	15	**Mitigar:** Adotar uma abordagem de desenvolvimento incremental, assegurando a estabilidade do núcleo de visualização e deteção básica (*pipeline* bifásica) como um MVP robusto, antes de iterar para as funcionalidades avançadas de extração de atributos (pipeline trifásica), que devem ser tratadas como trabalho futuro se o seu desenvolvimento se revelar incompatível com o tempo disponível para o mesmo.

Pela análise à Tabela 3, destaca-se os 1º e 4º riscos, Indisponibilidade de Hardware (GPU) e Atraso no Cronograma, com os índices de risco mais elevados sendo eles 12 e 15, respetivamente. Por consequente, conclui-se que grande parte do sucesso do projeto e dos resultados obtidos dependerão intrinsecamente da gestão rigorosa dos recursos computacionais e do cumprimento dos prazos estipulados, bem como o seguimento do planeamento efetuado.

A estratégia de mitigação para estes riscos prioritários assenta fundamentalmente na modularidade e no desenvolvimento incremental. Ao garantir que a arquitetura do sistema é flexível quanto aos modelos de IA (Risco 1) e que as funcionalidades são entregues por fases (Risco 4), assegura-se que, mesmo na eventualidade destes riscos se materializarem, o projeto resultará sempre num produto funcional (MVP), salvaguardando a dissertação. Por outro lado, o risco de Incompatibilidade de Protocolos (Risco 2) apresenta o menor impacto e risco quantificado (4). A opção pela estratégia de "Aceitação" serve aqui para delimitar claramente o âmbito do projeto: o MVP a ser desenvolvido no âmbito do projeto não pretende ser universalmente compatível com todo o conjunto de câmaras existentes, mas sim provar o conceito através de um protocolo *standard* habitualmente presente (RTSP), permitindo focar o esforço de engenharia na inteligência do sistema e não na compatibilidade de *drivers*. A monitorização destes riscos será realizada periodicamente em cada reunião de ponto de situação com o orientador e supervisor, permitindo o ajuste dinâmico das estratégias de resposta caso a probabilidade ou impacto de algum fator sofra alterações ao longo do ciclo de vida do projeto.

7 - ETICA:

A realização deste trabalho rege-se pelos princípios de integridade, responsabilidade e rigor científico descritos no Código de Boas Práticas e de Conduta do P.PORTO [https://www.ipp.pt/comunidade/missao-equidade-diversidade-inclusao/DespachoP.PORTOP0402020CodigodeBoasPraticasedeConduta.pdf].

Do ponto de vista profissional, o trabalho enquadra-se nos princípios estruturantes da engenharia de software, alinhados com referências internacionais como o *Software Engineering Code of Ethics and Professional Practice*, desenvolvido em conjunto pela ACM[Association for Computer Machinery] e pela IEEE-CS[Institute of Electrical and Electronics Engineers Computer Society] (https://www.acm.org/code-of-ethics/software-engineering-code). A conformidade com estes princípios garante a qualidade e segurança dos sistemas desenvolvidos, a responsabilidade perante clientes e utilizadores, e a honestidade na comunicação de resultados, limitações e riscos associados às soluções tecnológicas.
O FUSE envolve uma *pipeline* de análise automática aplicada a contextos de videovigilância, potencialmente incidindo sobre a obtenção de dados pessoais identificáveis. Estes dados sensíveis apenas serão obtidos num contexto de validação do MVP em cenário real, que estará sempre salvaguardado por requerimento de despacho judicial para fornecimento de meios técnicos e respetiva autorização de captação de imagem. Ainda assim, a *pipeline* é desenhada em estrita observância do *EU AI Act* [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai], garantindo que o sistema não incorre em '*Unacceptable risks*'. O sistema não se destina, nem permite, práticas proibidas tais como:

- *Social scoring* ou manipulação comportamental;
- Recolha indiscriminada (*untargeted scraping*) de imagens de CCTV para criação de bases de dados de reconhecimento facial;
- Identificação biométrica remota em tempo real em espaços públicos para fins policiais (*real-time remote biometric identification*).

No âmbito do último ponto, apesar do alvo ser legislar o reconhecimento biométrico em tempo-real, justifica-se a conformidade pela natureza da análise automática, que será realizada sob gravações dos eventos, e não sob o próprio *streaming.*

A análise focada na "Fase 3" da pipeline de deteção automática restringe-se à classificação de características objetivas (e.g., cor de vestuário, tipo de veículo) para auxiliar a pesquisa forense, mantendo sempre o princípio da validação humana, onde a decisão final cabe ao agente humano e não ao algoritmo.

8 - BIBLIOGRAFIA

Para o Extended Abstract, os links para os artigos/sites estão disponíveis junto dos temas. Posteriormente serão formatados em rigor às normas aplicadas.

9 - ANEXO

Anexo não disponível para o extended abstract.