



/RootedCON



PROT  
APP

# iATTACK SURFACE MANAGEMENT

*DIY for free!*

Miguel de la Cal Bravo  
Félix Paniagua Mérida

# *External Attack Surface Management: DIY for free!*

**Miguel de la Cal Bravo  
Félix Paniagua Mérida**

**8 de marzo de 2024**



X



# Agenda

- 1. Introducción**
- 2. Necesidades y objetivos**
- 3. Inventario de activos**
- 4. Tecnologías y herramientas**
- 5. Demostración y ejemplos**
- 6. Futuras mejoras**



# 1. Introducción



# 1. Introducción

01



## External ASM (Attack Surface Management)

Exploración de la superficie expuesta en Internet de una organización (activos, tecnologías, servicios, versiones, ...)

02



## DIY (Do It Yourself)

- Organizaciones con pocos recursos
- *“La imaginación al poder.”*
- Desarrollo “sencillo”, con scripting en Python y otras utilidades

03



For free!

Herramientas y utilidades gratuitas

## 2. Necesidades y objetivos



## 2. Necesidades y objetivos

### Esquema Nacional de Seguridad (RD 311/2022)

#### Artículo 8. Prevención, detección, respuesta y conservación

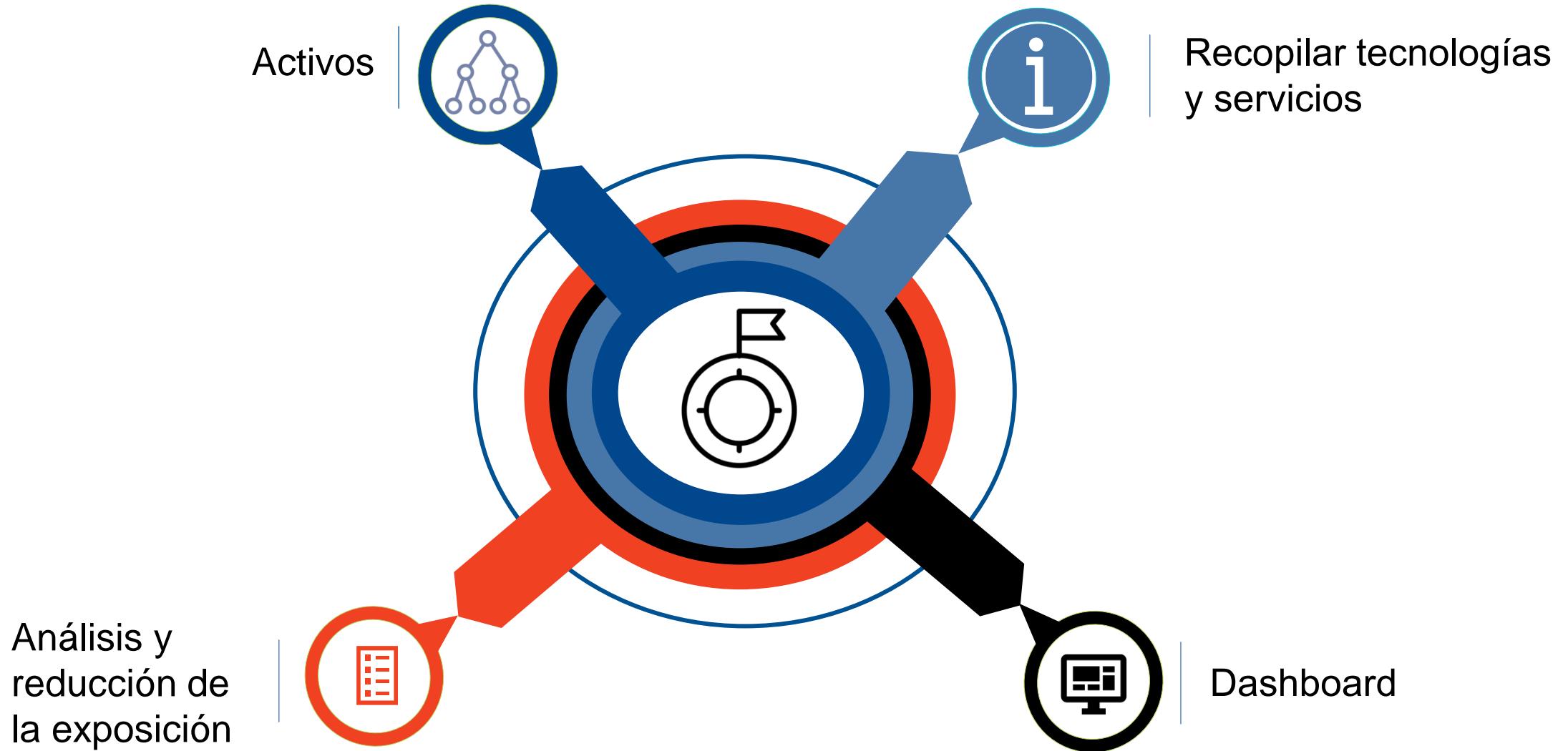
- “2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la **reducción de la superficie de exposición**, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse”

#### Nuevo principio básico

- Art. 10. **Vigilancia continua** y reevaluación periódica



## 2. Necesidades y objetivos



# 3. Inventario de activos



# 3. Inventario de activos

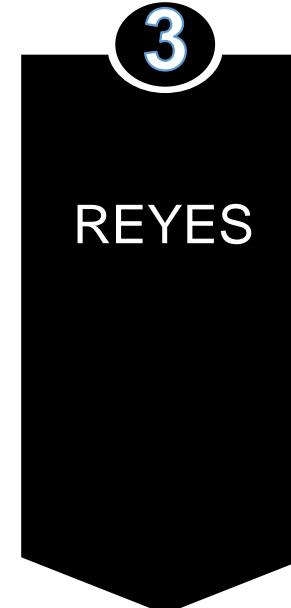
## 🔍 Búsqueda de dominios y subdominios (pasivas/activas)

- 🔒 [Crt.sh](#)
- 🔒 [DNSDumpster](#)
- 🔒 [OWASP Amass](#)
- 🔒 [SecurityTrails](#)
- 🔒 [Sublist3r](#)
- 🔒 [ViewDNS.info](#)
- 🔒 Google Dorks:
  - *site:\*.dominio.es filetype:...*



# 3. Inventario de activos

## 🗣 Fuentes internas



A S M

# 4. Tecnologías y herramientas



# 4. Tecnologías y herramientas

## ➤ Recopilación de información



Direcciones IP



Activo (Sí/NO)



¿HTTP/S?



Certificados:  
emisor, fecha de  
validez, nº serie,  
versión TLS



Tecnologías y  
versiones



Otros: códigos de  
estado, agrupar  
por dominios, TLD

# 4. Tecnologías y herramientas

## 🛠 Herramientas



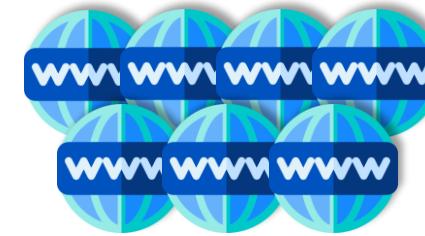
Scripting en Python

WebAnalyzer: <https://github.com/webanalyzer/webanalyzer.py>

WebAnalyzer (rules): <https://github.com/webanalyzer/rules>



Librerías: DNS, requests, ssl, re, socket, datetime, pytz, json, ...



{  
}

¿está activa?: "true",  
¿HTTP/S?: "true",  
Tecnologías: "x",  
Versiones: "y",  
...  
}

# 4. Tecnologías y herramientas

 Cuadro de mandos interactivo (aplicación web)

 Utilización del stack de **Elastic – ELK** (open source)

 Herramientas:

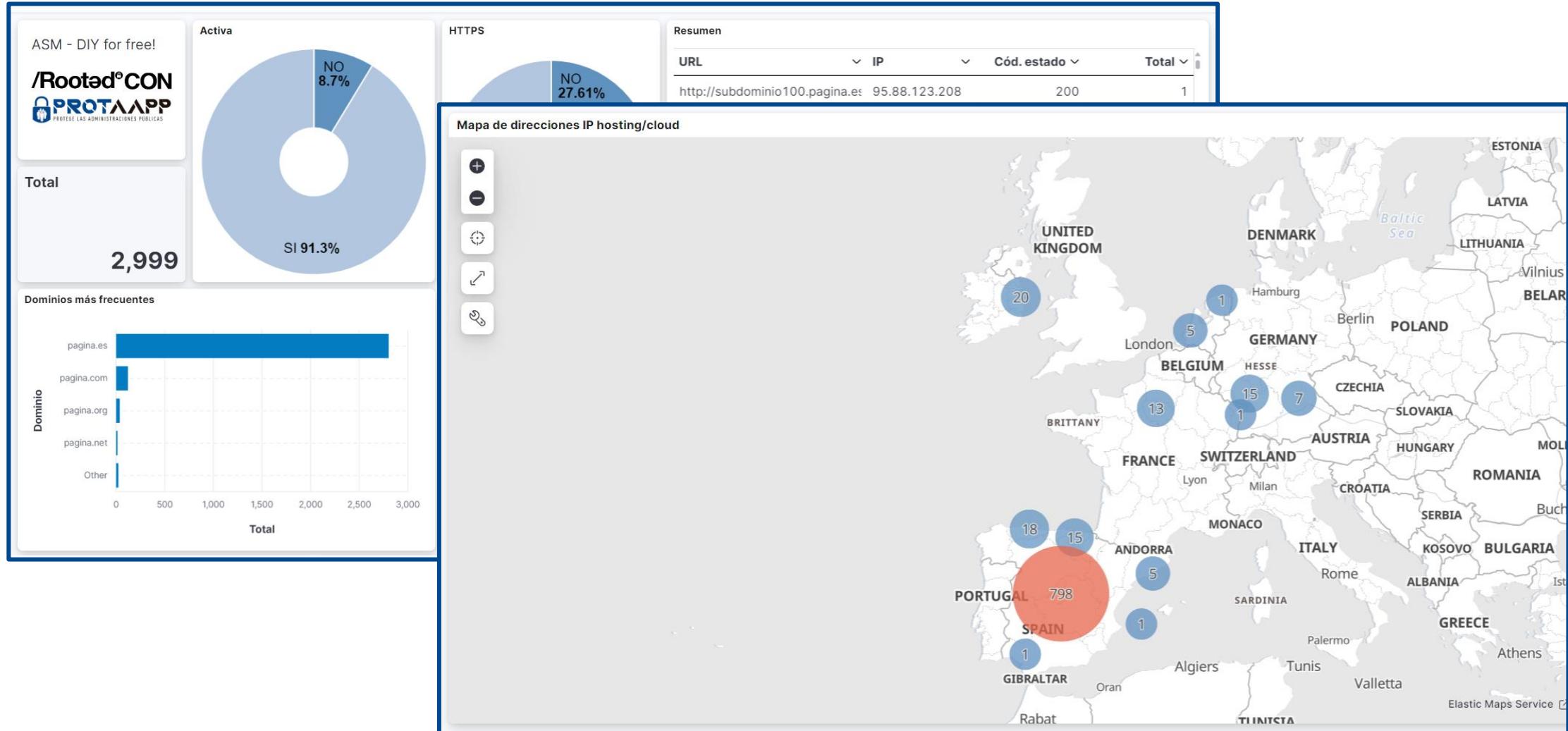
- **Logstash**: ingestá de datos y procesamiento de **JSON**
- **Elasticsearch**: indexado y almacenamiento de datos
- **Kibana**: interfaz gráfica, cuadro de mandos



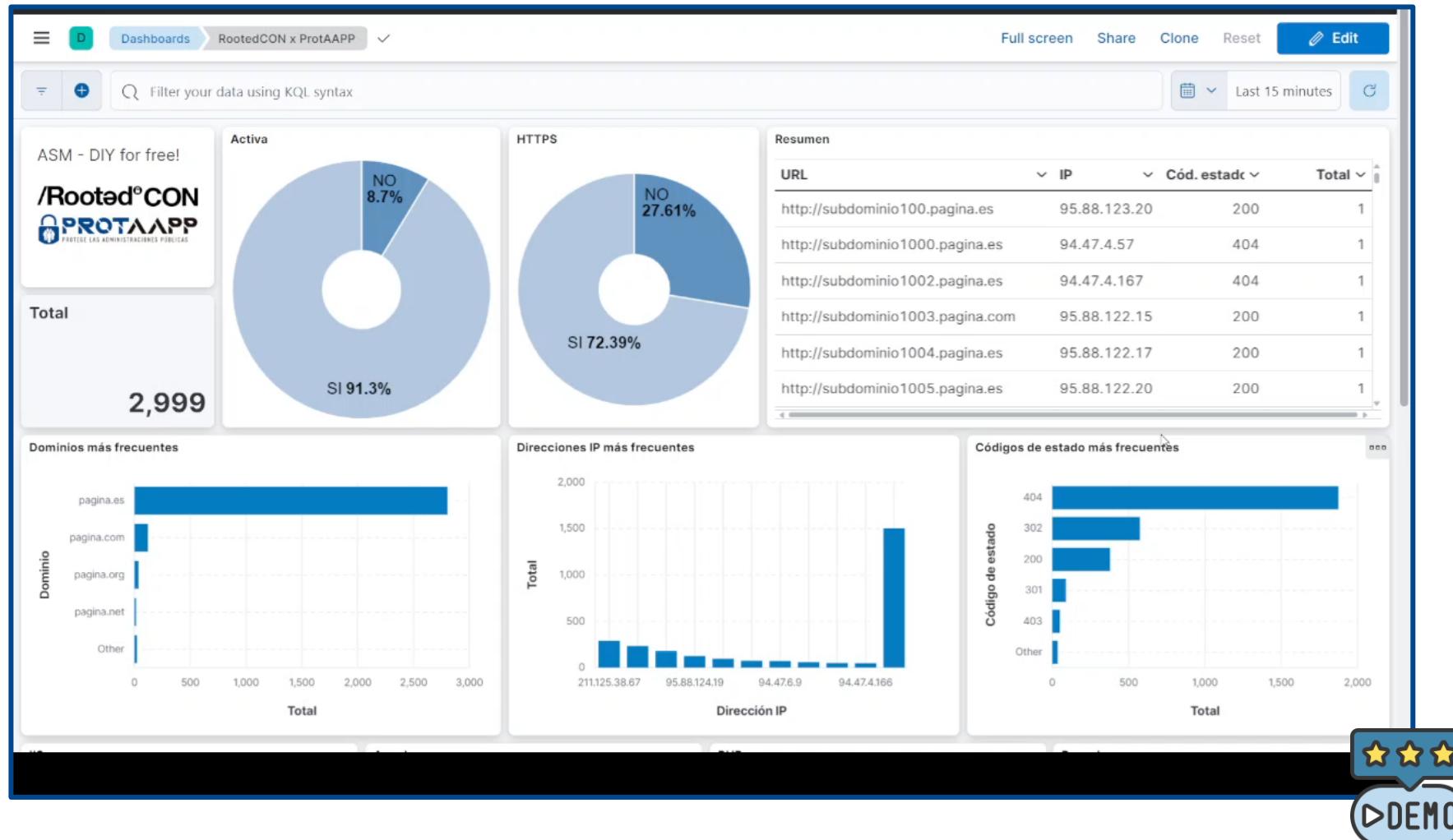
# 5. Demostración y ejemplos



# 5. Demostración y ejemplos



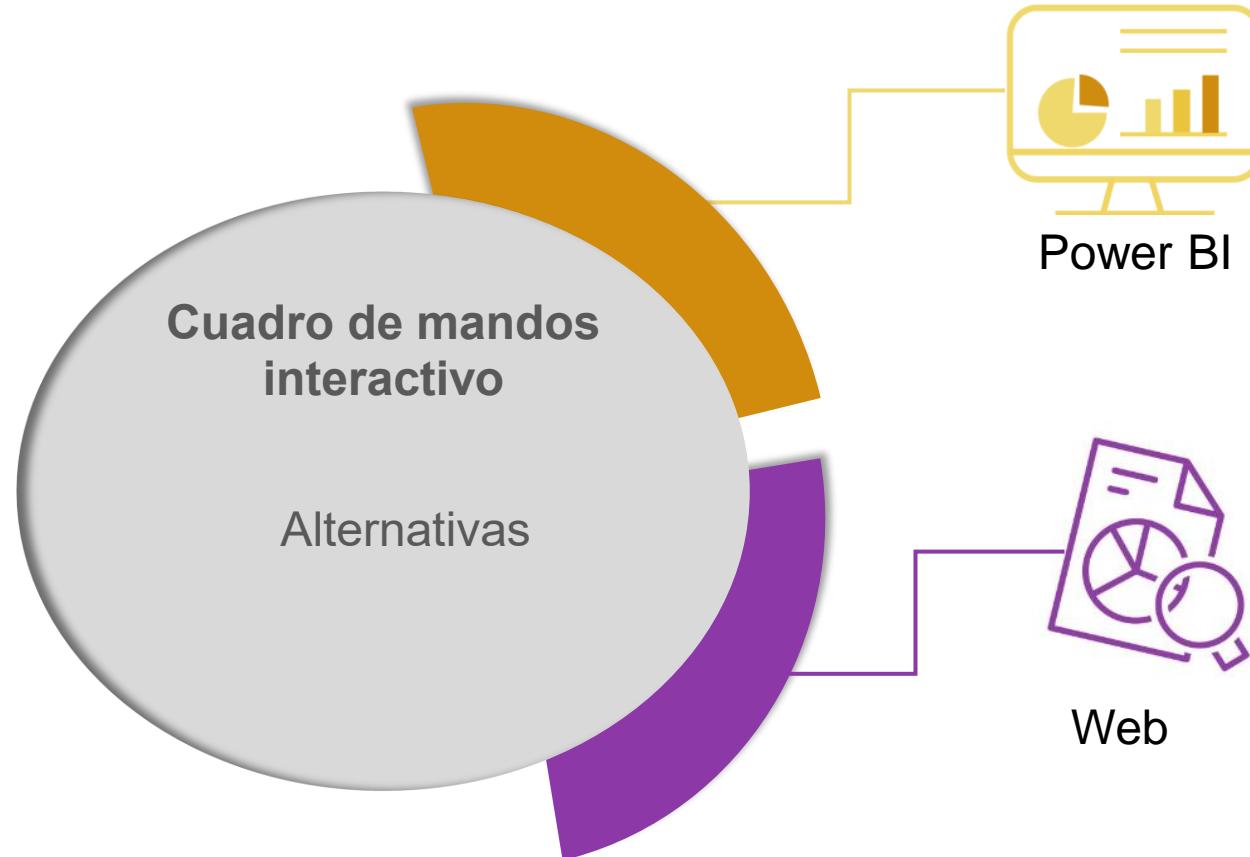
# 5. Demostración y ejemplos



# 6. Futuras mejoras



# 6. Futuras mejoras



# 6. Futuras mejoras

The screenshot displays a web application interface for managing web exposure. The main header reads "Exposición web" and "Dashboard". The top navigation bar includes links for "Dashboard", "RootedCON", and "PROT APP".

**Left Panel:** A bar chart titled "Grafico Barras" showing the distribution of technologies across different classifications. The Y-axis ranges from 0 to 1500. The X-axis categories are "Clasificación" (Clasification) and include "Php", "Cms", "Apache", "IIS", "Tomcat", "JBoss", and "Citrix".

**Right Panel:** A detailed view of a specific URL entry.

- Summary Metrics:** Shows 1 URL, 1 IP, 0 web vulnerabilities, 1 web alert, and 2 total alerts.
- Filter Options:** Includes "Clasificación" (set to "Todas"), "URL" (set to "723"), and "Tecnologías" (set to "apache-tomcat\_version").
- Table View:** Displays a table with columns "clean\_url", "Atributo", "Valor", and "Clasificación". One row is shown: "subdominio723.pagina.es", "apache-tomcat\_version", "7.0.107", and "Tomcat".

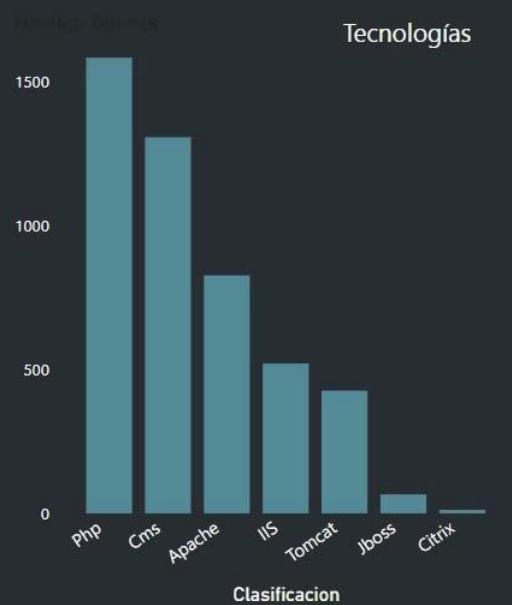


# 6. Futuras mejoras

### Exposición web

Dashboard /RootedCON PROT ANFT

### Tecnologías



Tecnología	Cantidad
Php	1500
Cms	1300
Apache	800
IIS	500
Tomcat	400
Jboss	100
Citrix	50

### Servicios Desplegados



Servicio Desplegado	Cantidad
Toledo	5004
Dublin	1438
Berlin	4
Londres	2

### Alertas

7247

Dashboard Detalles

Microsoft Bing © 2024 Microsoft Corporation. Términos de uso.

★★★

▶ DEMO



# 6. Futuras mejoras

dominio.tld / Vision Dominio

Creado: 2001-05-22 00:00:00  
Expira: 2026-05-22 00:00:00

Subdominios: 12.962 (-36%)

IPs: 3.411 (-34%)

Puertos: 1.243 (+11%)

SSL: 439 (+36%)

Servicios: 12 (-33%)

HTTP: 765 (-44%)

Paneles: 36 (-36%)

Metadatos: 6.943 (+13%)

Phishing: 32 (-7%)



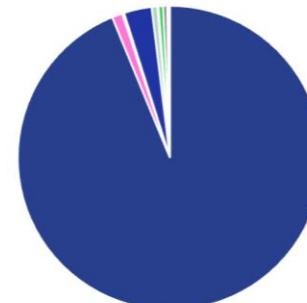
Top Activos por País

País	Hits
Spain	~950
Unknown	~100

Top Activos por Ciudad

Ciudad	Hits
Almería	~250
Seville	~700
Unknown	~100

Top Servicios



Top CPEs

CPE	HITS
apache:http_server	20
cpe:/o:microsoft:windows	14
isc:bind	11
apache:coyote_http_connector:1.1	10
igor_sysoevnginx	8
cpe:/o:canonical:ubuntu_linux	7

Top Tecnologías

NAME	COUNT
Java	620
Apache HTTP Server	346
Apache Tomcat	320
Google Tag Manager	261
PHP	231
Bootstrap	213



# 6. Futuras mejoras

## ➡ SOON Mejoras y algunas limitaciones:

### ⌚ Detección automática de **nuevos dominios**/subdominios

- ¡OJO al ruido! Comprobar si los activos nos pertenecen

### ⌚ Obtención de **vulnerabilidades**

- ¡OJO a los falsos positivos!

### ⌚ Scoring/puntuación de **riesgo** de los activos

- No es tan fácil de determinar



# *External Attack Surface Management: DIY for free!*

**Miguel de la Cal Bravo  
Félix Paniagua Mérida**

**8 de marzo de 2024**



X

