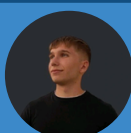


OSINT: LA FORMA LEGAL DE ACCEDER A INFORMACIÓN VALIOSA



[@saulruizplaza](https://twitter.com/saulruizplaza)



01

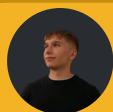
¿QUÉ ES OSINT?

OSINT (Open Source Intelligence) es la recopilación de información de fuentes accesibles públicamente. En ciberseguridad, se usa tanto para defender como para atacar, ya que esta información puede ser explotada por ciberdelincuentes para obtener ventajas tácticas.



FUENTES COMUNES

- Redes Sociales: Facebook, LinkedIn, Twitter, Instagram.
- Sitios Web Públicos: Blogs, noticias, foros, repositorios.
- Registros Públicos: WHOIS, registros gubernamentales.
- Documentos Abiertos: PDFs, informes, investigaciones disponibles públicamente.



[@saulruizplaza](https://twitter.com/saulruizplaza)

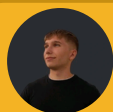




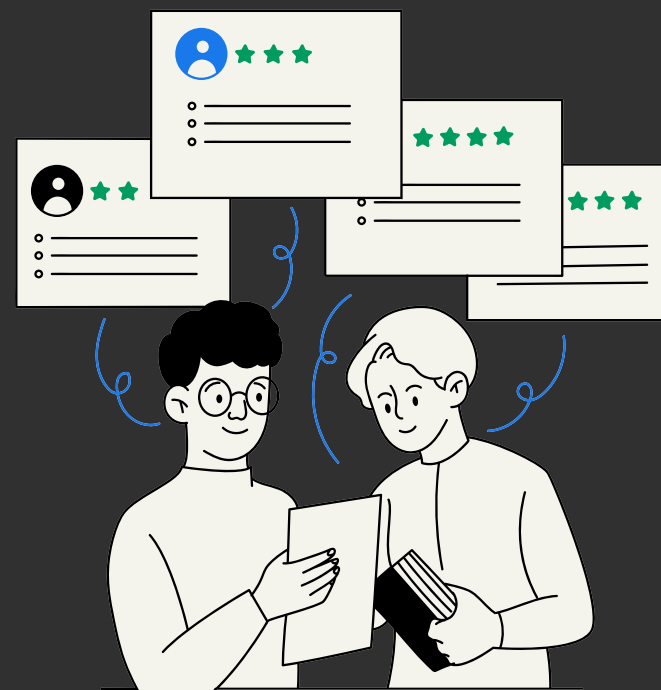
APLICACIONES DE OSINT EN CIBERSEGURIDAD

En el ámbito defensivo, OSINT se utiliza para identificar vulnerabilidades, detectar amenazas tempranas y proteger sistemas contra intrusiones. También es clave en la investigación forense, ya que permite analizar incidentes cibernéticos previos y comprender las tácticas empleadas por los atacantes.

En el ámbito ofensivo, OSINT facilita la realización de ataques de ingeniería social, como el phishing, al recolectar información pública para diseñar ataques más específicos. Además, juega un papel crucial en la fase de reconocimiento, donde los atacantes extraen datos de fuentes abiertas para planificar y ejecutar ataques más efectivos.



[@saulruizplaza](#)





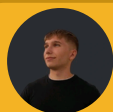
TÉCNICAS OSINT

@saulruizplaza



ANÁLISIS DE METADATOS

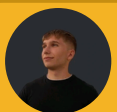
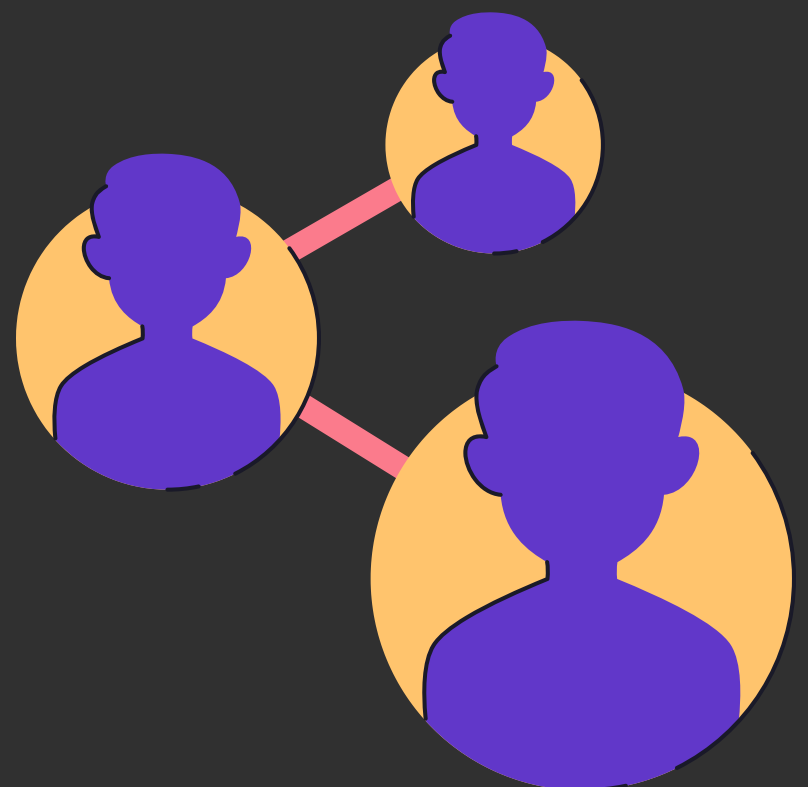
Los metadatos son datos que describen otros datos, y se encuentran ocultos en archivos como documentos, imágenes, videos y más. El análisis de metadatos permite obtener información sobre la creación de un archivo, el software utilizado, las fechas de modificación, la ubicación geográfica de fotos, e incluso las personas que han trabajado con el archivo. Esta técnica puede ser crucial para detectar si un archivo ha sido alterado o para obtener información adicional que no es visible a simple vista.





SCRAPING DE REDES SOCIALES

Consiste en la recolección de información pública de plataformas como LinkedIn, Facebook, Twitter, e Instagram. Las herramientas de scraping permiten extraer datos como nombres, ubicaciones, correos electrónicos y conexiones. Esta técnica se usa tanto para realizar investigaciones de inteligencia como para obtener datos para ataques dirigidos.





HERRAMIENTAS DE OSINT

@saulruizplaza



05

SHODAN

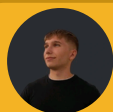
Shodan es un motor de búsqueda que permite encontrar dispositivos conectados a Internet. A diferencia de Google, que busca contenido web, Shodan busca dispositivos (cámaras, routers, servidores, etc.).

FUNCIONALIDADES

- Permite buscar dispositivos expuestos en línea, con detalles como puertos abiertos, direcciones IP y banners de servicios.
- Ayuda a localizar dispositivos IoT inseguros, lo que puede ser crítico para prevenir ataques como DDoS, explotación de vulnerabilidades conocidas e incluso conexión remota a cámaras de seguridad.



SHODAN



[@saulruizplaza](https://twitter.com/saulruizplaza)



06

MALTEGO

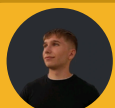
Herramienta de inteligencia visual que permite el análisis y la visualización de las relaciones entre diversos elementos, como personas, dominios, direcciones IP, organizaciones y otros objetos. Utiliza una serie de “transformaciones” que extraen datos de diversas fuentes para construir un gráfico que muestra las conexiones entre los objetos investigados.

FUNCIONALIDADES

- Mapea y visualiza las relaciones entre personas, empresas, direcciones IP y más.
- Utiliza una variedad de fuentes de datos públicas, como bases de datos WHOIS, redes sociales, registros de DNS, entre otros.



MALTEGO



[@saulruizplaza](#)

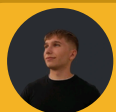


THEHARVESTER

Recopila información sobre correos electrónicos, subdominios, direcciones IP y otros datos a partir de fuentes públicas. Es especialmente útil para la fase de reconocimiento en pruebas de penetración (pentesting), ya que permite identificar activos de una organización a partir de fuentes abiertas.

FUNCIONALIDADES

- Recopila información de motores de búsqueda como Google, Bing y Yahoo.
- Permite extraer detalles de registros DNS, servidores de correo electrónico y otras fuentes relacionadas.



[@saulruizplaza](https://twitter.com/saulruizplaza)





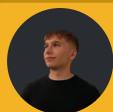
CONSIDERACIONES ÉTICA Y LEGALES

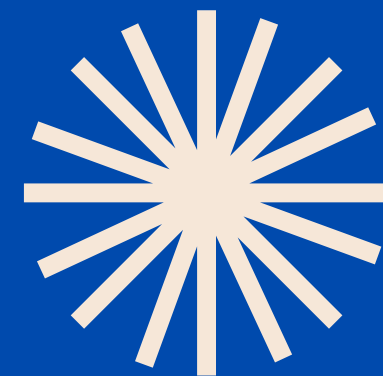
PRIVACIDAD Y PROTECCIÓN DE DATOS

El uso de OSINT debe respetar las leyes de privacidad y protección de datos a nivel mundial. A pesar de ser información pública, debe cumplir con normativas como el GDPR y otras regulaciones locales.

LÍMITES DEL USO DE OSINT

El uso de OSINT debe ser legítimo y ético. No debe emplearse para actividades ilegales como espionaje, acoso o recopilación de datos con fines malintencionados.





MUCHAS GRACIAS



@saulruizplaza