



Universidade do Minho

Departamento de Informática

Mestrado em Engenharia Informática

Mineração de Dados

1º Ano, 2º Semestre

Ano letivo 2025/2026

Ficha de Exercícios PL2

Data Sources & Data Collection (OSINT)

Duração: 2 horas

Modalidade: Individual ou a pares

Docente: Diana Ferreira

Contexto: Desenvolver habilidades práticas em técnicas de OSINT de forma exclusivamente passiva sobre a empresa GALP Energia S.A. Cada exercício simula cenários de investigação empresarial, *compliance* e análise de segurança, utilizando ferramentas específicas para recolher e analisar informações de fontes abertas.

⚠️ Regras obrigatórias

- Apenas informação pública
- Sem login em contas pessoais
- Sem scans ativos
- Sem inferências sobre indivíduos

Parte 1 - Reconhecimento de Infraestrutura GALP

Análise da presença digital da GALP para auditoria de segurança.

Questão 1.1. Utilizando **WHOIS**, analise o domínio galp.com e galp.pt e determine:

- Data de registo do domínio
- Informações de registante (se disponíveis)
- *Nameservers* e histórico

Interpretação: O domínio é antigo? O que é que isso significa? A empresa garante resiliência? Como?

Questão 1.2. Com recurso a **Amass** ou **theHarvester**, execute enumeração de:

- Subdomínios (ex: *.galp.pt, *.galp.com)
- Endereços de email corporativos



Universidade do Minho

Departamento de Informática

Mestrado em Engenharia Informática

Nota: Para a resolução desta questão, deve ser previamente verificada a instalação das ferramentas mencionadas. A enumeração passiva pode ser realizada com recurso aos seguintes comandos:

```
amass enum -passive -d example.com
amass enum -passive -d example.com -src -> limitar fontes
timeout 300 amass enum -passive -d galp.com -> limitar tempo
theHarvester -d example.com -b all
```

Os exemplos apresentados utilizam o domínio example.com, devendo este ser substituído pelo domínio em análise. Em alternativa, podes utilizar uma das seguintes Ferramenta web DNSDumpster, SecurityTrails, crt.sh (certificados SSL – pesquisar por %.galp.com). Para a identificação dos emails corporativos, utilize Google Dorks para pesquisa de emails ("@galp.com") em pdfs.

Parte 2 - Análise de Presença Digital e Social

Mapear a presença online da GALP em plataformas portuguesas e internacionais.

Questão 2.1. Utilize **Sherlock** ou **WhatsMyName** para procurar por perfis oficiais:

- @galp_energia, @galp, etc.

Questão 2.2. Utilize **Twint** (Twitter Intelligence Tool) para:

- Analisar atividade recente nos perfis oficiais
- Identificar menções relevantes no contexto português
- Extrair metadados de publicações

Questão 2.4. Aplique **ExifTool** em:

- Imagens do site corporativo
- Fotos de projetos divulgados
- Material de comunicação social

Parte 3 - Documentos Públicos e *Compliance*

Investigação de documentos públicos da GALP em fontes portuguesas.

Questão 3.1. Usando **Google Dorks**, executa no mínimo 6 pesquisas avançadas, usando operadores:

- site:cmvm.pt galp
- site:galp.com filetype:pdf
- site:galp.com sustentabilidade
- site:portaldocidadao.pt "GALP"

Questão 3.2. Utilize **Wayback Machine** para analisar versões do site da Galp em anos diferentes

- Estratégia
- Sustentabilidade



Universidade do Minho
Departamento de Informática
Mestrado em Engenharia Informática

Parte 4 - Análise Geográfica e Operacional

Mapear ativos físicos e operações em Portugal.

Questão 4.1. Usando **Google Earth Pro** ou QGIS:

- Localize estações de serviço GALP
- Identifique instalações industriais

Parte 5 - Segurança e Vulnerabilidades

Análise de segurança da infraestrutura digital.

Questão 5.1. Usando **Shodan** e **Censys**:

- Pesquise por `org:"GALP"`
- Identifique serviços expostos
- Verifique configurações de segurança

Questão 5.2. Com **Have I Been Pwned** e **DeHashed**:

- Verifique vazamentos de emails corporativos
- Pesquise por credenciais associadas a domínios GALP
- Analise padrões de passwords vazadas

Questão 5.3. Aplique **BuiltWith** ou **Wappalyzer**:

- Identifique tecnologias web utilizadas
- Analise stack tecnológica

Parte 6 - Análise de Mercado e Competidores

Posicionamento no mercado energético português.

Questão 6.1. Usando **SEMrush** ou **SimilarWeb** (versões gratuitas):

- Analise tráfego do site galp.pt
- Compare com os competidores EDP e Repsol

Questão 6.2. Com **Google Trends**:

- Analise interesse por "GALP" em Portugal
- Compare com termos do setor energético
- Identifique sazonalidade e tendências