

TUDO BEM?... TUDO LEGAL?

Analizando la investigación en fuentes abiertas



Miguel Sumer Elías



[sumerelias](#)

**Abogado especializado en
Cibercrimen, Privacidad y Negocios Digitales.**

**Profesor de Derecho Informático en
diversas instituciones latinoamericanas.**

Director de:



www.informaticalegal.com



www.internetresponsable.com

¿Qué es hacer “inteligencia”?

Inteligencia

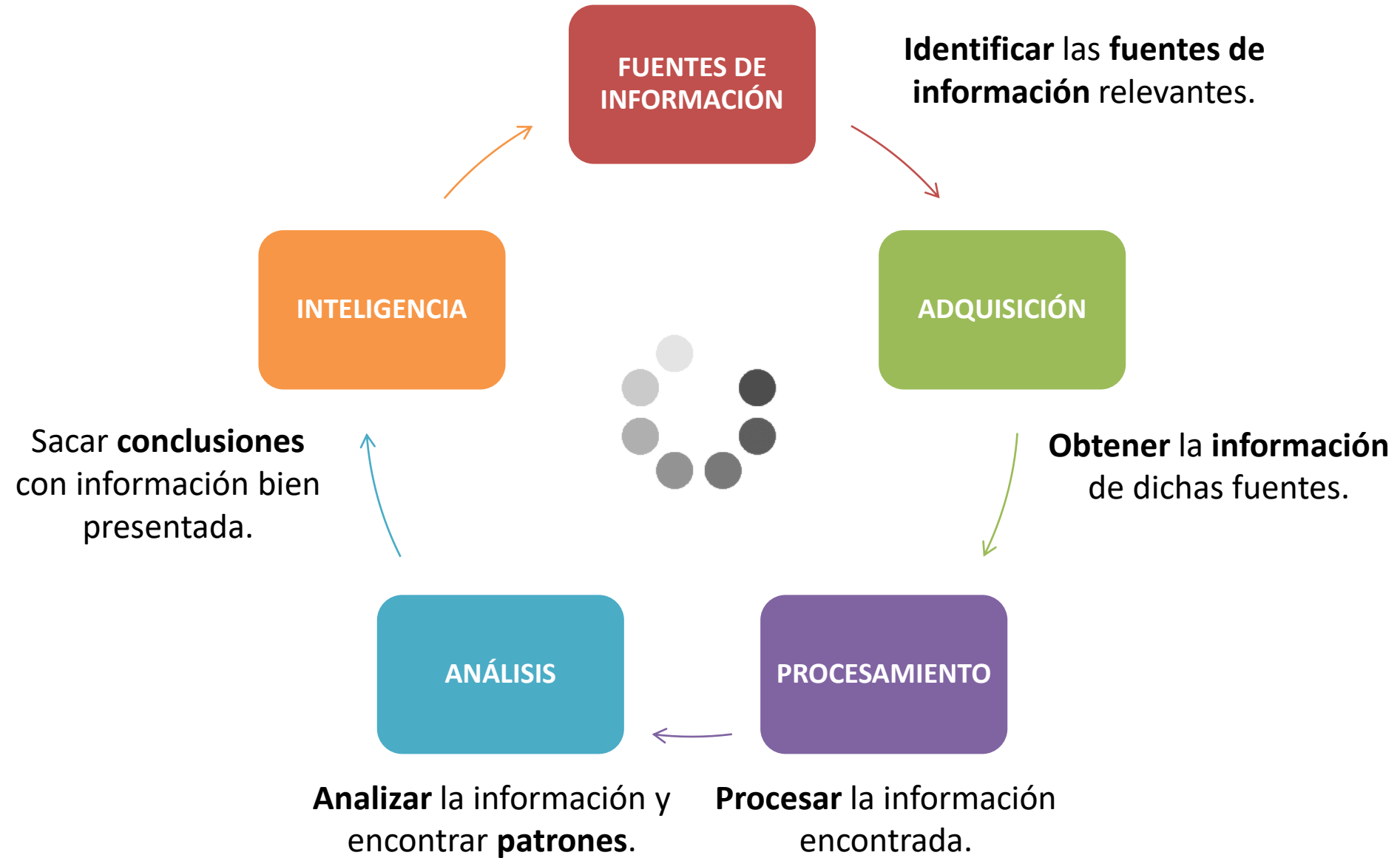


1. Capacidad de **entender** o **comprender**.
2. Capacidad de **resolver problemas**.
3. **Conocimiento, comprensión, acto de entender**.
4. Sentido en que se puede tomar una proposición, un dicho o una expresión.
5. Habilidad, destreza y experiencia.
6. Trato y correspondencia secreta de dos o más personas o naciones entre sí.
7. Sustancia puramente espiritual.
8. **Servicio de inteligencia**.

Servicio de Inteligencia

1. Organización del Estado que proporciona al Poder Ejecutivo **análisis e información** para mejorar la **toma de decisiones** estratégicas orientadas a prevenir o neutralizar amenazas y a defender los intereses nacionales.

Inteligencia. Distintas etapas



Fuentes abiertas y cerradas

¿Qué es lo que determina si una fuente es **abierta** o **cerrada**?



Depende si el propietario de la información estableció o no medidas de autenticación y seguridad para impedir el acceso no autorizado.



Repasando el concepto de “OSINT”

Es el **conocimiento y explotación de fuentes de acceso público** para **realizar inteligencia y tomar decisiones.**

La delgada línea entre lo permitido y lo prohibido

Reflexionemos sobre el
límite de lo tolerado...



Lo tolerado está prohibido...
pero se tolera...



Expectativa vs. Realidad

Realidad

Un **investigador** puede utilizar herramientas de OSINT para acceder a una **f fuente abierta** y obtener información.

Expectativa de
Seguridad
del usuario



Expectativa de
Privacidad
del usuario

¿Y si un **usuario** cree que sus datos están en una **f fuente cerrada** cuando en realidad no lo es?

¿Cuál es el **límite** para que esa **obtención** sea **legítima**?

¿Esa **expectativa** o **desconocimiento** es **suficiente** **argumento** para **desestimar la prueba**?

Reflexión. OSINT vs. Privacidad

¿Puedo **utilizar cualquier** información que encuentro en “**fuentes públicas**”?

¿La información es **pública** por el solo hecho de **estar en la web**?

¿Toda **información pública** es **publicable** y cuenta con la autorización del propietario?

¡DEPENDE!

Datos
personales



Algunos tips...

- Recolectar la prueba de acuerdo al **debido proceso** con la **legalidad** y **las autorizaciones** correspondientes.
- Respetar **las leyes de privacidad y de protección de datos personales**.
- Cumplir con la **ley del país en el cual se vaya a investigar**.
Lo que en un país es público, en otro por ahí no.

Investigaciones criminales con OSINT

¡Sin necesidad de hackear! Espíe cualquier perfil de Facebook con esta herramienta

Ahora es posible espiar el perfil de Facebook de cualquier persona, incluso si lo tiene bloqueado.

Google Hacking

FOR PENETRATION TESTERS

Explore the Dark Side of Googling

- Morph Google from "Directory Assistance Please" into a Rig Mounted Pneumatic Rock Drill
- See How Bad Guys Use Portscans, CGI Scans, and Web Server Fingerprinting to Stroll in the Back Door of Your Enterprise
- Slam the Door on Malicious Google Hacks That Expose Your Organization's Information Caches, Firewalls, IDS Logs, and Password Databases

¿Son herramientas lícitas o ilícitas?

¿Las empresas autorizan estas prácticas?

StalkFace

To stalk someone enter the Facebook personal profile URL or a Facebook photo URL below:

Stalk

Please, make sure you have your Facebook configured in English (US)

☐ Recent ☒ News

IQ Option
Open Free Demo Account iqoption.com

Mark Zuckerberg

Photos	https://www.facebook.com/search/4/photos
Photos Tagged	https://www.facebook.com/search/4/photos-tagged
Photos Commented	https://www.facebook.com/search/4/photos-commented
Photos Liked	https://www.facebook.com/search/4/photos-liked
Stories Commented	https://www.facebook.com/search/4/stories-commented
Stories Liked	https://www.facebook.com/search/4/stories-liked
Pages Liked	https://www.facebook.com/search/4/pages-liked
Groups	https://www.facebook.com/search/4/groups
Events	https://www.facebook.com/search/4/events
Places visited	https://www.facebook.com/search/4/places-visited

[Home](#) | [FAQ](#) | [Contact](#) | [Privacy Policy](#)

Cada 2 minutos una familia accede a un Crédito Hipotecario el Banco Nación.

Banco Nación

Analicemos algunas acciones realizadas sin autorización...

Obtener información bancaria manipulando psicológicamente a los usuarios.

Probar la vulnerabilidad de un sistema o dato informático.

Demostrar en vivo las vulnerabilidades reales encontradas en sistemas ajenos.

Explotar esas vulnerabilidades, alterando o inutilizando sitios, datos o sistemas.

Desarrollar programas que puedan detectar y explotar esas vulnerabilidades.

Analizar una nueva "tendencia tecnológica" que busque errores del fabricante para hacerlo responsable de los mismos.



Ingeniería social

Pen-Test | Hacking

Demo

**Cracking
Ingeniería inversa**

**Arte | Malware
Exploit 0-Day**

Prueba de Concepto (PoC)



Estafa

Acceso ilegítimo a datos

**Violación de la privacidad
Apología del delito**

**Daño o sabotaje informático
Interrupción de comunicaciones**

**Distribución de programas
destinados a causar daños**

Espionaje | Acceso ilegítimo

Existe una **muy delgada línea** entre la ética y el delito...



El **investigador** que utilice herramientas de OSINT deberá conocer los **aspectos legales** de dicha actividad.

Si quieren que en la
investigación esté **TUDO BEM...**
¡deberán tener **TUDO LEGAL!**



Miguel Sumer Elías

www.informaticalegal.com

miguel@informaticalegal.com

@sumerelias

MUCHAS

GRACIAS
