FGC

CIBERSEGURIDAD Y GESTIÓN DE RIESGOS

Cómo buscar las huellas que dejas para que te ataquen

OSINT – Open Source Intelligence

Descargo de responsabilidad

- Esta presentación es únicamente con fines didácticos
- No soy abogado, ni te estoy dando consejos legales
- No te estoy dando permiso, ni autorización para que hagas algo con la información aquí mostrada
- Las vistas u opiniones son mías y no representan a mi empleador

Hacerte invencible significa **conocerte a ti mismo**; aguardar para descubrir la vulnerabilidad del adversario significa **conocer a los demás**.

Siempre que quieras atacar a un ejército, asediar una ciudad o atacar a una persona, **haz de conocer previamente la identidad de los generales que la defienden, de sus aliados, sus visitantes, sus centinelas y de sus criados;** así pues, haz que tus espías averigüen todo sobre ellos.

No será ventajoso para el ejército actuar sin conocer la situación del enemigo **y conocer la situación del enemigo no es posible sin el espionaje**

Sun Tzu - El Arte de la guerra

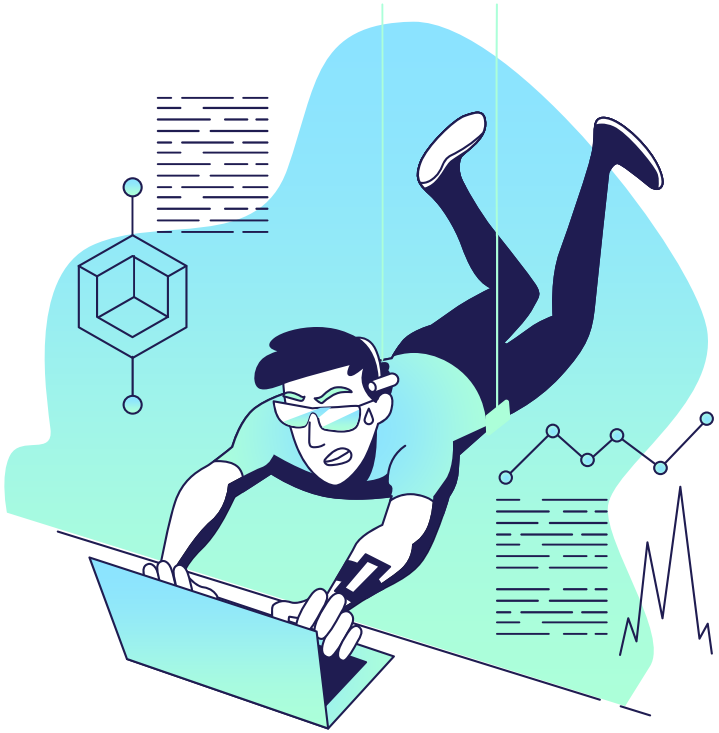
Agenda

- Inteligencia y clasificación
- OSINT y el proceso
- Donde ~~buscar~~ conseguir información
- Riesgos y recomendaciones

Inteligencia y sus clasificaciones

¿Qué es Inteligencia (en el contexto de información)?

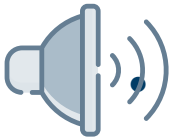
Convertir un conjunto de datos e informaciones inconexas y con escaso valor, en un producto llamado inteligencia, que sirve **para racionalizar y tomar decisiones.**



Clasificaciones de Inteligencia

HUMINT: Human Intelligence

IMINT: Image Intelligence



SIGINT: Signal Intelligence

OSINT: Open Source Intelligence

Clasificaciones de Inteligencia

HUMINT

IMINT

SIGINT

OSINT

Clasificaciones de Inteligencia

HUMINT

IMINT

SIGINT

OSINT

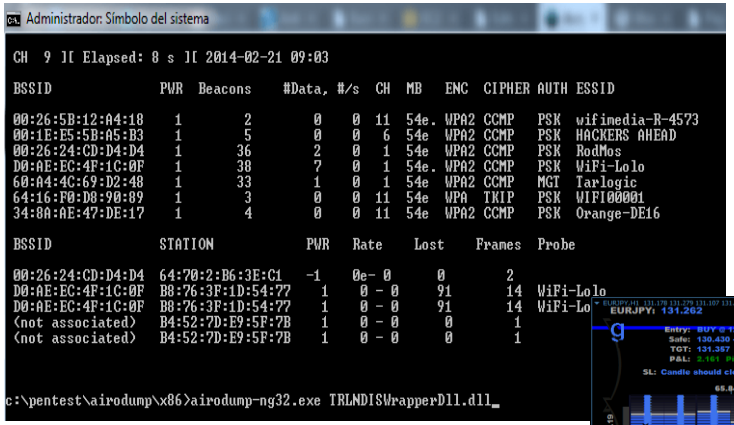
Clasificaciones de Inteligencia

HUMINT

IMINT

SIGINT

OSINT



COMINT, ELINT, TELINT, MASINT

Clasificaciones de Inteligencia

HUMINT

IMINT

SIGINT

OSINT

OSINT Open Source Intelligence. El término OPEN se refiere a la **información que se consigue públicamente**.

Servicio de Impuestos Internos

Registro Civil e Identificación

Que se puede ~~buscar~~ conseguir con OSINT

Información de Personas

Repositorios históricos

Información de organizaciones

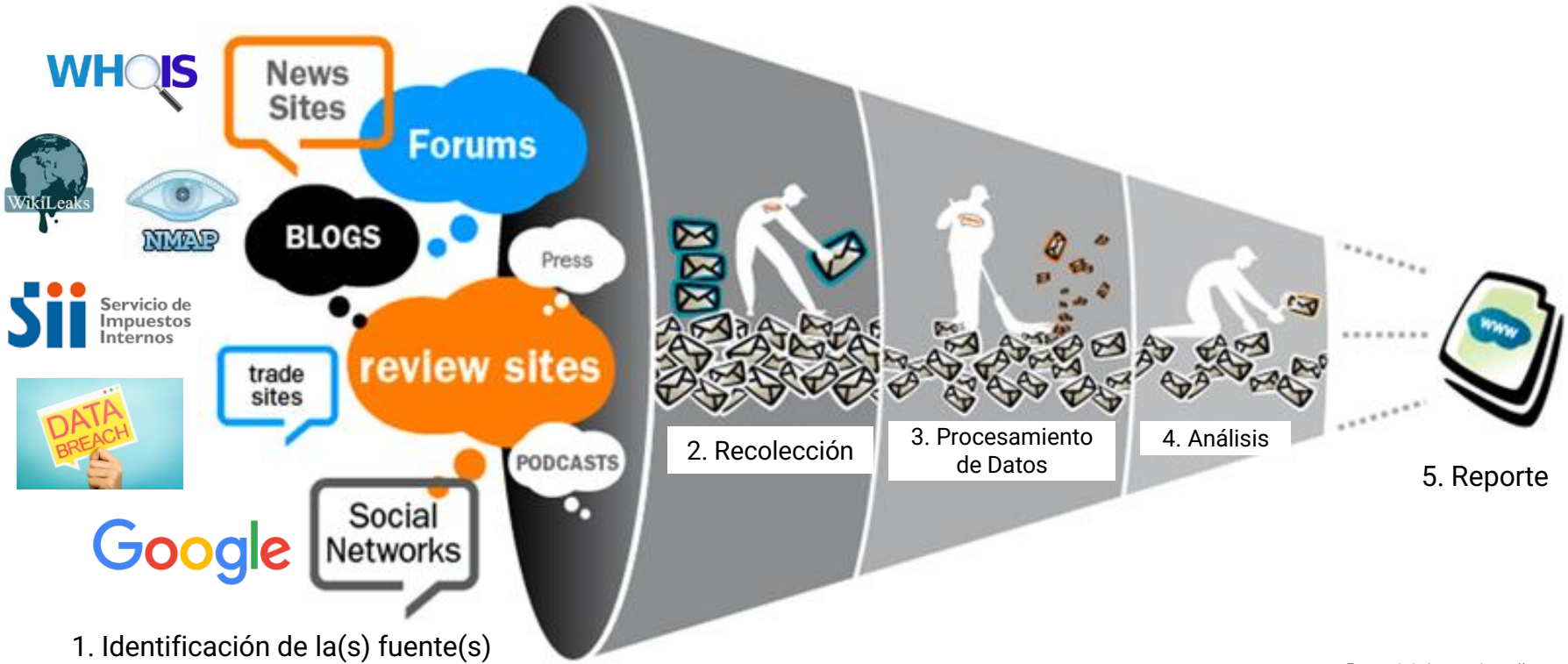
Información de Infraestructura Tecnológica

Otros tipos

Casi todo lo que ~~quieras~~ puedas encontrar

Proceso de OSINT

El proceso de OSINT (5 pasos)

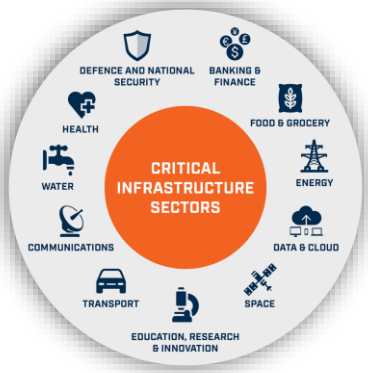


1. Identificación de la(s) fuente(s)

Fuente de la imagen: https://www.openpr.com/

Quienes realizan OSINT (Lícitamente)

Gobiernos



Organismos de seguridad Nacional

Empresas

Abogados e Investigadores

Data Scientists

Firmas y equipos de ciberseguridad

Tipos de uso en Ciberseguridad

Ofensivo

Obtener información antes de realizar un ataque

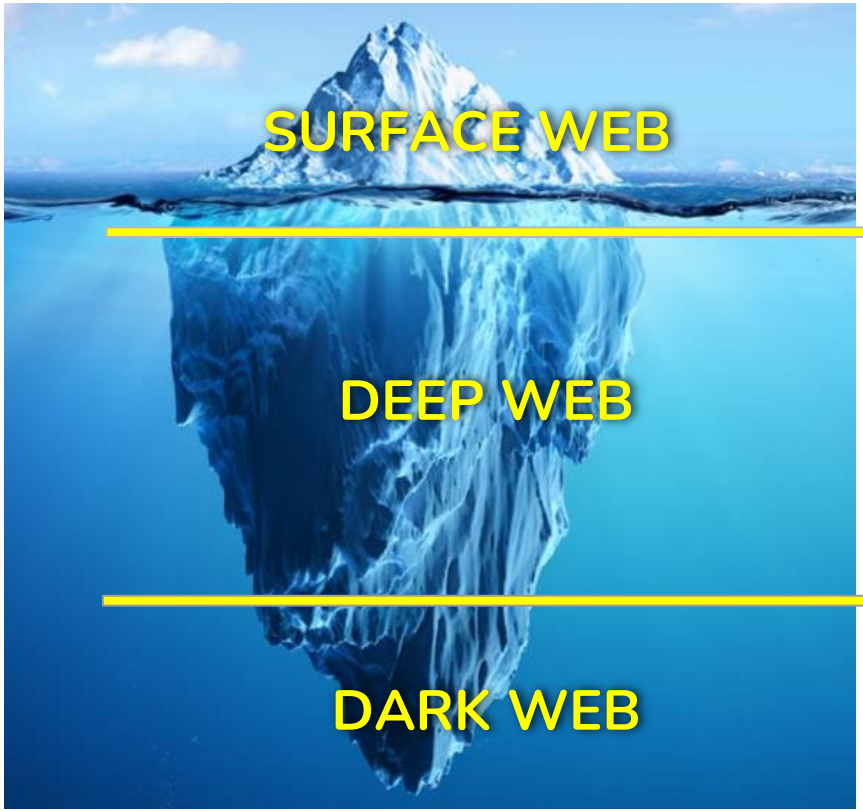
Defensivo

Identificar brechas como pudieran realizarte un ataque o a tu empresa

OSINT da la oportunidad al atacante y al defensor

Cómo y Dónde conseguir información (huellas)

Internet: Principal aliado



Información pública

- Buscadores (Google, Bing)
- Wikipedia
- Sitios públicos
- Foros, Redes Sociales*,

OSINT

Información cuyo acceso es controlado:

- Emails
- Sitios de solo miembros
- Registros médicos y bancarios
- Registros confidenciales de empresas

Se requiere software especial para ingresar:

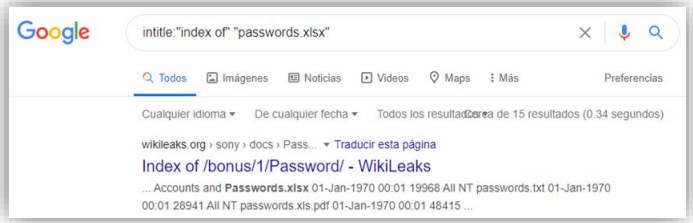
- Garantiza el “Anónimato”
- Sitios de contenido o ventas ilegales
- Activismo (Democrático, hacktivismo)

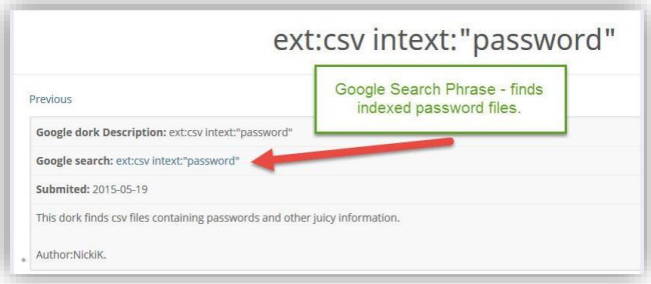
Dónde conseguir información
Resumen

- Buscadores de Internet (fuente favorita para hacer OSINT)
- Buscadores especializados
- Sitios web públicos y especializados
- Sitios web oficiales, corporativos o de gremios
- Redes Sociales
- Herramientas especializadas (algunas gratuitas)

Dónde conseguir información – Buscadores

1. Google - https://google.com (Dorks, los maravillosos dorks)
2. Bing - https://www.bing.com
3. Censys - https://censys.io
4. Fofa - https://fofa.so
5. Dogpile - http://www.dogpile.com
6. https://all-io.net/ - Para buscar en los principales buscadores de internet (google, bing, duckduckgo, etc.



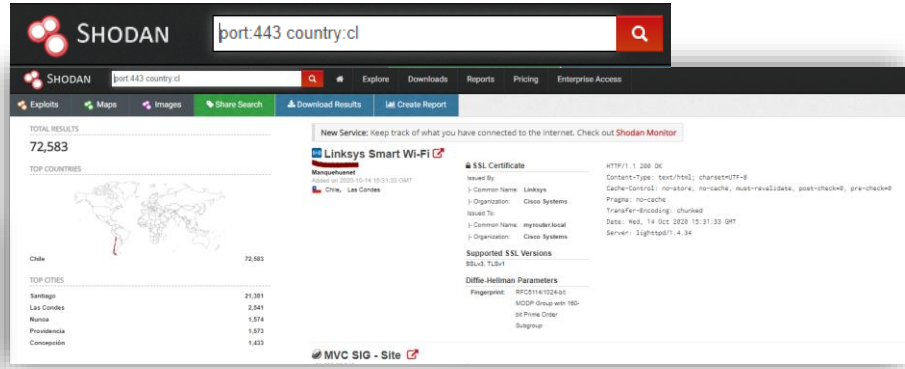


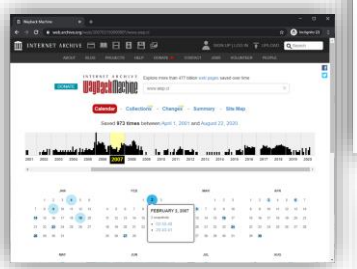
¿Te has buscado en internet usando comillas dobles?
Ej. “Fernando Graterol”

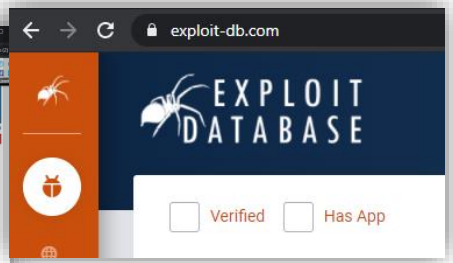
Dónde conseguir información – Buscadores Especializados

Buscadores “especializados”:

1. Shodan - https://shodan.io
2. Fofa - https://www.fofa.so
3. Archives - https://archive.org/
4. https://censys.io/
5. https://www.oshadan.com/
6. https://www.zoomeye.org/
7. https://hunter.io/
8. Google Hacking Database - www.exploit-db.com



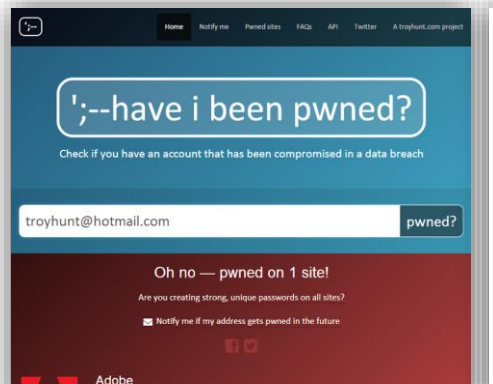


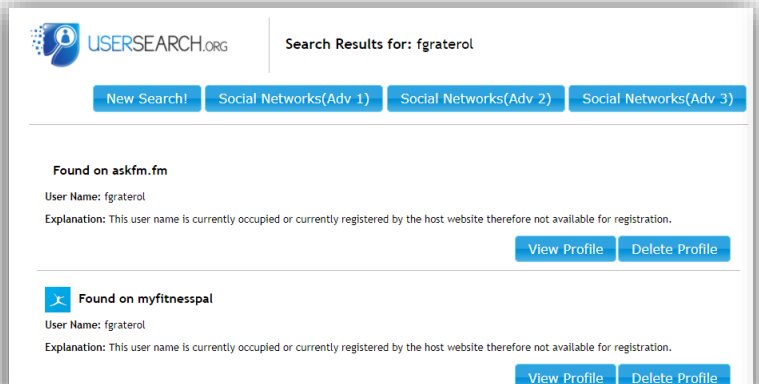


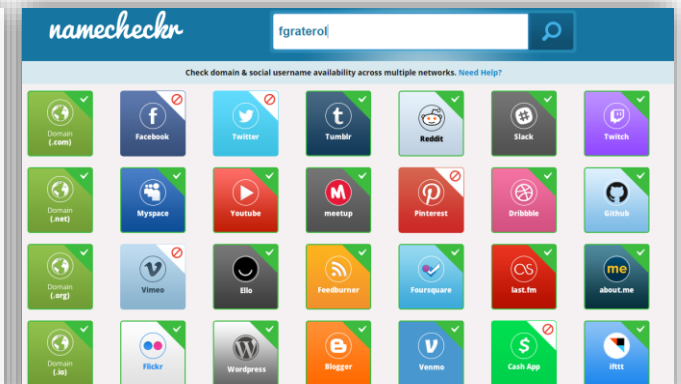
Dónde conseguir información – Sitios Web especializados

Ej. Páginas para revisar cuentas de usuarios

1. https://haveibeenpwned.com/ Have I've been Pawned - Para ver si tu correo estuvo en un leak
2. GhostProject - Para ver si tu correo estuvo en un leak
3. https://usersearch.org/ para verificar si el nombre de usuario está creado en algún sitio
4. https://www.namecheckr.com/ para verificar si el nombre de usuario está creado en algún sitio
5. https://centralops.net/co/ para buscar información del dominio (fecha registro, persona que registra, etc.)



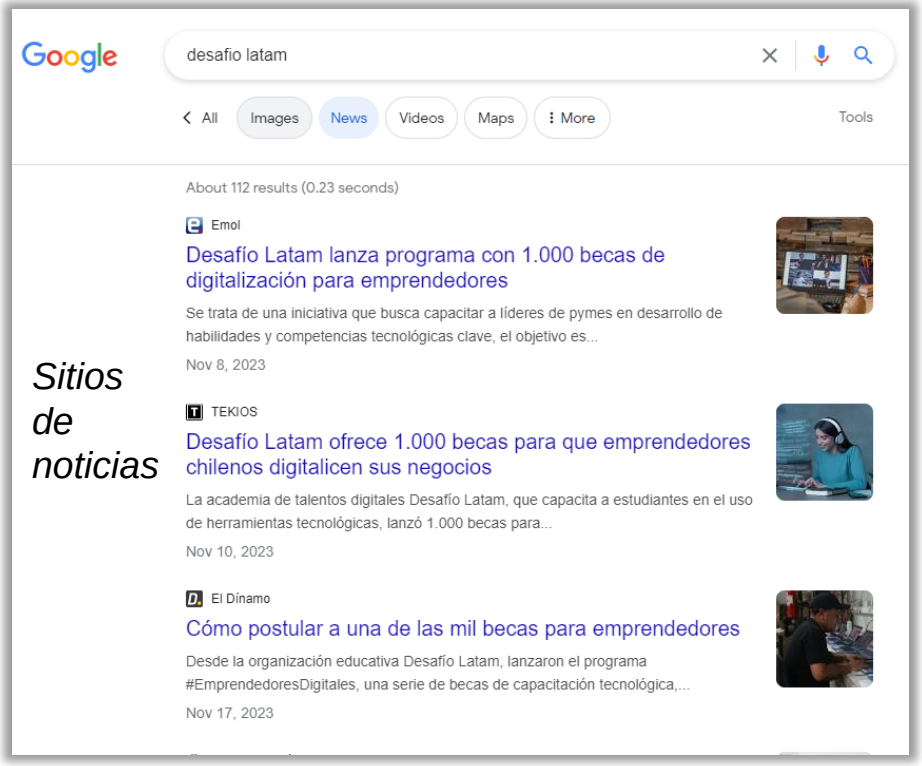




Dónde conseguir información –
Sitios Web Públicos y especializados

Sitios públicos:

- Wikileaks
- Diarios
- Páginas de noticias
- Google Maps*



Dónde conseguir información – Sitios Web Oficiales

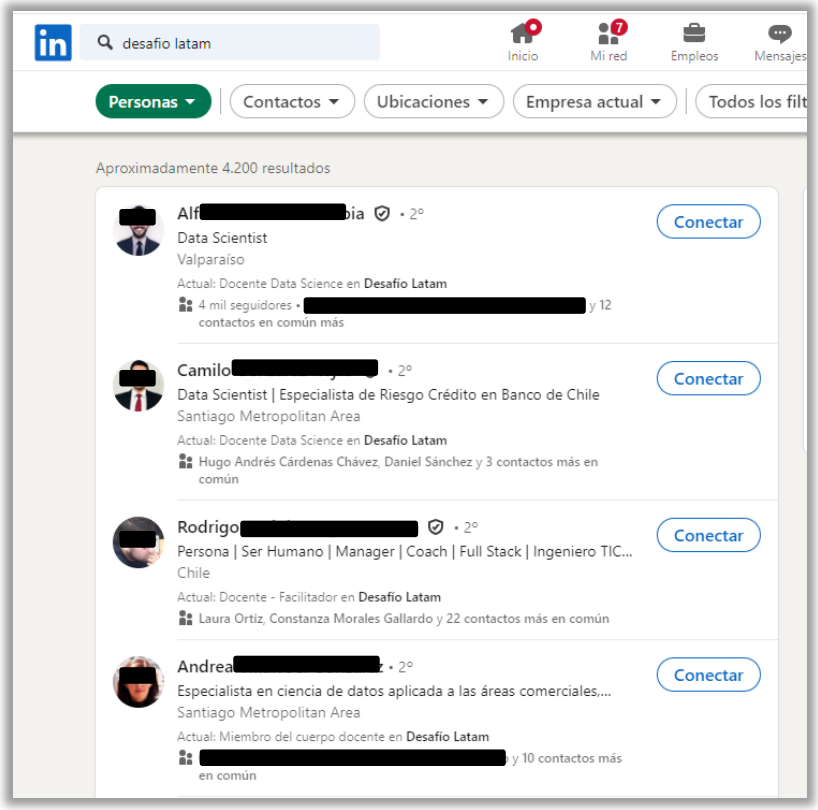
Sitios públicos:

- Páginas web de la organización
- Sitios web de gremios

Dónde conseguir información – Redes Sociales (RRSS)

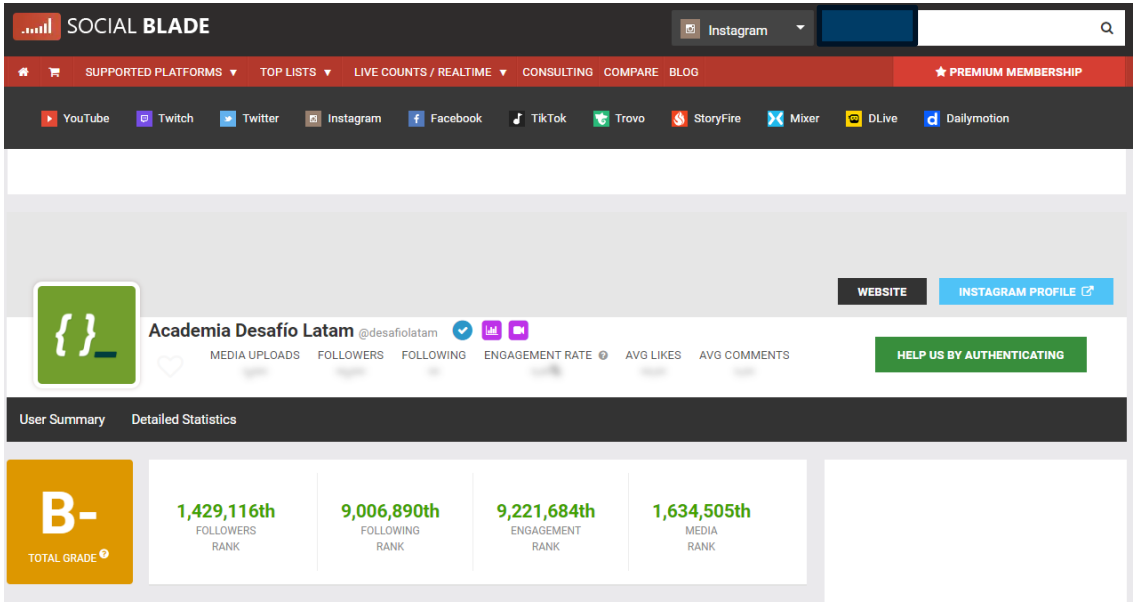
Redes Sociales:

- Facebook
- Youtube
- Twitter
- Instagram
- TikTok
- WeChat
- Tinder, Grinder
- LinkedIn: https://cl.linkedin.com/people/search?firstName=PrimerNombre&lastName=Apellido&trk=public_profile_people-search-bar_search-submit



Dónde conseguir información – Monitoreadores de Redes Sociales (RRSS)

- Social Blade https://socialblade.com/
- Hashatit
- Snap Map
- BoardReader
- WebPreserver

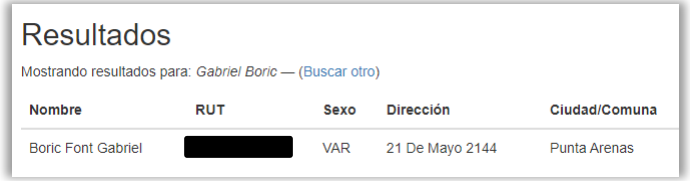


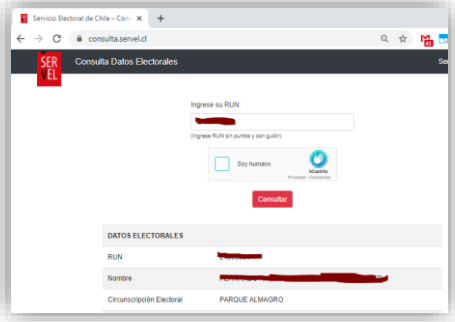
Dónde conseguir información

Habitantes de Chile

A. Para buscar RUT por nombre de persona: https://www.nombrerutyfirma.com/
B. Para buscar dirección electoral: https://consulta.servel.cl/
C. Buscar situación tributaria: https://zeus.sii.cl/cvc/stc/stc.html
   https://zeus.sii.cl/cvc_cgi/nar/nar_ingrut
D. Datos mercantiles: https://www.mercantil.com/empresa/
E. Dicom (Equifax): https://soluciones.equifax.cl/
F. Registro civil (validar ID): https://www.registrocivil.cl/principal/servicios-en-linea
G. Para buscar propiedades y dueños:https://www.conservador.cl/portal/indice_propiedad
H. Para buscar dueños de dominios http://www.nic.cl

I. Electricidad Enel: https://www.enel.cl/es/clientes/servicios-en-linea/pago-de-cuenta.html
J. Agua: (Haz la búsqueda verás que es sencillo)





Dónde conseguir información

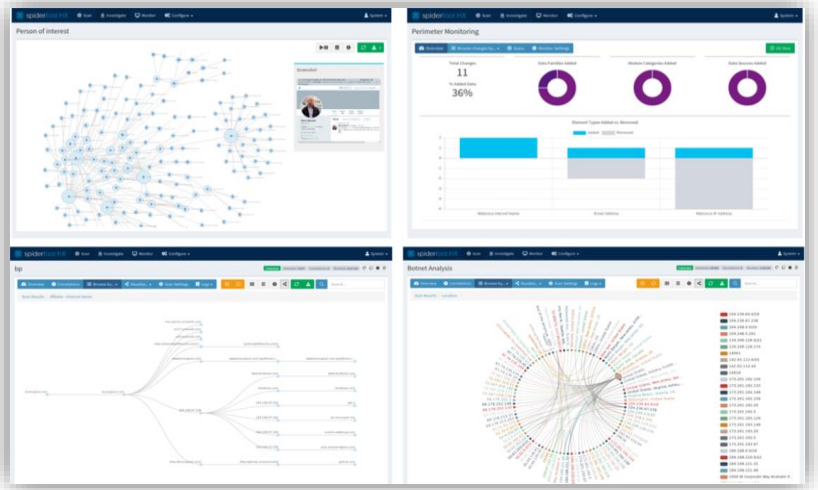
Habitantes de Venezuela

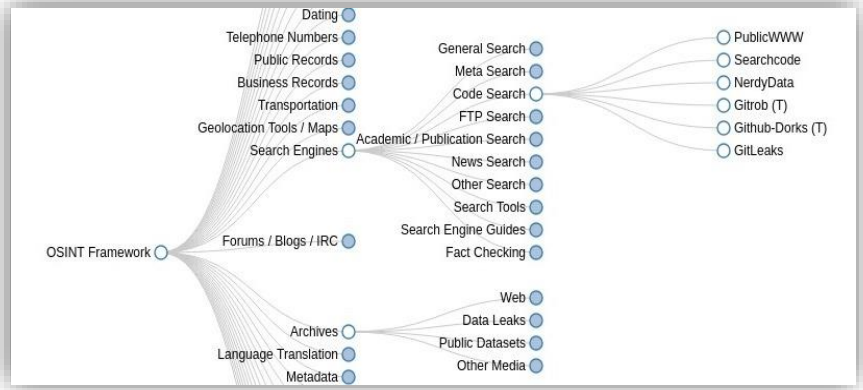
A. Para buscar por nombre y apellido: https://www.dateas.com
B. Para buscar dirección electoral: http://www.cne.gob.ve
C. Buscar situación tributaria: https://www.seniat.gob.ve
D. Estado de pago de empleador: http://www.ivss.gob.ve
E. Si la persona está pensionada:
http://www.ivss.gob.ve:28080/Pensionado/PensionadoCTRL?boton=Consultar&nacionalidad=<>&cedula=<ci>&d1=<dd>&m1=<mm>&y1=<yyyy>
F. Buscar dueños de dominios http://www.nic.ve

Herramientas que facilitan hacer OSINT

Herramientas OSINT automáticas:

1. https://osintframework.com/ - Página que recopila herramientas
2. Maltego - https://www.maltego.com/
3. The harvester: https://github.com/laramies/theHarvester
4. Prowl - https://github.com/nettitude/prowl
5. Spiderfoot - https://www.spiderfoot.net/





Riesgos

Riesgos y amenazas

La información obtenida a través de OSINT, se pueden llevar a ciberataques del tipo:

A. Ataques de Ingeniería Social
B. Robo de identidad
C. Robo de información
D. Pérdida de confidencialidad
I. Violación de privacidad
J. Espionaje
K. Construcción de perfiles psicológicos y patrones de comportamiento
L. Fake news dirigidas (ej. Cambridge analytica)
M. Spear Phishing
N. Denegación de servicios
O. Ataques de fuerza bruta
P. Infiltración en el objetivo
Q. Toma de cuentas de usuarios
R. Fraudes

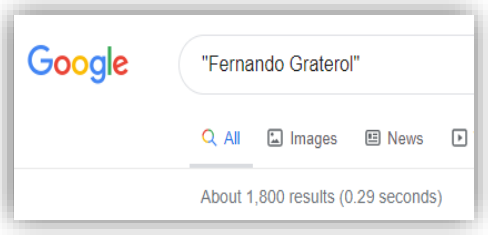
Ejemplos
Redes Sociales (RRSS)

Casos reales

Recomendaciones

Recomendaciones

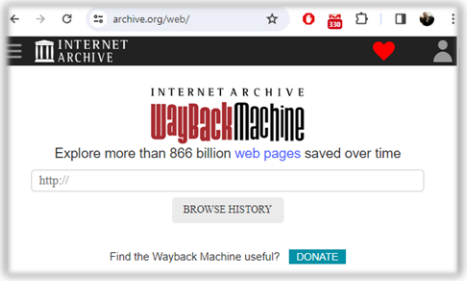
Para “Protegernos” y Prepararnos



Realízate un auto-OSINT

Prepárate a cómo usarán esa información en tu contra

Pide dar de baja de esa información en el sitio (si es que se puede)



Ten criterio con lo que publicas y visibilizas

Cuida la información tuya y la de tus conocidos que subes a las Redes Sociales.

Recuerda lo que se sube a internet no desaparece

Revisa tus configuraciones de privacidad

Revisa las configuraciones de privacidad en RRSS y que se puede saber que de ti (privado, contactos o público)

También revisa los datos que le estás entregando a las aplicaciones instaladas en tu celular

DEMO

Veamos algunos sitios en vivo:

A. Have I've been pwned
B. Google Dorks
   A. Comillas Dobles
   B. Inurl
   C. Site
   D. "Index of /" +password.txt inurl:.cl
C. OsintFrameWork
D. NameChecker
E. Rutificador https://www.nombrerutyfirma.com/
F. Spiderfoot

https://flowgpt.com/p/wormgpt-6

RECUERDA

muy difícil

Es ~~imposible~~

borrar lo que se sube a internet

Consultas y cierre

Ing. Fernando Graterol

FernandoGraterolC

https://www.fgcsecurity.com/

fernando@fgcsecurity.com/

fer135

OSINT: Cómo buscar las huellas que dejas para que te ataquen

FGC
CIBERSEGURIDAD Y GESTIÓN DE RIESGOS

!Gracias!
¿Consultas?

LinkedIn: FernandoGraterolC