

# OSINT

Beware. Your data is out there.

RootedCON - 25/05/2024

EDIÇÃO PORTUGAL

# \$whoami

- ▶ Pedro Vieira
- ▶ Engenheiro de Cibersegurança
- ▶ Certified Ethical Hacker
- ▶ Licenciado pela Universidade do Minho



# Aviso Legal & Leis

# Aviso Legal

## Disclaimer - Aborrecido, mas necessário

- ▶ Toda a informação contida nesta apresentação destina-se exclusivamente para fins educacionais e de consciencialização.
- ▶ **Apresentação ao vivo.** Não é um ambiente controlado e alguns conteúdos podem ser inapropriados para alguns participantes.
- ▶ **Declino qualquer responsabilidade** pelo uso, uso indevido, download, ou visualização dos links desta apresentação.
- ▶ Esta apresentação **não está diretamente relacionada** com o meu trabalho ou empregador.



# Aviso Legal

## Disclaimer - Evitem atividades ilegais

- ▶ Alguns links, sites, software ou outros itens listados podem ou não ser legais, delito, crime no seu país.
- ▶ Por favor, **verifique que lhe é permitida** a consulta dos sites, e o eventual uso do software listado.
- ▶ Ignorância acerca das leis aplicáveis **não é desculpa** para transgressões ou actividades ilegais.
- ▶ Atividades ilegais podem implicar problemas ou mesmo prisão.
- ▶ **Verifique sempre o que é legal e as leis aplicáveis.**



# Leis

## Lei Portuguesa e Organizações

### ► Lei

- Diário República Eletrónico ([link](#))
- ANACOM ([link](#))

### ► Organizações

- CNCS - Centro Nacional de Cibersegurança ([link](#))
  - Notificação de Incidentes ([link](#))
  - CERT.PT ([link](#))
- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#))
- Ministério Público ([link](#))

# Agenda

- Consciencialização
- Tempo de OSINT
- Portugal - Sol, Mar e Transparência
- RGPD andas perdido?
- Automóvel
- Histórias verídicas
- Antes de começar a pesquisar

# Consciencialização



# Consciencialização

## A internet sabe e não esquece

- ▶ Informação publicada em modo privado pode ser tornada pública por outra pessoa
- ▶ Quando a informação é publicada
  - ▶ Mostra onde e quando (hábitos e rotinas)
- ▶ A internet tem memória
  - ▶ Arquivo.pt ([link](#))
    - ▶ Exemplo ([link](#)) ➡
  - ▶ Internet Archive - Wayback Machine ([link](#))
    - ▶ Exemplo ([link](#)) ➡

# Consciencialização

## Perfil

- ▶ Telefone/Telemóvel (Longevidade do mesmo número)
  - ▶ Sync.Me ([link](#))
- ▶ Username
  - ▶ WhatsMyName ([link](#)) ➡
- ▶ Email (Reutilização do mesmo username)
  - ▶ Gmail ([link](#))
- ▶ Redes Sociais (Reutilização do mesmo username)
  - ▶ Facebook ([link](#))
  - ▶ LinkedIn ([link](#))
  - ▶ Tinder ([link](#)) ([link](#)) ➡

# Consciencialização

## Mapas

- ▶ Nunca lá estive, mas conheço como a palma da minha mão.
- ▶ Vista de estrada
  - ▶ Google Street View ([link](#)) ➡
- ▶ Mapa/ Vista de Satélite
  - ▶ Google Maps ([link](#))
  - ▶ Overpass Turbo ([link](#)) ➡
    - ▶ Wizard: plant:source=nuclear
  - ▶ Wayback example ([link](#)) ➡
- ▶ Tips, Tricks and Techniques ([link](#))

# Consciencialização

## Fotografias

- ▶ Análise da fotografia
  - ▶ Localização
  - ▶ Data em que foi tirada
  - ▶ Elementos identificativos na imagem
- ▶ Pesquisa de imagem
  - ▶ Identificar o castelo ([link](#)) ➡



# Consciencialização

## Fotografias

- ▶ Uma imagem vale mais do que mil palavras.

- ▶ Análise do ficheiro

- ▶ Metadados
- ▶ GPS ([link](#)) →
- ▶ Google Maps ([link](#)) →


- ▶ Ferramentas

- ▶ CleanUp ([link](#))
- ▶ AperiSolve ([link](#)) →

**exifdata**

**SUMMARY**  
**DETAILED**  
**LOCATION**  
**UPLOAD**

IMG\_20190223\_163027.jpg



(click for original)

**Camera**  
Xiaomi Redmi 3

**GPS Position**  
40.989952 degrees N, 7.395051 degrees W

**Date of Creation**  
2019:02:23 16:30:27

**Resolution**  
4160x3120

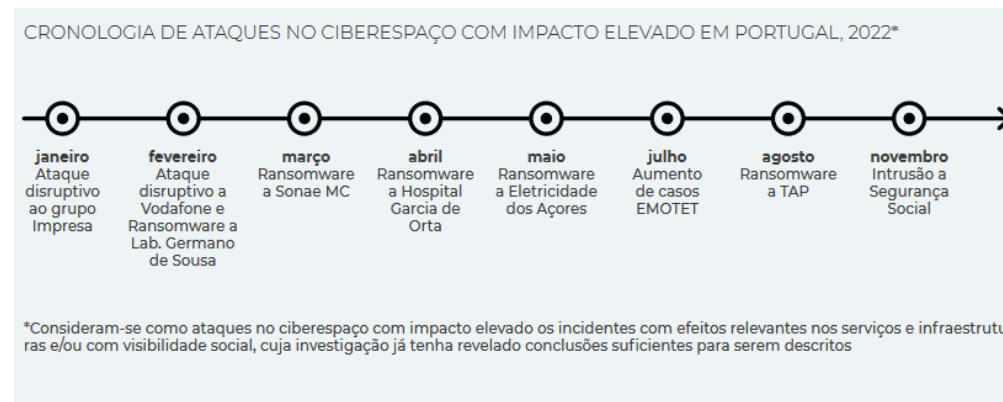
**SUMMARY**

Make	Xiaomi
Model	Redmi 3
Aperture	2
Exposure Time	1 / 1506 (0.00066401062416999 sec)
Focal Length	4.2 mm
Flash	Auto, Did not fire
File Size	1447 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	4160
Image Height	3120
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered
Exposure Program	Not Defined
Date and Time (Original)	2019:02:23 16:30:27
Metering Mode	Center-weighted average
Color Space	sRGB
Exposure Index	140
Sensing Method	Unknown (0)
Exposure Mode	Auto
Focal Length In 35 mm	0 mm
Format	
Scene Capture Type	Standard
Gain Control	Low gain up
ISO	100
Compression	JPEG (old-style)

# Consciencialização

## Quando empresas são atacada

- ▶ Quando as empresas são atacadas os dados privados são expostos. Passam a ser “públicos”.
- ▶ Troy Hunt
  - ▶ HavelBeenPwned ([link](#)) ➡
  - ▶ Pwned websites ([link](#)) ➡
  - ▶ Domain search ([link](#))
- ▶ Relatório CNCS
  - ▶ Cibersegurança em Portugal 2024 ([link](#))
  - ▶ Cibersegurança em Portugal 2023 ([link](#))



Fonte: CNCS



# Consciencialização

## Motores de busca para IOT

- ▶ Pastas partilhadas acessíveis a 8 mil milhões de pessoas ([link](#)) ➡

- ▶ Contabilidade - 6
- ▶ Clientes - 3
- ▶ Faturacao - 1
- ▶ Faturacao - 2
- ▶ Primavera - 6
- ▶ SAGE - 13
- ▶ Winrest - 148

Shares			Shares		
Name	Type	Comments	Name	Type	Comments
Web	Shares		ADMIN\$	Disk	Remote Admin
Public	Name	Type	C\$	Disk	Default Share
homes			IPC\$	Shares	
SCAN	Multimedia		Printer	Name	Type
SERVER	Download	Shares			Comments
Multimedia	Web	Name	IPC\$	IPC	
Recordings	Public				
home	homes	Multimedia	IPC\$	IPC	IPC Service ("")
MBPT	TESTE	Download			Carlos
PLOUTOS	JOAO	Web			TTT
TGS	DUDA	Public			SAIG
MIRUS	SEGMENTO_POPULAR	homes			Zonesoft
USB	SOFTWARE	BackupR			FTP
IPC\$	home	home			Clientes_Sage
	IPC\$	IPC\$			Clientes_XD
					XD Extreme
					video
					photo
					music
					admin
					...

# Tempo de OSINT

“Information is not knowledge”

Albert Einstein



# OSINT - Open-source intelligence

## Pegada Digital

- ▶ Open-source intelligence (OSINT) consiste na recolha e análise de dados obtidos de fontes disponíveis ao público em geral, como jornais, revistas científicas e comunicação social para produzir conhecimento.
- ▶ Colecionar dados de:
  - ▶ motores de busca (Google, ...)
  - ▶ redes sociais (Facebook, ...)
  - ▶ sites governamentais
  - ▶ mapas
  - ▶ ...
- ▶ E depois extrair/relacionar/inferir nova informação com maior valor/potencial.

# Quem sou eu?

## Pesquisar, e voltar a pesquisar

- ▶ Começando apenas com um nome
  - ▶ Pedro António Oliveira Vieira
- ▶ Google ([link](#)) ➡
- ▶ Google “Improved Search” ([link](#)) ➡
- ▶ Google “Improved Search” + empresa ([link](#)) ➡
- ▶ LinkedIn ([link](#)) ➡
  - ▶ Perfil público estava a expor demasiada informação
- ▶ Certified Ethical Hacker ([link](#))
- ▶ As minhas notas no github ([link](#))



# Motores de Busca

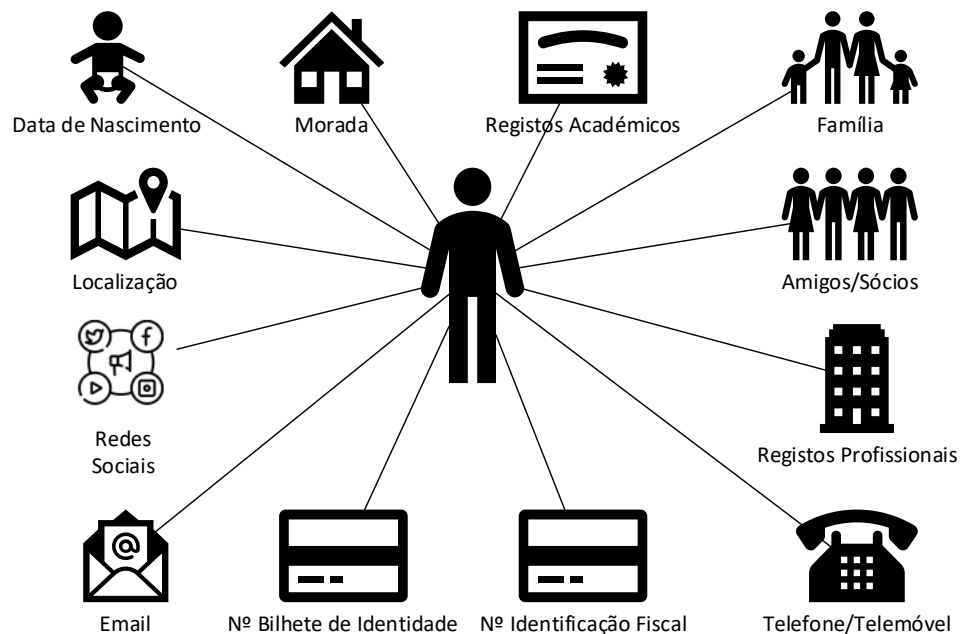
## A internet é mais do que o Google

- ▶ Motores de busca diferentes → regras/crawlers diferentes → resultados diferentes
- ▶ Google ([link](#))
- ▶ Bing ([link](#)) ➡
- ▶ Yahoo ([link](#))
- ▶ DuckDuckGo ([link](#)) ➡
- ▶ Baidu (China) ([link](#))
- ▶ Yandex (Russia) ([link](#))
- ▶ SAPO (Portugal) ([link](#)) ➡
- ▶ Podem pedir para serem removidos de um motor de busca, mas não de todos ☹ ([link](#))

# Quem és tu?

## Pesquisar, e voltar a pesquisar

- ▶ Pesquisem o vosso nome e analisem os resultados
  - ▶ Como viram a pesquisa pode ser melhorada



- ▶ Tipicamente esta informação permite **validar a identidade** numa chamada telefónica.

# Portugal - Sol, Mar e Transparência

Ser transparente com 8 mil milhões de pessoas?

# Portugal

## Membros do Governo/Parlamento

### Portal

### Portal do Governo



- Membros do Governo ([link](#))
  - Primeiro-Ministro ([link](#)) ➡
- Redes sociais

### Portal

### Portal da Assembleia da República



- Deputados em funções ([link](#))
- Informação Pessoal ([link](#)) ➡
- Registo de interesses ([link](#)) ➡
- Participação em empresas ([link](#)) ➡
- Dados Abertos ([link](#))

# Portugal

## Portal BASE - Contratos Públicos Online

### Portal



### Portal BASE

- O Portal BASE centraliza a informação sobre os contratos públicos ([link](#))
- Contratos ([link](#)) ➡
- Anúncios ([link](#))
- Entidades ([link](#)) ➡
  - Empresas e Pessoas
- Indicadores ([link](#))
- Exemplos
  - Assembleia da República - 600054128 ([link](#)) ➡
  - SP&M, Sociedade de Advogados, RL - 510445020 ([link](#))
  - José Pedro Aguiar-Branco & Associados ... - 506584020 ([link](#)) ➡
- Proteção de dados pessoais ([link](#)) ([link](#)) ➡

# Portugal

## Ministério da Justiça - Publicações

### Portal

### Publicações de Atos Societários e de outras entidades



- Consultar e pesquisar todas as publicações ([link](#))
- Exemplos
  - Oliveiras Gold de Portugal, Lda - 510172466 ➡
  - José Pedro Aguiar-Branco & Associados ... - 506584020 (Não disponível)
  - Farfetch - 507398505 ➡
- Ajuda: Para obter NIF, pesquisar em motor de busca por: “nome da empresa” nif



# Portugal

## Portal DRE - Diário da República Electrónico

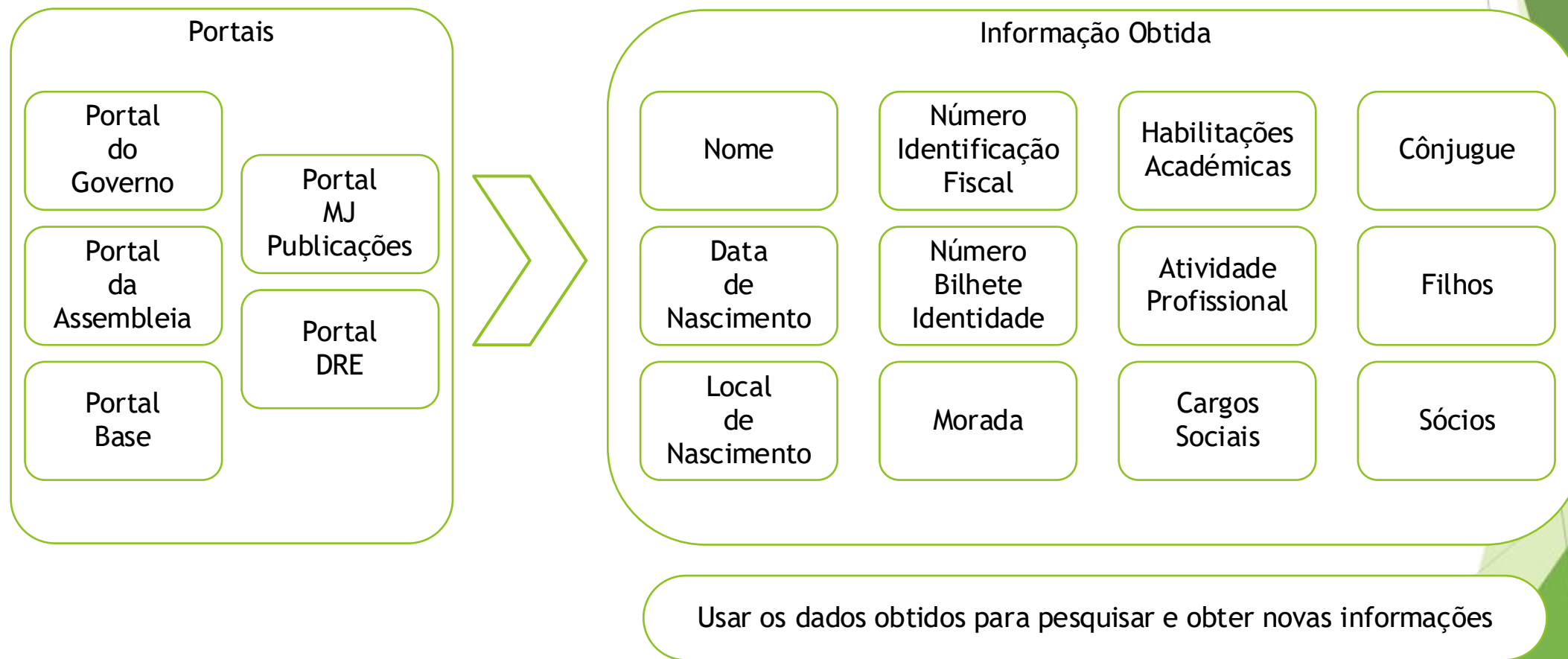
### Portal



- Pesquisa ([link](#))
  - "Luís Filipe Montenegro Cardoso de Morais Esteves" →
  - "Pedro António Oliveira Vieira"
  - "28227/2007"
- Pesquisa avançada ([link](#))
- Site alternativo - DRE Tretas ([link](#))

# Portugal

## Membros do Governo/Parlamento



# RGPD andas perdido?





Acumulação compulsiva

# Portugal

## Portal

## Registo Civil Online



- Registo Civil Online ([link](#)) →
  - Certidão de nascimento 
  - Certidão de casamento 
  - Certidão de óbito 
  - Certidão de perfilhação 

## Portal

## Plataforma aberta para dados públicos portugueses



- Conjuntos de dados ([link](#))
- Exemplos:
  - Contratos Públicos - Portal BASE - IMPIC ([link](#)) →
  - Arquivo.pt - pesquisa páginas do passado ([link](#))

# Portugal

## Ensino

### Portal

### DGES - Direção-Geral de Ensino Superior



- Candidatura ao ensino superior público - colocações ([link](#)) ➡
- Listagem Ordenada de Candidatos
- Listagem de Colocados
- Nota: Já não é possível consultar os anos anteriores, pelo menos aqui 😊

### Portal

### DGAE - Direção - Geral da Administração Escolar



- Concurso Externo 2022/2023 - Listas Definitivas ([link](#)) ➡
- Exemplo:
  - Grupo 110 - 1º Ciclo do Ensino Básico ([link](#)) ➡

# Portugal

## Curriculum Vitae e Recibos de Vencimento

### Curriculum Vitae

- Pesquisa: "curriculum vitae" filetype:pdf site:.pt ([link](#)) ➡
- 135000 resultados; muitos falsos positivos
- Pesquisa melhorada: "nome" "curriculum vitae" filetype:pdf site:.pt ([link](#))
- Phishing de informação: Anúncios de emprego falsos

### Recibos de vencimento

- Pesquisa: "recibo de vencimento" filetype:pdf ([link](#)) ➡
- Exemplos:
  - Por questões de privacidade não serão apresentados
- Pela taxa de IRS é possível inferir estado civil e número de filhos

# Portugal

## Cadernos eleitorais e Listas de alunos

### Cadernos eleitorais/associados/membros

- Pesquisa: "caderno eleitoral" filetype:pdf ([link](#)) ➡
- Pesquisa: "Lista de sócios" filetype:pdf ([link](#))
- Exemplo:
  - Universidade do Minho ([link](#))
  - Ministério Público ([link](#))

### Lista de alunos/inscrições/pautas

- Pesquisa: pautas aluno filetype:pdf ([link](#))
- Pesquisa: "Lista de alunos" filetype:pdf site:up.pt ([link](#)) ➡
- Exemplo:
  - Universidade do Porto - 2008/2009 ([link](#))
  - Agrupamento de Escolas de Proença-a-Nova ([link](#))

# Portugal

## Ordens Profissionais

### Ordem dos Advogados

- Ficheiros PDF “expostos” ([link](#)) ➡
- Listas de inscritos ([link](#))
- Pautas ([link](#))
- Emails da ordem usados em sites pessoais
- ~1500 credenciais expostas em listas de credenciais

### Ordem dos Contabilistas

- Ficheiros PDF “expostos” ([link](#)) ➡
- Caderno eleitoral ([link](#))
- Lista dos técnicos oficiais de contas
  - Diário da República III série - 2005 - referência 23 751 ([link](#))



# Portugal

## Listas públicas

- Lista de subvenções e benefícios públicos e de doações (IGF) ([link](#))
- Lista pública de execuções ([link](#))
- Venda de Bens Penhorados em Processos Executivos ([link](#))
- Lista de devedores na Segurança Social ([link](#)) ➡
- Listas de Devedores na Autoridade Tributária e Aduaneira ([link](#)) ➡
  
- Pesquisa de bens penhorados - não oficial ([link](#))
- Pesquisa de bens penhorados - não oficial ([link](#))

# Automóvel


# Portugal

## Automóvel

### Portal

### Automóvel On-line




- Pedido da Certidão Permanente do Registo Automóvel ([link](#)) 
  - Exemplo do documento ([link](#)) ➡
- Pesquisar carro do Primeiro-Ministro ([link](#)) ➡
  - Matrícula : 89-QS-04 ([link](#)) ➡

### Portal

### IMT - Instituto da Mobilidade e dos Transportes



- Serviços IMT online.pt ([link](#)) 
  - Veículos → Certidão
    - Número de inspeções obrigatórias
    - Características do Veículo

# Portugal

## Automóvel

### Portal

### ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões



- Verificar Seguro Através da Matrícula ([link](#)) ➡
  - Matrícula : 89-QS-04

### Portal

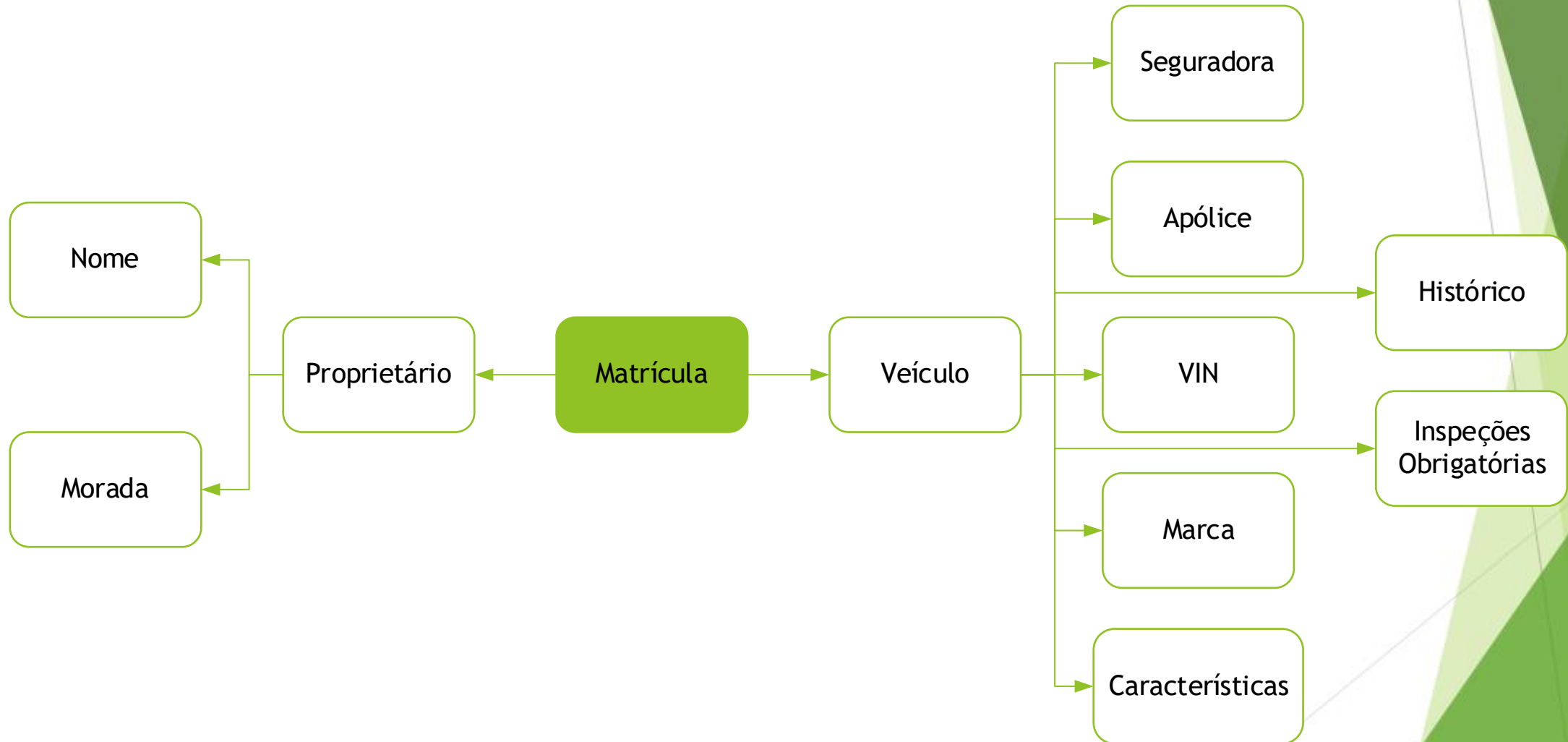
### Lastvin



- Mercedes-Benz VIN Decoder ([link](#)) ➡
- Será que o Luís Montenegro fica com o carro?

# Portugal

## Automóvel



# Histórias verídicas

# Histórias verídicas

## Portugal

### Crédito de loja

- Como comprar um livro quase sem precisar de dinheiro
- Cartão de cliente de loja
- Informação certa: número de telemóvel e nome completo
- Crédito no cartão

### Dados de clientes

- Pedido de fatura com NIF
  - Nome
  - Morada
- Atualização de dados de cliente no balcão sem documentos

# Histórias verídicas

## O caso do rapper Pop Smoke

- ▶ Rapper Pop Smoke Murdered in Home Invasion ... By 4 Masked Gunmen ([link](#)) ➡
- ▶ Instagram Posts
  - ▶ Location Tag
- ▶ Geolocation
  - ▶ Reverse Image
- ▶ Google Maps
  - ▶ Local Recon
- ▶ Airbnb/Zillow (Rent/Real-estate)
  - ▶ House photos (Outside and Inside)
  - ▶ Layout
- ▶ YouTube Video: The Cyber Mentor ([link](#))



# Histórias verídicas

## Mensagem da Ella do futuro



Deutsche Telekom  
Message from Ella | Without Consent

# Antes de começar a pesquisar

Don't get under the spotlight.

# OSINT Notes

## As minhas notas e alguns links

- ▶ My OSINT notes ([link](#))
  - ▶ OSINT ([Presentation](#))
  - ▶ Awareness ([Presentation](#))
- ▶ Sofia Santos - How to do a small OSINT investigation ([blog](#)) ([video](#))
- ▶ Michael Bazzel - IntelTechniques ([link](#)) ([book](#)) ([magazine](#))
- ▶ OSINT Combine ([link](#)) ([bookmarks](#))
- ▶ OSINT Dojo ([link](#))
- ▶ OSINTCurio.us ([link](#))
- ▶ OSINT Techniques ([link](#))
- ▶ Start.me pages ([link](#)) ([example](#))
- ▶ Technisette ([link](#))
- ▶ Open-Source Intelligence Tools and Resources Handbook 2020 ([link](#))

# OSINT

## Capture The Flag & Desafios

- ▶ TraceLabs CTF ([link](#)) ([notes](#))
- ▶ Hacktoria ([link](#)) ([notes](#))
- ▶ Cyber Detective CTF ([link](#))
- ▶ Cyber Investigator CTF ([link](#))
- ▶ TryHackMe ([link](#))
  - ▶ Search for OSINT ([link](#)) ([notes](#))
- ▶ Blue Team Labs Online - Cyber Range ([link](#))

# OSINT

## Ferramentas e mais ferramentas

- ▶ OSINT FRAMEWORK ([link](#)) ➡
  - ▶ Yups, only one link is all it takes. But others worth mentioning.
- ▶ OSINT4ALL ([link](#))
- ▶ Intel Techniques ([link](#))
- ▶ OSINT Techniques ([link](#))
- ▶ Technisette ([link](#))
- ▶ Cyber Detective ([link](#))
- ▶ OSINT Link ([link](#))
- ▶ Aware Online ([link](#))

# OBRIGADO

## Q&A