

Herramientas OSINT gratuitas que todo investigador digital debería conocer

Cuando hablamos de **OSINT (Open Source Intelligence)** nos referimos a la obtención y análisis de información procedente de fuentes públicas.

Ya sea para ciberseguridad, periodismo, investigación, auditorías, reputación online o análisis de empresas, estas herramientas permiten recopilar una enorme cantidad de información sin necesidad de acceder a sistemas privados.

□ Buscadores tradicionales (más potentes de lo que parecen)

Google Dorks

Permite realizar búsquedas avanzadas mediante operadores especiales.

Ejemplos:

```
site:empresa.com filetype:pdf  
intitle:"index of"  
inurl:admin
```

□ Útil para localizar documentos, directorios expuestos o información publicada accidentalmente.

- [Google Search](#)

Bing

A menudo devuelve resultados diferentes a Google y puede ser muy útil en investigaciones.

- [Microsoft Bing](#)
-

☐ Infraestructura y dispositivos expuestos

[Shodan](#)

El buscador más famoso para encontrar dispositivos conectados a Internet:

- Cámaras IP
- Routers
- Servidores
- Sistemas industriales
- Equipos IoT

Permite filtrar por:

- País
 - Ciudad
 - Puerto
 - Producto
 - Organización
-

[Censys](#)

Alternativa moderna a Shodan.

Especialmente útil para:

- Certificados SSL
 - Infraestructura web
 - Subdominios
 - Hosts expuestos
-

□ Investigación de usuarios y redes sociales

[Namechk](#)

Comprueba si un nombre de usuario existe en decenas de plataformas.

Ideal para:

- Investigación de perfiles
 - Marca personal
 - Detección de cuentas relacionadas
-

[WhatsMyName](#)

Una de las mejores herramientas OSINT actuales para rastrear usuarios en cientos de servicios online.

[Sherlock Project](#)

Proyecto open source que busca automáticamente un nombre de usuario en múltiples redes sociales.

☐ Búsqueda inversa de imágenes

[TinEye](#)

Permite saber dónde aparece una imagen en Internet.

Muy útil para:

- Verificar fotografías
 - Detectar perfiles falsos
 - Encontrar versiones originales
-

[Google Lens](#)

Actualmente suele ofrecer mejores resultados que la búsqueda clásica por imágenes.

☐ Información sobre dominios

[Whois Lookup ICANN](#)

Consulta información de registro de dominios.

Permite conocer:

- Registrador
 - Fechas de creación
 - Servidores DNS
-

[SecurityTrails](#)

Excelente para:

- DNS históricos
 - Subdominios
 - Cambios de infraestructura
-

[DNSDumpster](#)

Genera mapas visuales de dominios y subdominios.

☐ Metadatos de documentos

[ExifTool](#)

La referencia absoluta para extraer metadatos de:

- Fotografías
 - PDFs
 - Documentos Office
 - Vídeos
-

□ **Análisis de tráfico web**

Si quieres estimar visitas de una web:

[Similarweb](#)

Muestra gratuitamente:

- Tráfico estimado
 - Principales países
 - Fuentes de tráfico
 - Sitios similares
-

[SEMrush](#)

La versión gratuita ofrece datos básicos de tráfico y posicionamiento SEO.

[Ahrefs Webmaster Tools](#)

Especialmente útil para análisis SEO y enlaces.

☐☐ Visualización y análisis de relaciones

[Maltego Community Edition](#)

Una de las herramientas OSINT más conocidas.

Permite representar gráficamente relaciones entre:

- Personas
 - Empresas
 - Correos
 - Dominios
 - Redes sociales
-

[SpiderFoot HX Community Edition](#)

Automatiza gran parte del trabajo OSINT.

Puede recopilar información sobre:

- Dominios
- IPs
- Emails
- Usuarios
- Infraestructura

□ Inteligencia artificial aplicada a OSINT

Perplexity AI

Muy útil para:

- Investigación rápida
- Resumen de fuentes
- Verificación inicial

ChatGPT

Ayuda a:

- Organizar hallazgos
- Analizar información
- Crear informes
- Generar consultas avanzadas