**AVISO DE ABERTURA DE CONCURSO**

**INVESTIMENTO C05-i08.02 – Inteligência Artificial na Administração Pública**

**N.º 02/C05-i08.02/2025**

**Desenvolvimento de soluções setoriais de Inteligência Artificial para a Administração Pública**

**25-07-2025**

**ÍNDICE**


1. Preâmbulo ..... 3
2. Objetivos e Tipologia de Operações ..... 3
3. Condições de acesso e de elegibilidade dos Beneficiários Finais ..... 4
4. Área geográfica de aplicação ..... 6
5. Regras e limites à elegibilidade de despesas ..... 6
6. Taxa de financiamento e limite do apoio ..... 7
7. Dotação do fundo a conceder ..... 7
8. Condições de atribuição de apoio financeiro ..... 7
9. Modo de apresentação das candidaturas ..... 8
10. Critérios de seleção de Candidaturas ..... 8
11. Identificação das entidades que intervêm no processo de decisão do financiamento. ..... 8
12. Prazo para apresentação de candidaturas ..... 9
13. Procedimentos de análise e decisão de candidatura ..... 9
14. Contratualização ..... 9
15. Tratamento de Dados Pessoais ..... 10
16. Divulgação de resultados e pontos de contato ..... 10

ANEXO I – PROJETOS E ENTIDADES CONVIDADAS ..... 11

ANEXO II – PROCESSO DE SELEÇÃO DE CASOS DE USO ..... 12

ANEXO III – FICHAS DE CARATERIZAÇÃO DE PROJETO E DE PRODUTO ..... 14

ANEXO III.1 – FICHA DE CARATERIZAÇÃO DE PROJETO 1 ..... 14

ANEXO III.2 – FICHA DE CARATERIZAÇÃO DE PROJETO 2 ..... 19

ANEXO III.3 – FICHA DE CARATERIZAÇÃO DE PROJETO 3 ..... 25

## 1. Preâmbulo

Agência para a Modernização Administrativa, I.P. (AMA) é o instituto público responsável pela promoção e desenvolvimento da modernização administrativa em Portugal. A sua atuação divide-se em três eixos: Transformação Digital, Serviço Público Omnicanal e Simplificação Administrativa., encontrando-se sob superintendência e tutela do Secretário de Estado da Digitalização.

A matéria de Inteligência Artificial (IA) é posicionada pelo Governo como uma temática estratégica para o país, razão pela qual a Agenda Nacional de IA figura como uma das 16 iniciativas da Estratégia Digital Nacional (EDN).

A Agenda Nacional de IA reunirá as principais ações estratégicas a desenvolver nos próximos anos. Nestas ações, estão enquadradas as medidas já anunciadas como (i) o desenvolvimento de um Modelo de Linguagem em Grande Escala em língua portuguesa de Portugal, (ii) a criação de uma fábrica de IA em território nacional, e (iii) a aquisição de capacidade computacional dedicada ao desenvolvimento, inovação e investigação na matéria de IA, para que possa ser utilizada por entidades e empresas na implementação de soluções neste domínio.

Na dimensão da Administração Pública, identifica-se a necessidade de apoiar entidades no desenvolvimento de soluções disruptivas fornecendo o apoio financeiro necessário para que estas possam ter o impacto desejado na vida das pessoas e das empresas. A IA abre oportunidades ímpares de transformação das entidades e organismos da Administração Pública, com um grande potencial de aumento de eficiência de processos, de melhorar a qualidade dos serviços públicos e a incrementar a capacidade de resposta das mesmas.

## 2. Objetivos e Tipologia de Operações

Com este investimento pretende-se financiar o desenvolvimento de soluções estruturais e transformadoras, em que o seu mérito será medido pela capacidade de impacto na vida das pessoas e das empresas.

Pretende-se por isso, o investimento no desenvolvimento de soluções de IA em processos da Administração Pública, de forma a melhorar a eficiência/qualidade dos processos internos da

Administração Pública, com vista a redução de custos, ou a melhoria da transparência e qualidade dos serviços de atendimento aos cidadãos e às empresas.

A IA pode ter um impacto significativo nas políticas e na disponibilização de serviços públicos. Entre outros benefícios destaca-se:

- o potencial de reduzir o tempo necessário para executar tarefas pelo ser humano, criando disponibilidade para a realização de trabalho de alto valor;
- o aumento de produtividade e eficiência nas ações, conseguindo maior consistência que o ser humano;
- a capacidade de interpretar e processar grandes quantidades de dados, identificando e relacionando padrões;
- a projeção de melhores e mais sustentadas políticas e decisões;
- a simplificação da comunicação e o envolvimento dos cidadãos;
- a rapidez e a melhoria da qualidade dos serviços públicos;
- e a criação de emprego.

O presento Aviso-convite permitirá assegurar o cumprimento da seguinte meta do PRR, nomeadamente:

- Conclusão e entrada em produção de 6 soluções de IA em processos da Administração Pública.

## 3. Condições de acesso e de elegibilidade dos Beneficiários Finais

Para efeitos do presente Aviso-convite são beneficiários finais as entidades da Administração central do Estado, as entidades da Administração desconcentrada do Estado, as entidades públicas empresariais, outros níveis da Administração ou outras entidades públicas, no âmbito das suas atividades sem fins lucrativos, ao abrigo de protocolos celebrados com a Administração central, incluindo a desconcentrada, previamente identificadas no Anexo I, que reúnam as seguintes condições cumulativas de acesso:

A. <u>Condições gerais de acesso:</u>

a) Ter a situação tributária e contributiva regularizada perante Administração Fiscal e a Segurança Social, a verificar até ao momento da assinatura do Termo de Aceitação;

b) Ter a situação regularizada em matéria de reposições, no âmbito dos financiamentos dos Fundos Europeus;

c) Cumprimento dos princípios horizontais para a promoção da igualdade de género entre homens e mulheres e da igualdade de oportunidades e não discriminação;
d) Cumprimento das regras de contratação pública, nomeadamente o Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual e normativos comunitários sobre a matéria;
e) Conforme estabelecido no Regulamento do Mecanismo de Recuperação e Resiliência (MRR) é obrigatório o respeito do princípio *Do No Significant Harm* (DNSH) que significa não apoiar ou realizar atividades económicas que causem danos significativos a qualquer objetivo ambiental na aceção do Artigo 17.º do Regulamento (UE) 2020/852 do Parlamento Europeu e do Conselho (Regulamento da Taxonomia da UE);
f) Cumprir os requisitos de informação, comunicação e publicidade relativos à origem do financiamento, conforme disposto no n.º 2 do artigo 34.º do Regulamento (UE) 2021/241 do Parlamento Europeu e do Conselho de 12 de fevereiro de 2021, que criou o MRR;
g) A candidatura efetuada no contexto do presente aviso não pode ter sido objeto de outro financiamento no âmbito dos Fundos Europeus nos últimos 5 anos, condição a confirmar à data da assinatura do Termo de Aceitação.

B. <u>Condições específicas de acesso da candidatura:</u>
   a) Cada candidatura implica obrigatoriamente a conclusão e entrada em produção da solução de IA em processos da Administração Pública objeto de financiamento;
   b) Disponibilização da documentação, produzida no âmbito do projeto, necessária à disseminação e replicabilidade do mesmo por outras entidades da Administração Pública;
   c) Cumprimento dos termos referidos no Anexo III – Ficha de Caraterização de Projeto e do Produto;
   d) Cumprimento do cronograma das atividades, nos termos descritos no respetivo Anexo III, desde a fase de concurso até à entrada em produção (a entrada em produção não pode ultrapassar 30 de junho de 2026);

O não cumprimento das condições gerais e específicas de acesso da candidatura, determina a não elegibilidade da candidatura.

Todas as condições gerais e específicas de acesso acima referidas devem ser reportadas à data da candidatura.
A seleção das entidades convidadas seguiu a metodologia descrita no Anexo II.

De acordo com os marcos e metas relevantes para comprovar a execução do PRR, a execução física do objeto deste Aviso deverá ser até 30 de junho de 2026, sendo que a sua execução financeira poderá ser até 30 de setembro de 2026, com a apresentação de todas as faturas e despesas até esta data.

## 4. Área geográfica de aplicação

São elegíveis para efeitos do presente Aviso Convite as operações no território nacional, incluindo Regiões Autónomas da Madeira e dos Açores, que preencham as condições de acesso.

## 5. Regras e limites à elegibilidade de despesas

**5.1.** Despesas elegíveis

São consideradas elegíveis as despesas que vierem a ser aprovadas no âmbito do presente procedimento, resultantes dos custos reais incorridos no desenvolvimento e adoção das soluções a apoiar, nomeadamente:

a) Aquisição de serviços a terceiros, incluindo assistência técnica e consultoria, quando demonstrada inequivocamente a sua necessidade para a operação;
b) Aquisição de serviços em *cloud* para disponibilização da solução de IA a adotar;
c) Aquisição de serviços de reforço de capacidade de infraestrutura, desde que seja para garantir o desempenho, escalabilidade e eficiência dos serviços a financiar, que não poderão representar mais de 20% do total das despesas elegíveis da operação;
d) Despesas com a proteção da propriedade intelectual e industrial dos resultados da operação;
e) Despesas com a promoção e divulgação da operação, que não poderão representar mais de 15% das demais despesas elegíveis da operação;
f) Despesas com pessoal técnico do beneficiário dedicado às atividades da operação, que não poderão representar mais de 20% das demais despesas elegíveis da operação.

**5.2.** Despesas não elegíveis

a) Despesas realizadas pelos beneficiários finais no âmbito de operações de locação financeira, de arrendamento ou de aluguer de longo prazo;
b) Despesas anteriores a 1 de fevereiro de 2020;

c) Custos normais de funcionamento do beneficiário, não previstos no investimento contratualizado, bem como custos de manutenção e substituição e custos relacionados com atividades de tipo periódico ou contínuo;
d) Pagamentos em numerário, exceto nas situações em que se revele ser este o meio de pagamento mais frequente, em função da natureza das despesas, e desde que num quantitativo unitário inferior a 250 euros;
e) Despesas pagas no âmbito de contratos efetuados através de intermediários ou consultores, em que o montante a pagar é expresso em percentagem do montante financiado pelo PRR ou das despesas elegíveis da operação;
f) Aquisição de bens em estado de uso;
g) Imposto sobre o Valor Acrescentado (IVA), recuperável ou não pelo beneficiário;
h) Aquisição de veículos automóveis, aeronaves e outro material de transporte;
i) Juros e encargos financeiros;
j) Fundo de maneio;
k) Despesas de apoio à candidatura do presente Aviso.

## 6. Taxa de financiamento e limite do apoio

A taxa máxima de financiamento aplicável a cada operação a apoiar no âmbito do presente Aviso Convite é de 100%. O limite de apoio a conceder por operação é o que se encontra definido no Anexo I. Cada organismo apenas pode apresentar uma candidatura, nos termos listados no Anexo I, contudo uma candidatura pode incluir uma ou mais soluções de IA a apoiar.

## 7. Dotação do fundo a conceder

A dotação afeta ao presente concurso para as candidaturas é de 1.660.397,50 €.

Prevê-se a possibilidade de reforço da dotação orçamental prevista para o presente Aviso-Convite, caso se revele necessário e mediante decisão da AMA, em articulação com a Estrutura de Missão Recuperar Portugal.

## 8. Condições de atribuição de apoio financeiro

Os apoios a conceder no âmbito destas medidas terão a taxa de financiamento de 100% e revestem a forma de apoio não reembolsável. O pagamento do financiamento atribuído será processado através das seguintes modalidades:

a) Pagamento de adiantamento (PA) correspondente a 10% do apoio aprovado e processado mediante solicitação do beneficiário, após assinatura do Termo de Aceitação das condições de financiamento e comunicação de início do projeto;

b) Em situações de natureza excecional justificadas pelo cumprimento das condições de fornecimento dos bens e serviços contratados ou de outras condições específicas de execução dos Investimentos, o limite máximo referido na alínea anterior pode ir até 20% do apoio, mediante proposta devidamente fundamentada apresentada pelo beneficiário à AMA;

c) Pagamentos a título de reembolso (PTR) mediante a apresentação de documentos comprovativos da realização do investimento e de relatórios de progresso;

d) Caso tenham sido efetuados os adiantamentos previstos nas alíneas a) e b), será aplicada, em cada pedido de pagamento, uma retenção proporcional ao adiantamento processado, até à recuperação da totalidade do adiantamento;

e) A soma de todos os pagamentos a título de adiantamento ou a título de reembolso não poderá ultrapassar 90% do apoio total aprovado ou apurado em função do grau de execução da operação;

f) Pagamento de Saldo Final (PSF), que corresponde à diferença entre o apoio elegível final apurado e o somatório dos pagamentos efetuados, é processado após verificação e avaliação final, física, técnica ou científica, financeira e contabilística, da execução da operação e comprovação do cumprimento das condicionantes e obrigações do beneficiário.

## 9. Modo de apresentação das candidaturas

A apresentação de candidaturas é efetuada através de formulário eletrónico, a disponibilizar a partir de 25 de julho de 2025, através do seguinte link de acesso: Formulário

## 10. Critérios de seleção de Candidaturas

São selecionadas as candidaturas apresentadas por beneficiários finais, identificados neste convite e que preencham as condições de acesso e de elegibilidade.

## 11. Identificação das entidades que intervêm no processo de decisão do financiamento.

A avaliação e o acompanhamento dos projetos são assegurados pela AMA, sem prejuízo das competências de outras entidades na gestão e governação do PRR.

## 12. Prazo para apresentação de candidaturas

O prazo para a apresentação de candidaturas decorre entre o dia 25 de julho e 31 de julho de 2025 (17:00 horas).

## 13. Procedimentos de análise e decisão de candidatura

As candidaturas são selecionadas de acordo com as condições de acesso, de elegibilidade e de seleção previstas no presente Aviso.

A decisão fundamentada sobre o apoio financeiro a atribuir é proferida pela AMA no prazo de 30 (trinta) dias úteis a contar da data final para apresentação da candidatura.

O prazo referido suspende-se quando sejam solicitados ao candidato quaisquer esclarecimentos, informações ou documentos, o que só pode ocorrer por uma vez. A não apresentação pelo candidato, no prazo de 10 (dez) dias úteis, dos esclarecimentos, informações ou documentos solicitados, determina a análise da candidatura apenas com os elementos disponíveis.

O candidato é ouvido no âmbito do procedimento de audiência prévia, nos termos legais, sendo concedido um prazo máximo de 10 (dez) dias úteis, contados a partir da data da notificação da proposta de decisão, designadamente quanto à eventual intenção de indeferimento e aos respetivos fundamentos.

A decisão final deve ser proferida no prazo máximo de 5 (cinco) dias após o termo do prazo de audiência prévia dos interessados.

## 14. Contratualização

A contratualização da decisão da concessão do apoio é feita mediante assinatura do **Termo de Aceitação** das condições de financiamento por parte do beneficiário final.

A decisão de aprovação caduca caso não seja assinado o Termo de Aceitação no prazo máximo de 30 (trinta) dias úteis, a contar da data da notificação da decisão, salvo motivo justificado e não imputável ao candidato.

O incumprimento das condições gerais e especificas de acesso listadas no ponto 3. poderá determinar a revogação do contrato.

## 15. Tratamento de Dados Pessoais

Todos os dados pessoais são processados de acordo com o Regulamento Geral de Proteção de Dados (RGPD) de 25 de maio de 2018 e a Lei de Proteção de Dados Pessoais (LPDP) – Lei n.º 58/2019, de 8 de agosto, na sua atual redação.

## 16. Divulgação de resultados e pontos de contato

No portal da AMA e no portal PRR os candidatos têm acesso a:

a) Outras peças e informações relevantes, nomeadamente legislação enquadradora;
b) Pontos de contato para obter informações adicionais;
c) Resultados deste concurso.

Os pedidos de informação e de esclarecimentos devem ser apresentados por escrito e remetido para o seguinte endereço de correio eletrónico: ama.prr@ama.pt

O Conselho Diretivo

## ANEXO I – PROJETOS E ENTIDADES CONVIDADAS

| NIF | BENEFICIÁRIO | PROJETO | SOLUÇÃO DE IA PRODUTO | APOIO |
|---|---|---|---|---|
| 600012662 | Marinha Portuguesa | Marinheiro de Silício | Assistente de IA para documentação sensível | 740.000,00 € |
| 600010180 | Estado-Maior-General das Forças Armadas | AI Ethical Hacking – Solução de IA para Ethical Hacking | AI Ethical Hacking – Solução de IA para Ethical Hacking | 482.397,50 € |
| | | Digital Sentinel | Digital Sentinel | 438.000,00 € |

## ANEXO II – PROCESSO DE SELEÇÃO DE CASOS DE USO


A seleção dos casos de uso seguiu a seguinte metodologia:

- Foi efetuado um levantamento inicial das iniciativas de IA na Administração Pública, realizado pelos vários gabinetes governamentais, no âmbito da CID - Conselho Interministerial para a Digitalização, que deu origem ao registo de 338 iniciativas de IA;
- No âmbito do CDAP foi solicitado a todos os Representantes Ministeriais e Tecnológicos, nas reuniões de Comité Estratégico e Operacional, respetivamente, e aos membros do Grupo Técnico de Trabalho de IA que validassem a informação inicial e que identificassem novas iniciativas, totalizando um levantamento de 365 iniciativas;
- Posteriormente foi efetuada uma análise preliminar para aferir o cumprimento dos seguintes requisitos mínimos, que implicou a redução da lista para 31 soluções de IA:
    - Estado de Maturidade da Solução
    - Potencial de Produtização
    - Código Aberto (Open Source)
    - Potencial de Escalabilidade
    - Impacto e Valor para a Administração Pública
    - Indicadores de Impacto
    - Capacidade Técnica da Entidade Responsável
    - Integração e Interoperabilidade
    - Segurança e Conformidade
    - Adoção de Princípios de IA Responsável
- Foi iniciado um ciclo de reuniões técnicas para validar o cumprimento dos requisitos junto das entidades executoras dos projetos. Serão selecionadas 6 a 12 soluções para

financiamento, sendo que o atual convite contempla 3 soluções, descritas nas fichas de projeto constantes no Anexo III.

## ANEXO III – FICHAS DE CARATERIZAÇÃO DE PROJETO E DE PRODUTO

### ANEXO III.1 – FICHA DE CARATERIZAÇÃO DE PROJETO 1

**Projeto 1 – Marinheiro de Silício**

**A. Caraterização do Beneficiário Final**

1. **NIF:** 600012662
2. **Designação:** Marinha Portuguesa
3. **Tipo de Entidade:** Forças Armadas

**B. Caraterização do Projeto**

1. **Designação** – Marinheiro de Silício

2. **Calendarização**
   1. **Data de Início** 22/07/2025
   2. **Data de fim** 30/06/2026

3. **Cronograma**

| | Atividade | Data de início | Data de Fim | Duração |
|---|---|---|---|---|
| **0.0** | **Gestão de Projeto** | | | |
| 0.1 | Gestão de Projeto | 22/07/2025 | 30/06/2025 | 344 |
| | | | | |
| **1.0** | **Requisitos e Especificações Técnicas** | | | |
| 1.1 | Recolha de dados | 22/07/2025 | 21/08/2025 | 30 |
| 1.2 | Levantamento de requisitos | 22/07/2025 | 21/08/2025 | 30 |
| 1.3 | Desenho de especificações técnicas | 21/08/2025 | 05/09/2025 | 15 |
| | | | | |
| **2.0** | **Implementação de Sistema** | | | |
| 2.1 | Plataforma de *back-end* | 05/09/2025 | 05/10/2025 | 30 |
| 2.2 | Treino de Codificadores-duais para pesquisa | 05/09/2025 | 05/10/2025 | 30 |
| 2.3 | Treino de LVLM generativo | 05/09/2025 | 05/10/2025 | 30 |
| 2.4 | Implementação de UI | 05/09/2025 | 05/10/2025 | 30 |
| | | | | |
| **3.0** | **Integração e testes** | | | |

| | | | | |
|---|---|---|---|---|
| 3.1 | Integração | 20/10/2025 | 19/11/2025 | 30 |
| 3.2 | Testes preliminares e recolha de dados de interação | 19/11/2025 | 04/12/2025 | 15 |
| | | | | |
| **4.0** | **Piloto e *hand-over* do sistema** | | | |
| 4.1 | Piloto e entrega de sistema | 18/01/2026 | 17/02/2026 | 30 |
| 4.2 | Instalação e configuração de hardware | 05/09/2025 | 05/10/2025 | 30 |
| 4.3 | Formação relativa à operação do sistema | 19/03/2026 | 18/04/2026 | 30 |
| 4.4 | Calibrações e melhoramentos | 17/02/2026 | 18/04/2026 | 60 |

### 4. Orçamento

| **Designação da despesa** | **Tipo de despesa** | **Valor (sem IVA)** |
|---|---|---|
| *Hardware* | Equipamento | 148.000,00 € |
| Atividade 1 - Requisitos e Especificações Técnicas | Serviços | 72.000,00 € |
| Atividade 2 - Implementação de Sistema | Serviços | 210.000,00 € |
| Atividade 3 - Integração e testes | Serviços | 160.000,00 € |
| Atividade 4 - Piloto e *hand-over* do sistema | Serviços | 140.000,00 € |
| Gestão de Projeto | Pessoal | 10.000,00 € |
| TOTAL | --- | 740.000,00 € |

## C. Caraterização do Produto

### 1. Identificação do Produto

- **Nome do Produto:** Assistente de IA para documentação sensível
- **Responsável pelo Produto:** Marinha Portuguesa

### 2. Descrição do Produto

O Assistente "Marinheiro de Silício" foi concebido para facilitar a interação rápida e intuitiva com documentação sensível usando linguagem natural. Este sistema inovador baseia-se num modelo de linguagem pré-treinado que aproveita as suas capacidades semânticas avançadas para compreender as solicitações dos utilizadores. As respostas são geradas com base na informação contida numa base de dados documental existente ou no *dataset* de treino. É importante notar que este último será um modelo de pequena dimensão, especificamente treinado com publicações de referência navais para garantir a precisão e relevância das informações fornecidas.

O Assistente "Marinheiro de Silício" tem como objetivo permitir a interação rápida através de linguagem natural com documentação sensível. O sistema baseia-se num modelo de linguagem pré-treinado que utiliza as suas capacidades semânticas para entender o pedido do utilizador e responder com base na documentação

existente na base de dados, ou com base na informação presente no *dataset* de treino. Este último deve considerar um modelo de pequena dimensão, treinado em publicações de referência navais.

## 3. Objetivos do Produto

O principal objetivo do Assistente "Marinheiro de Silício" é otimizar a gestão e acesso à informação sensível. Para isso, focamo-nos em:

- Reduzir significativamente o tempo de pesquisa em documentos sensíveis, tornando a recuperação de dados mais eficiente.
- Compilar e sintetizar informações documentais de forma precisa para responder a solicitações específicas dos utilizadores.
- Apoiar a tomada de decisão dos diferentes utilizadores, fornecendo acesso rápido e atualizado à informação relevante.
- Facilitar a redação de novos documentos ao providenciar referências e provas documentais de forma ágil e fiável.

## 4. Requisitos Técnicos

Esta ficha de requisitos foi elaborada para garantir que a solução de IA atenda às necessidades da administração pública, proporcionando eficiência, segurança e conformidade com as normas vigentes.

### a. Requisitos Funcionais

O Assistente de "Marinheiro de Silício" será composto por quatro componentes principais, cada uma com funções distintas e interligadas para garantir a sua operação robusta e eficiente:

- Interface do Utilizador: Esta componente será dividida em duas partes principais. A primeira, para o administrador, permitirá a gestão de utilizadores e configurações gerais do sistema. A segunda, para os utilizadores finais, será uma interface de chat web intuitiva, que incluirá um histórico de conversação para fácil consulta. A interação ocorrerá através de uma caixa de texto que suportará o anexo de ficheiros como contexto para as perguntas. As respostas do sistema serão apresentadas em *streaming* e formatadas utilizando Markdown para maior legibilidade.
- Componente de Geração Textual: Agindo como o "cérebro" do sistema, esta componente receberá as solicitações (*prompts*) dos utilizadores. Fará uma análise da intenção do utilizador e, se a pergunta puder ser respondida com base no seu conhecimento pré-treinado, gerará a resposta diretamente. Contudo, para perguntas que exijam dados específicos e contextuais, acionará a Componente de *Retrieval* para enriquecer e fundamentar a sua resposta. Em cenários puramente conversacionais e genéricos, a resposta será gerada unicamente com base no treino do modelo, sem recorrer à base de dados externa.

- Componente de *Retrieval*: Esta componente crucial será responsável por pesquisar e recuperar informações ou porções documentais da base de dados que apresentem a maior semelhança semântica com a consulta do utilizador. Atuará como a ponte entre a intenção do utilizador e a documentação sensível, garantindo que as respostas sejam precisas e contextualmente relevantes.
- Componente de Alimentação da Base de Dados: Esta componente assegurará que a base de dados esteja sempre atualizada. Será encarregue de indexar a informação dos documentos presentes na base de dados de objetos, conforme definido e gerido pelo administrador. Isso garante que o Assistente "Marinheiro de Silício" tenha sempre acesso aos dados mais recentes e relevantes para as suas operações.

### b. Requisitos Não Funcionais

Para garantir a robustez e adaptabilidade do Assistente "Marinheiro de Silício", estabelecemos os seguintes requisitos não funcionais:

- Implantação (*Deployment*): O sistema deve operar *on-premise*, ou seja, em infraestruturas controladas pelo cliente. O desenvolvimento inicial pode ser realizado externamente, utilizando-se para tal apenas documentação não classificada.
- Escalabilidade: A solução deve ser escalável, permitindo a sua adaptação e implementação em diferentes organizações que partilhem requisitos de segurança semelhantes. Para isso, todos os seus componentes devem ser heterogéneos, facilitando a instalação com apenas pequenas modificações nas configurações.
- Desempenho: O Assistente "Marinheiro de Silício" deve apresentar um desempenho rápido, sendo capaz de suportar entre 100 a 200 utilizadores em simultâneo sem comprometer a sua eficiência e tempo de resposta.

### c. Requisitos de Dados

- Os dados a serem utilizados pelo Assistente "Marinheiro de Silício" consistirão em documentação variada proveniente de diferentes órgãos da Marinha Portuguesa. A qualidade dos dados é variável, sendo a maioria dos documentos em formato PDF. No entanto, alguns documentos podem estar em formatos como OCR (Reconhecimento Ótico de Caracteres) e Microsoft Office, o que exigirá capacidades de processamento adequadas para lidar com essa diversidade.
- Em relação ao modelo de pequena dimensão, os dados de treino serão especificamente gerados a partir de publicações de referência nacionais e estrangeiras. Estas publicações focar-se-ão nas táticas, técnicas e procedimentos operacionais de unidades navais, garantindo que o modelo seja altamente especializado e relevante para o domínio marítimo.

### d. Requisitos de Implementação

A implementação do Assistente "Marinheiro de Silício" pode ser realizada utilizando diferentes arquiteturas, no entanto, alguns componentes de hardware são essenciais para o seu funcionamento otimizado:

- Hardware: Será indispensável a utilização de GPUs (*Graphics Processing Units*) para a inferência dos modelos de linguagem, garantindo respostas rápidas e eficientes. Para o cálculo de similaridade entre as porções documentais e as *queries* dos utilizadores, serão necessários CPUs (*Central Processing Units*) robustas. O armazenamento de dados e documentos será feito em SSDs (*Solid State Drives*) para assegurar alta velocidade de acesso e recuperação de informação.
- Avaliação do Sistema: A unidade utilizadora será responsável por criar um *dataset* dedicado que permitirá a avaliação rigorosa da performance do sistema. Este *dataset* será crucial para medir a eficácia e a precisão das respostas do Assistente "Marinheiro de Silício" em cenários reais.
- Treino do Modelo de Pequena Dimensão: O treino do modelo de linguagem de pequena dimensão terá como ponto de partida um modelo pré-treinado existente. Este modelo base será então refinado utilizando o *dataset* específico criado pela unidade utilizadora. A avaliação deste modelo refinado será feita com recurso a um subconjunto do mesmo *dataset*, garantindo uma validação coerente e representativa do seu desempenho no domínio naval.

### e. Requisitos de Manutenção

Para garantir o contínuo funcionamento e otimização do Assistente "Marinheiro de Silício", os requisitos de manutenção são os seguintes:

- Otimização de *Hardware*: O desenvolvedor do sistema será responsável por analisar o hardware existente e configurá-lo de modo a potenciar a sua performance tanto para as tarefas de RAG (*Retrieval-Augmented Generation*) quanto para a conversação pura. Isso assegura que o sistema opere com a máxima eficiência, aproveitando ao máximo os recursos disponíveis.
- Mecanismo de *Feedback* do Utilizador: A componente de interface deve incluir uma funcionalidade que permita aos utilizadores fornecer feedback sobre as suas interações. Este *feedback* é crucial, pois será utilizado para medir o desempenho real do sistema e para identificar e corrigir possíveis erros, contribuindo para a melhoria contínua da solução.

### f. Considerações Éticas e Legais

A implementação do Assistente "Marinheiro de Silício" considera os seguintes pontos críticos relativos à ética e legalidade:

- Transparência e Responsabilidade: Os processos e o fluxo de informação entre as diferentes componentes do sistema serão transparentes, baseando-se em algoritmos claros e compreensíveis. No entanto, é fundamental reconhecer que as respostas geradas pelo sistema dependem

significativamente do modelo de linguagem base e dos seus dados de treino, os quais podem não ser totalmente conhecidos. Esta dependência pode ocasionalmente resultar em respostas desalinhadas com preceitos éticos e legais estabelecidos. Para mitigar esse risco, o sistema incorporará *guard-rails* e mecanismos de segurança projetados para prevenir tais ocorrências.

- Privacidade e Proteção de Dados: A privacidade dos dados dos utilizadores será uma prioridade. A segurança e a confidencialidade das informações serão asseguradas pelo administrador local do sistema, que implementará medidas robustas de proteção, incluindo a encriptação de dados sensíveis, em conformidade com as normas e regulamentações aplicáveis à proteção de dados.

## ANEXO III.2 – FICHA DE CARATERIZAÇÃO DE PROJETO 2

**Projeto 2 – AI Ethical Hacking – Solução de IA para Ethical Hacking**

### A. Caraterização do Beneficiário Final

1. **NIF:** 600010180
2. **Designação:** Estado-Maior-General das Forças Armadas
3. **Tipo de Entidade:** Entidade Pública / Órgão do Estado

### B. Caraterização do Projeto

1. **Designação** – AI Ethical Hacking – Solução de IA para Ethical Hacking

2. **Calendarização**
   1. **Data de Início** 01/08/2025
   2. **Data de fim** 30/06/2026

3. **Cronograma**

| Atividade | Data de início | Data de Fim |
|---|---|---|
| Levantamento de tecnologias existentes através de reconhecimento | 01/08/2025 | 30/11/2025 |
| Desenvolvimento dos módulos avançados automáticos de "ethical hacking" | 01/10/2025 | 30/04/2026 |
| Teste e afinação dos módulos avançados | 01/01/2026 | 30/06/2026 |
| Integrações, Implementação e Validação Final | 01/05/2026 | 30/06/2026 |

### 4. Orçamento

| Designação da despesa | Tipo de despesa | Valor (sem IVA) |
|---|---|---|
| *Hackers* Éticos | Aquisição de serviços a terceiros | 44.860,00 € |
| Plataformas de *compliance* RGPD, SOC2, EDR | Serviços em *cloud* | 18.500,00 € |
| *Advisory data security* | Aquisição de serviços a terceiros | 7.500,00 € |
| Advisory gestão do projeto - Financeira legal | Aquisição de serviços a terceiros | 56.000,00 € |
| Sistemas de AI Generativo | Serviços em *cloud* | 40.200,00 € |
| *Programming project management tools* | Serviços em *cloud* | 1.800,00 € |
| Desenvolvimento de Menus UI e análise de UX | Aquisição de serviços a terceiros | 75.000,00 € |
| AI e *product design Advisory* | Aquisição de serviços a terceiros | 48.000,00 € |
| Registo marca *umbrella* módulos – *HackIon* | Despesas proteção de propriedade intelectual | 5.000,00 € |
| Divulgação de operação | Divulgação de operação | 29.686,00 € |
| Melhoramento da Infraestrutura | Infraestrutura | 59.372,00 € |
| Alocação tempo interno | Despesas com pessoal técnico | 96.479,50 € |
| TOTAL | --- | 482.397,50 € |

## C. Caraterização do Produto

### 1. Identificação do Produto

- **Nome do Produto:** AI Ethical Hacking – Solução de IA para Ethical Hacking
- **Responsável pelo Produto:** Estado-Maior-General das Forças Armadas

### 2. Descrição do Produto

A Solução de IA para *Ethical Hacking* Autónomo visa automatizar e otimizar processos de cibersegurança administrativos, protegendo infraestruturas digitais críticas nacionais. A proposta melhora a segurança dos sistemas, aumenta a eficiência e rapidez na identificação de riscos, e reduz erros humanos. A solução será implementada em várias áreas governativas, com foco inicial na entidade Estado-Maior-General das Forças Armadas (EMGFA), bem como em infraestruturas digitais críticas ligadas à Presidência do Conselho de Ministros (PCM) e aos diversos Ministérios.

O projeto propõe o desenvolvimento de novos módulos altamente especializados, facilmente integráveis com a solução base existente. Esta base – o Portal da *Ethiack* – está no mercado desde 2022 e é utilizada por mais de 80 clientes em 9 países, cobrindo diversos setores como governos, câmaras municipais, universidades, companhias aéreas, telecomunicações, retalho, finanças, cuidados de saúde e tecnologia.

A proposta centra-se no desenvolvimento de integrações e módulos automáticos de *ethical hacking*, impulsionados por IA, que permitem testar as infraestruturas críticas das Forças Armadas e da AP. Estes módulos permitirão a realização de testes proativos com elevada frequência, profundidade e eficácia, cobrindo todas as fases do processo: reconhecimento, desenvolvimento, teste, integração e validação final. O teste contínuo e automatizado de cibersegurança previne a exploração de vulnerabilidades e minimiza (ou evita) as consequências do cibercrime. A visão do projeto é proporcionar à AP uma solução capaz de identificar, gerir e priorizar vulnerabilidades específicas, otimizando o uso de recursos para a sua mitigação rápida e eficaz. Tal abordagem contribui diretamente para o aumento dos padrões de cibersegurança, para o cumprimento da regulamentação aplicável e para a racionalização de recursos.

Este projeto está alinhado com o Decreto-Lei nº 49/2024, que reforça a cibersegurança, a interoperabilidade, o uso de IA ética, o acesso digital e a experiência do utilizador nos serviços públicos, bem como com EDN, que promove serviços mais seguros, rápidos e centrados no cidadão, com foco em dados, tecnologia de confiança e eficiência.

## 3. Objetivos do Produto

- Automatizar os testes de segurança em sistemas digitais com frequência de teste diária para análise de vulnerabilidades a ativos digitais;
- Desenvolvimento de Módulos avançados e especializados de testes de segurança para as Forças Armadas e Administração Pública para detetar vulnerabilidades e riscos de alta severidade,
- Reduzir o tempo de identificação de vulnerabilidades e suportar a sua mitigação;
- Poupança em serviços de cibersegurança e recursos humanos dedicados.

## 4. Requisitos Técnicos

Esta ficha de requisitos foi elaborada para garantir que a solução de IA atenda às necessidades da Administração Pública, proporcionando eficiência, segurança e conformidade com as normas vigentes.

### a. Requisitos Funcionais

A solução propõe um conjunto de funcionalidades orientadas à automação, precisão e escalabilidade da análise de vulnerabilidades nas infraestruturas críticas do Estado. Destacam-se:

- Automação de Processos: Execução autónoma e recorrente de tarefas de reconhecimento, varrimento, teste de segurança e priorização de riscos, sem intervenção humana contínua. A solução permite orquestrar fluxos de trabalho de testes de segurança de acordo com políticas predefinidas por ativos, segmentos de rede ou criticidade.
- Análise de Dados: Consolidação de resultados em *dashboards* interativos e relatórios de ciber-risco com métricas-chave (tempo médio para mitigação, severidade média, evolução por ativo ou unidade).

Os dados permitem visibilidade estratégica em tempo real e alimentam mecanismos de triagem automática baseados em IA com taxa de falsos positivos inferior a 1%.

- Integração com Sistemas Existentes: Interoperabilidade garantida via API, ou webhooks e integração com plataformas de gestão de risco. A solução permite integrar alertas, relatórios e fluxos de decisão nos sistemas já utilizados pela Administração Pública.
- Interface de Utilizador: Portal unificado com usabilidade adaptada a diferentes perfis – técnicos operacionais, gestores de risco, e decisores. Permite configurar testes, visualizar superfícies de ataque 3D, exportar relatórios, e priorizar vulnerabilidades com base em contexto operacional.
- Outros Requisitos Funcionais: Suporte a ambientes *cloud*, híbridos e redes segregada.

### b. Requisitos Não Funcionais

A proposta contempla um conjunto de requisitos não funcionais que asseguram a robustez, segurança e escalabilidade da solução no contexto da Administração Pública:

- Segurança:

  A solução cumpre com os requisitos de cibersegurança, proteção de dados pessoais e demais normas legais aplicáveis. A Ethiack possui certificação ISO/IEC 27001 para gestão de segurança da informação, assegura conformidade com o Regulamento Geral de Proteção de Dados (GDPR) e é detentora da Marca Nacional com Grau Secreto, atribuída pelo Gabinete Nacional de Segurança (GNS). Além disso, conta com auditores certificados pelas principais entidades internacionais: OSCP, OSWE, OSCE, CEH, CREST e CHECK, garantindo elevados padrões técnicos na operação e desenvolvimento da solução.
- Escalabilidade:

  A execução dos testes é suportada por uma infraestrutura dedicada baseada em *Kubernetes* e containers, garantindo isolamento, paralelismo e escalabilidade horizontal. Os módulos de teste são orquestrados por um sistema interno composto por uma API e um *Scheduler*, que automatiza operações regulares e programadas. Esta arquitetura permite executar múltiplos testes em paralelo, escalar a operação de forma eficiente por número de ativos ou entidades, e adaptar-se a redes distintas da Administração Pública (incluindo ambientes segregados). Toda a infraestrutura comunica com o portal central, garantindo sincronização e entrega dos resultados em tempo real com visibilidade por entidade, ativo ou criticidade.
- Desempenho:

  A solução é desenhada para ter um "*uptime*" superior a 99%. Os testes de segurança são otimizados para balancear profundidade, cobertura e tempo de execução, permitindo execuções frequentes sem impacto nos sistemas auditados.
- Conformidade:

  A solução cumpre o Regulamento Europeu de IA (AIA) e o RGPD, aplicando princípios de AI *explainability*, e mecanismos de anonimização. Está alinhada com os princípios da Estratégia Nacional de IA e da EDN. Todos os dados pessoais ou sensíveis são tratados de acordo com políticas definidas

e auditáveis. O produto e os módulos seguem as diretrizes do DL nº 49/2024 para serviços públicos digitais seguros, transparentes e confiáveis.

### c. Requisitos de Dados

A solução depende da recolha, processamento e gestão segura de grandes volumes de dados técnicos e contextuais associados aos ativos digitais das entidades da Administração Pública. Os requisitos de dados estão estruturados da seguinte forma:

- Fontes de Dados:

  A plataforma utiliza dados históricos e em tempo real provenientes de:

  - Inventários de ativos digitais (internos e externos);
  - Relatórios de vulnerabilidades (internos e públicos, ex. CVE/NVD);
  - Registos de comunicação e tickets técnicos (*helpdesk*, auditorias anteriores).

- Qualidade dos Dados:

  A solução integra mecanismos automáticos de verificação, enriquecimento e normalização dos dados, com foco na integridade, completude e atualidade das fontes. As vulnerabilidades e ativos são validados através de múltiplas fontes e triangulados para reduzir redundância, ruído ou obsolescência.

- Governança de Dados:

  Toda a gestão de dados é realizada de acordo com políticas internas da Ethiack e com as melhores práticas do setor. Estão definidos procedimentos de:

  - Minimização de dados;
  - Anonimização e pseudonimização (quando aplicável);
  - Retenção e eliminação segura;
  - Registo de acessos e alterações;
  - Auditoria periódica de conformidade com o RGPD e ISO 27001.

### d. Requisitos de Implementação

A implementação da solução será feita de forma faseada, garantindo segurança, fiabilidade e facilidade de integração com os sistemas existentes.

- Ambiente de Desenvolvimento:

  A solução será desenvolvida num ambiente seguro, com separação clara entre desenvolvimento, testes e produção. Utiliza tecnologia baseada em contentores (ex.: *Docker*) para garantir portabilidade e rapidez de instalação. Toda a infraestrutura está preparada para funcionar em ambientes da Administração Pública, incluindo redes isoladas.

- Testes e Validação:

Antes da entrada em produção, a solução será sujeita a testes funcionais, de segurança e desempenho. Estes testes serão realizados em conjunto com as equipas técnicas da entidade utilizadora. Só após validação conjunta é que os módulos serão disponibilizados em ambiente real.

- Modelo de IA:

  A solução cumprirá princípios de IA ética e confiável com a adoção de soluções de anonimização de dados e monitorização contínua do desempenho e impactos por revisão manual de resultados. A Ethiack implementa mecanismos de "*explainability*" e "*accountability*" nos processos de decisão automática. Além disso, o sistema é auditável, não toma ações destrutivas sem consentimento explícito, e está em conformidade com as diretrizes de IA ética europeia e nacional. Os componentes de IA são ajustados com base em dados públicos e anonimizados, garantindo total conformidade com a legislação aplicável. O sistema aprende com vulnerabilidades reais (por exemplo, CVEs) para melhorar a sua eficácia ao longo do tempo. O desempenho dos modelos é monitorizado e revisto regularmente por especialistas.

A integração com o EMGFA e AP será acompanhada por sessões técnicas de instalação e validação, com apoio direto da equipa Ethiack e mecanismos de apoio contínuo.

### e. Requisitos de Manutenção

A manutenção da solução é essencial para garantir o seu funcionamento contínuo, seguro e eficaz ao longo do tempo.

- Suporte Técnico:

  A Ethiack assegura suporte técnico especializado, disponível para resolução de problemas, aplicação de atualizações e acompanhamento contínuo. O suporte inclui resposta a incidentes, atualização de módulos de teste, correção de erros e apoio na operação da plataforma.

- Monitorização e Avaliação:

  A solução inclui ferramentas de monitorização permanente que verificam o estado do sistema, o desempenho dos testes e a disponibilidade dos serviços. Os resultados são apresentados em *dashboards* acessíveis aos responsáveis técnicos da entidade. São realizadas avaliações periódicas para garantir que os objetivos de segurança, cobertura e conformidade estão a ser cumpridos.

A manutenção pode ser prestada através de contrato de subscrição com SLAs adaptados às necessidades da Administração Pública e das Forças Armadas.

### f. Considerações Éticas e Legais

A solução segue os princípios da IA ética, responsável e auditável, garantindo o cumprimento das normas legais e regulamentares aplicáveis à Administração Pública.

- Transparência:

Todos os processos automatizados são documentados e auditáveis. A plataforma permite acompanhar o histórico de decisões, testes realizados e recomendações emitidas. Os relatórios são claros, justificáveis e compreensíveis por técnicos e decisores.

- Privacidade:
  Os dados são tratados com total respeito pela privacidade dos utilizadores e entidades envolvidas. Sempre que possível, os dados são anonimizados e sujeitos a políticas de retenção e minimização. A solução cumpre integralmente o Regulamento Geral de Proteção de Dados (RGPD) e a ISO 27001.
- Responsabilidade:
  Existem mecanismos de controlo humano em todas as fases críticas, desde a criação de módulos até à execução de testes. A Ethiack assume total responsabilidade pela segurança, correção e adequação dos módulos utilizados.

## ANEXO III.3 – FICHA DE CARATERIZAÇÃO DE PROJETO 3

**Projeto 3 – Digital Sentinel**

### A. Caraterização do Beneficiário Final

1. **NIF:** 600010180
2. **Designação:** Estado-Maior-General das Forças Armadas
3. **Tipo de Entidade:** Entidade Pública / Órgão do Estado

### B. Caraterização do Projeto

1. **Designação** – Digital Sentinel

2. **Calendarização**
   1. **Data de Início** 01/07/2025
   2. **Data de fim** 30/06/2026

3. **Cronograma**

| Atividade | Data de início | Data de Fim |
|---|---|---|
| Planeamento da arquitetura da solução | 01/07/2025 | 30/08/2025 |
| Desenvolvimento da estrutura base dos agentes AI | 15/08/2025 | 30/10/2025 |
| Identificação dos workflows de análise dos agentes AI | 01/09/2025 | 30/09/2025 |

| | | |
|---|---|---|
| Implementação do serviço de MCP | 01/11/2025 | 30/11/2025 |
| Desenvolvimento dos workflows nos agentes de AI | 01/11/2025 | 30/06/2026 |

### 4. Orçamento

| **Designação da despesa** | **Tipo de despesa** | **Valor (sem IVA)** |
|---|---|---|
| Contratação de serviços de desenvolvimento de software | Aquisição de bens e serviços | 368.000,00 € |
| Subscrição de provedores de *feeds* de dados | Aquisição de bens e serviços | 35.000,00 € |
| Modelos de IA na *cloud* | Aquisição de bens e serviços | 15.000,00 € |
| Aquisição de capacidade de infraestrutura computacional | Aquisição de ativos de capital | 8.000,00 € |
| Organização de eventos para disseminação e formação | Aquisição de bens e serviços | 2.000,00 € |
| Remunerações e encargos com funcionários públicos | Despesas com o pessoal | 10.000,00 € |
| TOTAL | --- | 438.000,00 € |

## D. Caraterização do Produto

### 5. Identificação do Produto

- **Nome do Produto:** Digital Sentinel
- **Responsável pelo Produto:** Estado-Maior-General das Forças Armadas

### 6. Descrição do Produto

O projeto "Digital Sentinel" representa uma solução inovadora de gestão de superfície de ativos externos (EASM - *External Asset Surface Management*), desenvolvida como um módulo *open-source* baseado no padrão de dados de cibersegurança STIX (Structured Threat Information Expression). Integrado na iniciativa nacional Caravel, uma plataforma de inteligência ciber com base em STIX 2.1, este módulo surge como uma extensão natural dos desenvolvimentos anteriores, agregando informação sobre ciber ameaças com dados de ativos para identificar riscos, considerando o panorama de ameaças específico de cada organização. O foco principal reside no avanço tecnológico, impulsionando a resiliência nacional, em particular das organizações da administração pública, através da aplicação de IA em processos de descoberta e análise de ativos que constituem a superfície de ataque no ciberespaço.

No centro da inovação técnica, o "Digital Sentinel" incorpora agentes de IA que tomam decisões autónomas durante a recolha e análise de dados, selecionando as ferramentas de cibersegurança adequadas para cada cenário e permitindo uma descoberta dinâmica de ativos com "*pivoting*" inteligente baseado em cada descoberta. Esta abordagem assegura um processo adaptativo e eficiente, otimizando a exploração de

superfícies de ataque das organizações no ciberespaço. Adicionalmente, o módulo utiliza o protocolo MCP (*Model Context Protocol*) para facilitar o acesso seguro e integrado às ferramentas de descoberta de ativos, promovendo uma interoperabilidade avançada entre componentes. Complementando estas funcionalidades, a integração de GraphRAG permite a criação dinâmica de relações entre os ativos identificados, gerando grafos de conhecimento que revelam interconexões de forma automática e escalável.

Estes avanços tecnológicos não só elevam a capacidade de processar grandes volumes de dados com consistência superior à intervenção humana, mas também projetam decisões mais sustentadas e políticas públicas otimizadas. Ao alinhar-se com investimentos em soluções de IA para a administração pública, o projeto visa melhorar a eficiência interna, reduzir custos operacionais e elevar a qualidade dos serviços prestados a cidadãos e empresas, contribuindo para a resiliência do ciberespaço nacional. Com um potencial impacto transformador, o "Digital Sentinel" contribui para a criação de emprego qualificado e para uma administração pública mais ágil e produtiva, posicionando Portugal como líder em soluções de inteligência ciber baseadas em padrões abertos.

## 7. Objetivos do Produto

- Melhorar a eficiência operacional para identificar ativos externos e os riscos associados nas organizações da administração pública.
- Reforçar a ciber resiliência nacional, alinhando com diretivas como a NIS2.
- Melhorar a visibilidade das organizações sobre a sua superfície de ataque no ciberespaço.

## 8. Requisitos Técnicos

Esta ficha de requisitos foi elaborada para garantir que a solução de IA atenda às necessidades da Administração Pública, proporcionando eficiência, segurança e conformidade com as normas vigentes.

### a. Requisitos Funcionais

Processamento de Linguagem Natural (NLP):

- Capacidade de processar *prompts* do utilizador, permitindo que o agente de IA interprete pedidos de análise de ativos digitais.
- Capacidade para que o agente de IA pode solicitar informações adicionais (ex.: domínios da organização) para refinar a análise.

Automação de Processos:

- Implementação de *workflows* para a identificação de ativos externos, utilizando ferramentas open-*source* via protocolo MCP, incluindo a obtenção de *domains*, gamas de IP, etc.

- Automatização do *pivoting* inteligente, onde o agente de IA toma decisões autónomas para selecionar e aplicar ferramentas adequadas com base nos resultados ao longo da análise, maximizando a cobertura de informações sobre ativos.
- Geração automática de relatórios finais e exportação de dados no formato padrão STIX 2.1, agregando os ativos identificados com informações para cálculo de risco organizacional.

Análise de Dados:

- Ferramentas para análise dinâmica de dados recolhidos, incluindo a criação de relações entre ativos através da abordagem GraphRAG, gerando grafos de conhecimento para identificar interconexões e padrões.
- Capacidade de processar grandes volumes de dados, identificando padrões.
- Visualização básica de resultados, grafos relacionais e gráficos, integrados no relatório final para facilitar a compreensão dos dados analisados.

Integração com Sistemas Existentes:

- Disponibilização de uma REST API para integração externa, permitindo que outros sistemas invoquem análises de ativos e recebam resultados em formato STIX.
- Disponibilização de um MCP server para integração com aplicações de AI como ChatGPT, Claude Desktop, LibreChat, etc.

Interface de Utilizador:

- Não será desenvolvida uma interface dedicada, uma vez que isso representaria uma duplicação de soluções existentes, como o LibreChat ou Claude Desktop. Em alternativa, o foco incide na disponibilização de um serviço via protocolo MCP, permitindo que as organizações da administração pública continuem a utilizar as suas ferramentas de "AI Desktop", tais como o LibreChat, uma aplicação *open-source* para interações com IA, customizável e compatível com múltiplos LLMs. Para utilizar, basta adicionar o link do MCP do Digital Sentinel para integrar automaticamente as capacidades. Esta abordagem alinha-se com os avanços em IA na interação com o utilizador.
- Para fins de demonstração, o LibreChat será utilizado para apresentar as funcionalidades do Digital Sentinel.

Outros Requisitos Funcionais:

- Garantia de conformidade com padrões abertos, como STIX 2.1, para padronização dos outputs e facilitação de partilha de dados entre organizações.

- Funcionalidades de escalabilidade, permitindo o processamento de análises para múltiplas organizações simultaneamente, com foco na eficiência e redução de custos operacionais na administração pública.

### b. Requisitos Não Funcionais

Segurança:

- Controlo de acessos para apenas utilizadores autenticados da administração pública possam iniciar análises ou aceder a resultados, com registo de auditoria para rastrear interações.
- Utilização de protocolos seguros no MCP para integração de ferramentas, evitando exposição de dados durante o *pivoting* inteligente e a recolha de ativos, e incorporação de mecanismos de deteção de anomalias para prevenir injeções ou abusos no processamento de linguagem natural.
- Mecanismos de *enforcing* para manter os agentes de IA com foco restrito na descoberta de ativos digitais, bloqueando-os de qualquer outro tipo de tarefa.

Escalabilidade:

- Arquitetura suporta o processamento simultâneo de análises para múltiplas organizações.
- Integração de GraphRAG otimizada para lidar com grandes grafos de conhecimento.
- Implementado com a utilização de containers para rápido *deployment* e escalabilidade.

Desempenho:

- Selecção de *libraries*, *frameworks* e base de dados modernas e com alta performance.
- Implementação para execução de múltiplas tarefas concorrentes.

Conformidade

- Adesão ao Regulamento de Inteligência Artificial da UE, através de avaliações de risco transparentes nos agentes de IA e documentação detalhada dos processos de decisão autónoma durante a análise de ativos.
- Cumprimento do Regulamento Geral de Proteção de Dados (GDPR), com minimização de dados pessoais recolhidos (ex.: limitando endereços de email a contextos estritamente necessários e que haja um risco de cibersegurança associado), consentimento explícito para análises e opções de anonimização nos relatórios STIX para partilha entre organizações.
- Integração de padrões abertos como STIX 2.1 para facilitar a interoperabilidade entre sistemas.

### c. Requisitos de Dados

Fontes de Dados:

- Utilização de dados iniciais fornecidos pelo utilizador, como domínios ou gamas de IP.
- Recolha dinâmica de dados de fontes abertas e comerciais acessíveis via APIs, permitindo a extração controlada de informações para *pivoting* inteligente, com minimização ao essencial e conformidade ao GDPR.

Qualidade dos Dados:

- Mecanismos de validação automática durante a recolha, incluindo cruzamento de múltiplas fontes para detetar duplicados ou possíveis erros, assegurando maior precisão.
- Avaliações de qualidade integradas nos *workflows*, forçando os agentes de AI a verificarem as informações recolhidas.

Governança de Dados:

- Políticas para gestão de dados, incluindo controlo de acessos, protegendo informações sensíveis em linha com o GDPR e minimizando recolha de dados pessoais.
- Procedimentos para remoção de qualquer histórico ao final de um tempo determinado.

### d. Requisitos de Implementação

Ambiente de Desenvolvimento:

- Utilização de Docker e Docker Compose para containerização e orquestração de serviços, facilitando ambientes isolados e replicáveis.
- Desenvolvimento em Python com FastAPI para a criação de APIs REST e MCP, assegurando performance e escalabilidade.
- Integração do *framework* Pydantic AI para construção de agentes de IA, suportando decisões autónomas e *pivoting* inteligente.

Testes e Validação:

- Aplicação de Pydantic AI Eval para avaliação de agentes de IA, verificando decisões e outputs em cenários simulados.
- Implementação de testes unitários com Pydantic para validar componentes individuais, como *parsing* de dados e *workflows* automatizados.
- Utilização de Pydantic Logfire para monitorização do comportamento dos agentes de IA e *logging* de erros durante testes, facilitando depuração em tempo real.
- Emprego de bibliotecas de validação STIX para confirmar a conformidade dos relatórios gerados com o padrão STIX 2.1.

Treino do Modelo:

- Não serão realizados treinos ou *fine-tuning* nos modelos usados, uma vez que o foco do desenvolvimento reside nos agentes de IA e não na camada de LLM, que será configurável para adaptar-se à evolução de modelos ao longo do tempo, promovendo flexibilidade e redução de custos.

### e. Requisitos de Manutenção

Suporte Técnico:

- Disponibilidade de suporte técnico dedicado durante pelo menos 1 ano após implementação, incluindo resolução de problemas operacionais e realização de atualizações de segurança para manter a integridade da solução.
- Procedimentos para atualizações, com foco em correções de bugs nos agentes de IA, garantindo compatibilidade com evoluções em protocolos como MCP e padrões STIX 2.1.

Monitorização e Avaliação:

- Integração de ferramentas de *logging* detalhado para registar ações dos agentes de IA, facilitando a análise de *workflows* e deteção de anomalias.
- Implementação de métricas para monitorização do desempenho computacional

### f. Considerações Éticas e Legais

Transparência:

- Integração de logs auditáveis e visualizações, permitindo rastreabilidade das análises e conformidade com o Regulamento AIA da UE através de avaliações de risco transparentes.

Privacidade:

- Minimização da recolha de dados pessoais, limitando informações como endereços de email a contextos essenciais, com anonimização automática nos outputs STIX e consentimento explícito para análises, em cumprimento do GDPR.
- Implementação de encriptação e controlos de acesso via MCP, protegendo dados sensíveis durante integrações e garantindo que a solução não armazene dados além do necessário para a descoberta de ativos externos.