

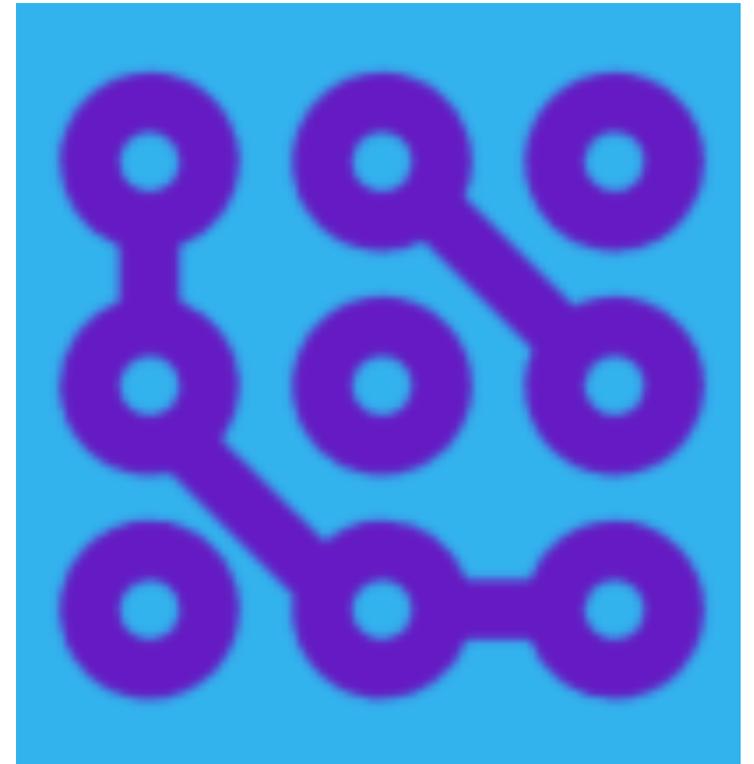


**INTELIGENCIA**  
MÁS LIDERAZGO

OSINTCITY 2019 SEVILLA  
26 Y 27 DE ABRIL DE 2019

# LAS TÉCNICAS DE ANÁLISIS EN OSINT

JOSÉ MANUEL DÍAZ-CANEJA GRECIANO



[jmdiazcaneja@inteligenciayliderazgo.com](mailto:jmdiazcaneja@inteligenciayliderazgo.com)



[www.linkedin.com/in/jose-manuel-diaz-caneja](http://www.linkedin.com/in/jose-manuel-diaz-caneja)



[@JDiaz\\_Caneja](https://twitter.com/JDiaz_Caneja)



## Así se propagó 'Wannacry' por el mundo

■ Países alectados



Fuente: Elaboración propia

Á. Matilla / EL MUNDO GRÁFICOS





Lo que sorprenda no nos debe apartar del camino; nos debe exigir una reflexión y un esfuerzo de imaginación.



¡La anticipación es la clave del éxito!



LOS PARAGUAS HAY QUE COMPRARLOS CUANDO NO LLUEVE. CUANDO EMPIEZA A CAER AGUA SON CAROS Y PROBABLEMENTE TE HABRÁS MOJADO

JACOBO ZARCO

[www.economipedia.com](http://www.economipedia.com)





INTELIGENCIA  
MÁS LIDERAZGO

ANALYSIS  
DRIVEN

DIRIGIDO  
POR EL  
ANÁLISIS

PROACTIVO

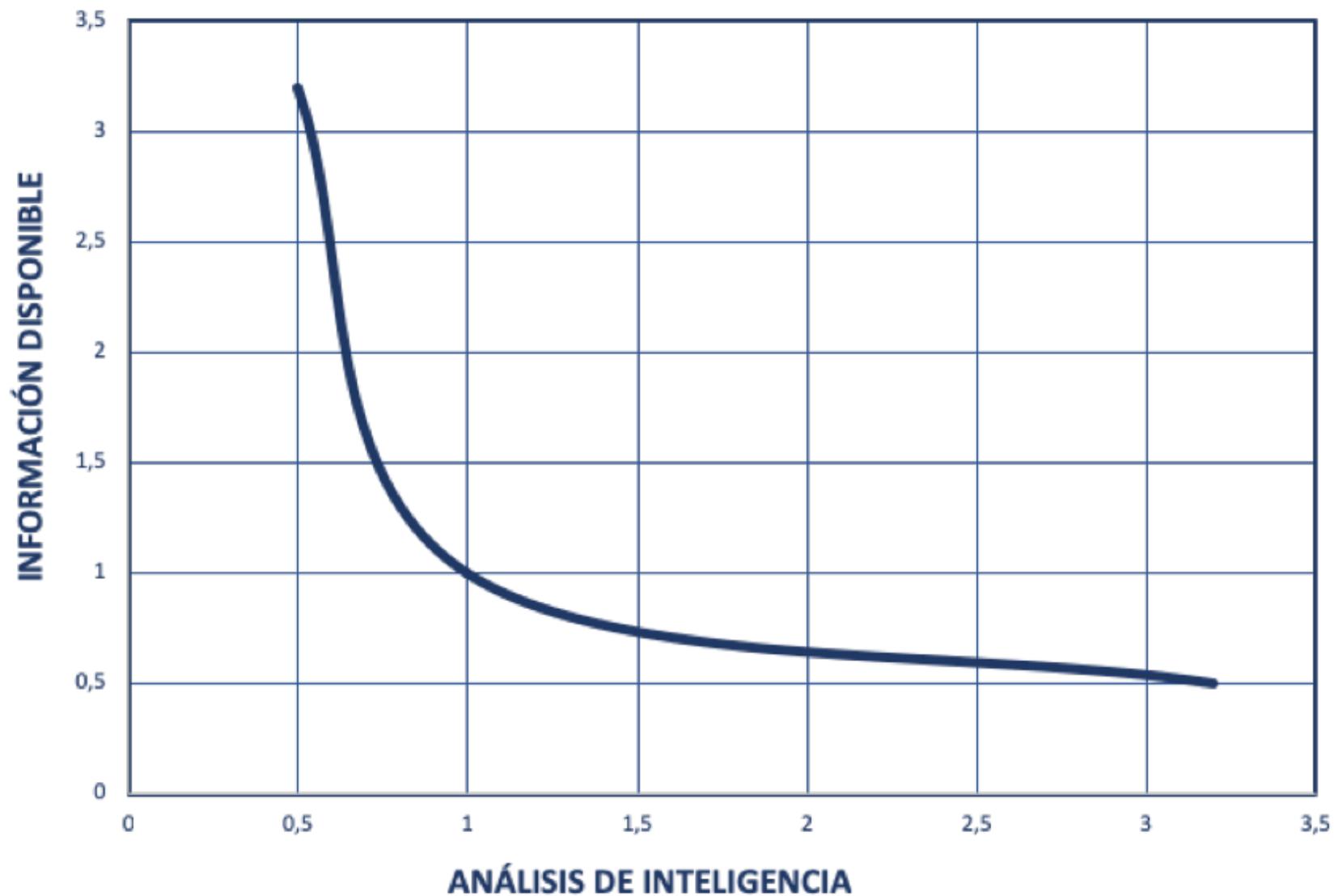
# Procesos de Inteligencia



COLLECTION  
DRIVEN

DIRIGIDO  
POR LA  
OBTENCIÓN

REACTIVO





“Information and Intelligence”  
is the “Fire and Maneuver” of the 21st Century.

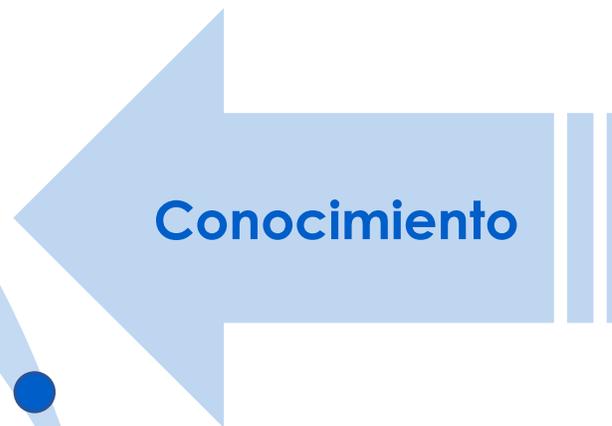
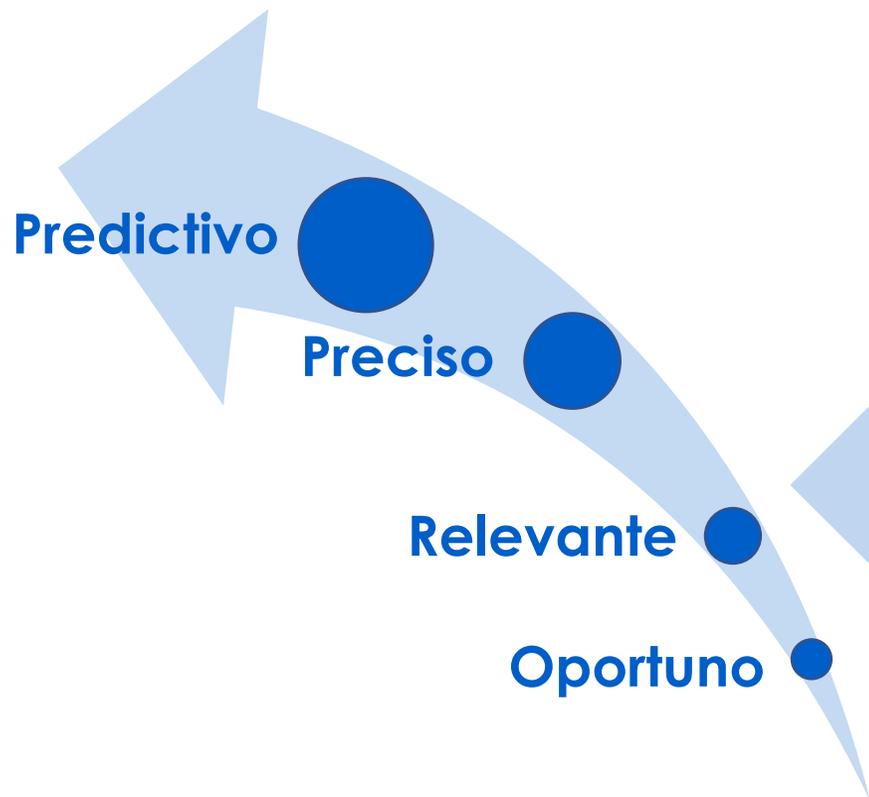
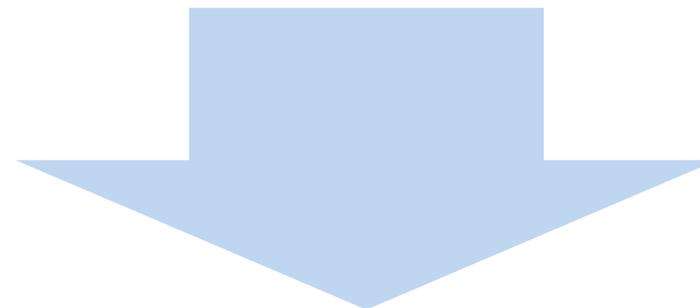
-Major General Michael Flynn, March 2011.



**Inteligencia**



**Conocimiento**





# Introducción

Inteligencia

Comprende el conjunto de actividades

Encaminadas a

Satisfacer las necesidades de conocimiento del Jefe

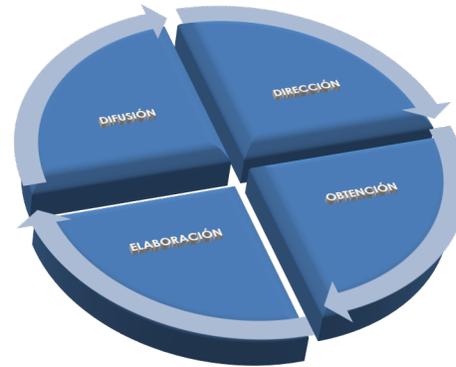
Relativas al

Identificación  
Amenazas/Oportunidades

Planeamiento

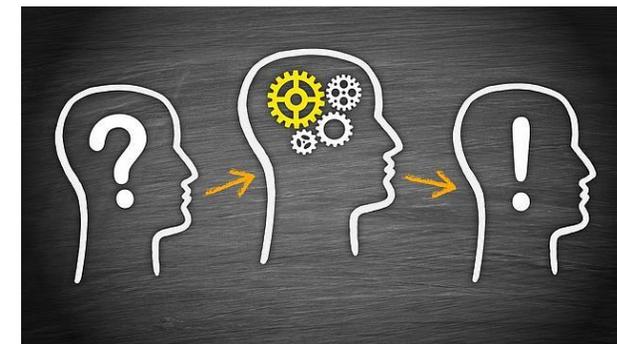
Conducción Ops.

Apoyar Toma Decisiones



Necesarias para

Entorno Operativo y Enemigo Competidor



- COMPILACIÓN
- EVALUACIÓN
- ANÁLISIS
- INTEGRACIÓN
- INTERPRETACIÓN

**Análisis**

Variables Actores

Factores internos: D (Definición), F (Factores), A (Análisis), O (Oportunidades)

Factores externos: personas, barreras

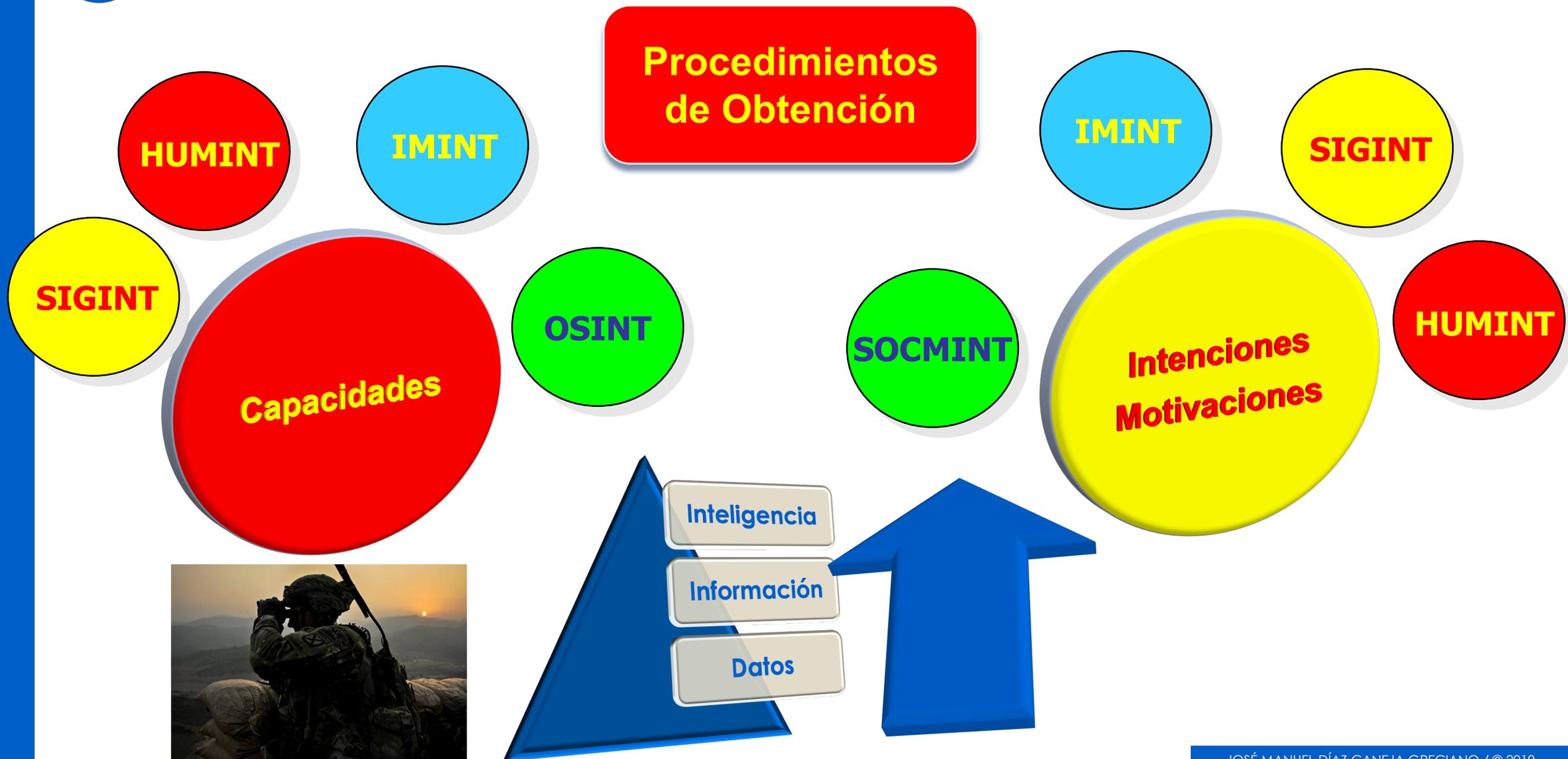
**Escenarios de Futuro**

WORST CASE → BEST CASE

**Variables Clave**

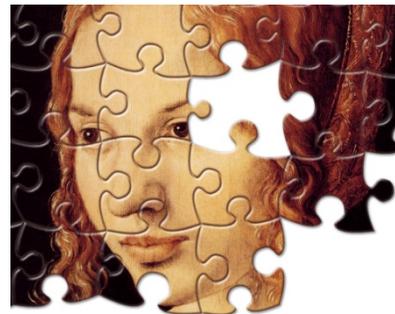
Variable	Valor	Impacto
1. Disponibilidad de recursos	Alto	Positivo
2. Disponibilidad de talento humano	Medio	Neutro
3. Disponibilidad de tecnología	Bajo	Negativo
4. Disponibilidad de capital humano	Alto	Positivo
5. Disponibilidad de infraestructura	Medio	Neutro
6. Disponibilidad de redes de distribución	Bajo	Negativo
7. Disponibilidad de canales de distribución	Alto	Positivo
8. Disponibilidad de canales de distribución	Medio	Neutro
9. Disponibilidad de canales de distribución	Bajo	Negativo
10. Disponibilidad de canales de distribución	Alto	Positivo
11. Disponibilidad de canales de distribución	Medio	Neutro
12. Disponibilidad de canales de distribución	Bajo	Negativo
13. Disponibilidad de canales de distribución	Alto	Positivo
14. Disponibilidad de canales de distribución	Medio	Neutro
15. Disponibilidad de canales de distribución	Bajo	Negativo



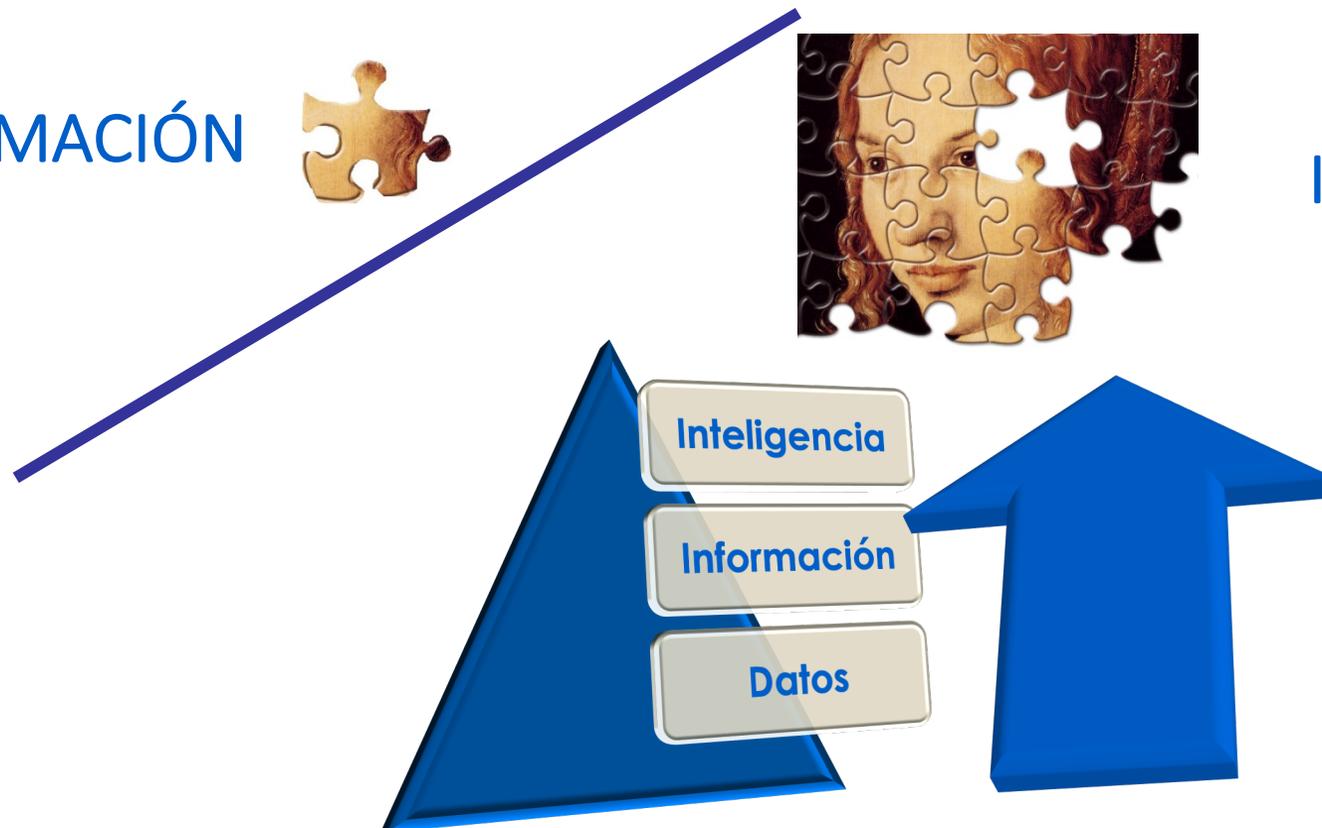


# Información Vs Inteligencia

INFORMACIÓN



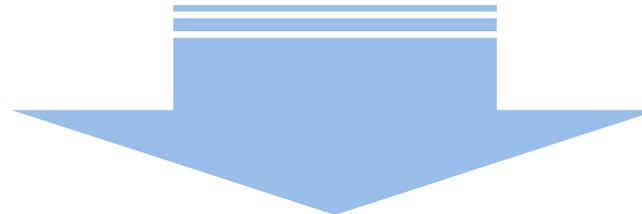
INTELIGENCIA



**INFORMACIÓN + ELABORACIÓN = INTELIGENCIA**



## Fases de la Obtención



Explotación de Fuentes

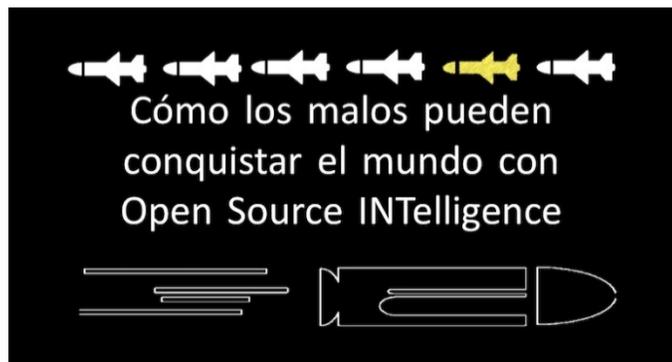
Transformación Información

Entrega Información



**Disciplinas de Obtención**

## OSINT (Inteligencia de Fuentes Abiertas)

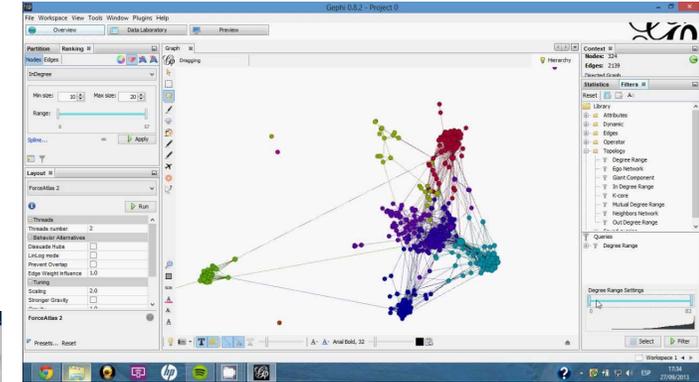
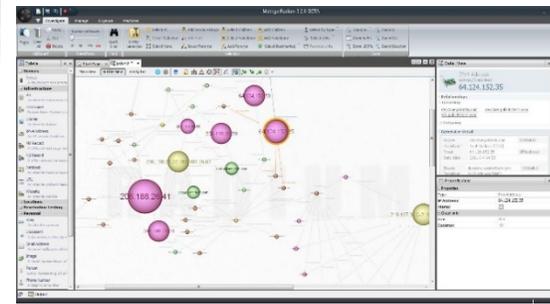
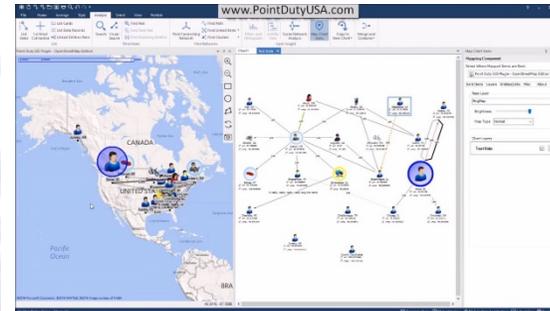


### OSINT INTEL REPORT

NAME:	Mr Brooks	
HOME PHONE:	1918	
MOBILE PHONE:	8031	
ADDRESS:	Custom Kitchens Inc., PRESTON, HG22 7NS	
EMAIL:	car@...@btinternet.com	
G.O.B.:	1918	
SOCIAL MEDIA:		
FACEBOOK ACCOUNT:	<a href="https://www.facebook.com/...">https://www.facebook.com/...</a>	
TWITTER ACCOUNT:	<a href="https://twitter.com/...">https://twitter.com/...</a>	
LINKEDIN ACCOUNT:	<a href="https://www.linkedin.com/in/...">https://www.linkedin.com/in/...</a>	
INSTAGRAM ACCOUNT:		
FAMILY:		
DAUGHTER:	Brooks	
MOTHER:	Brooks	
WIFE:	Brooks	
SON:	Brooks	
COMPANY:		
COMPANY NAME:		
COMPANY ADDRESS:	Travellers Tower, Millgate Road, W17 2EF	
COMPANY PHONE:	072	
WEBSITE:	<a href="http://www.fox.com/">http://www.fox.com/</a>	
DIRECTORS:	Fisher and Ains, Benjamin and Michael	
COMPANY NEWS:	<a href="http://www.bbc.co.uk/news">http://www.bbc.co.uk/news</a>	
ADDITIONAL INFORMATION:		
	Mr Brooks has shown to have a physically violent and verbally abusive tendencies.	

- Fuentes abiertas: Acceso público (no siempre son gratuitas)
- Tipos: MCS (video, radio, prensa)  
Publicaciones especializadas  
Redes de comunicación social  
Blogs, etc...

## OSINT- SOCMINT Software vs Mente

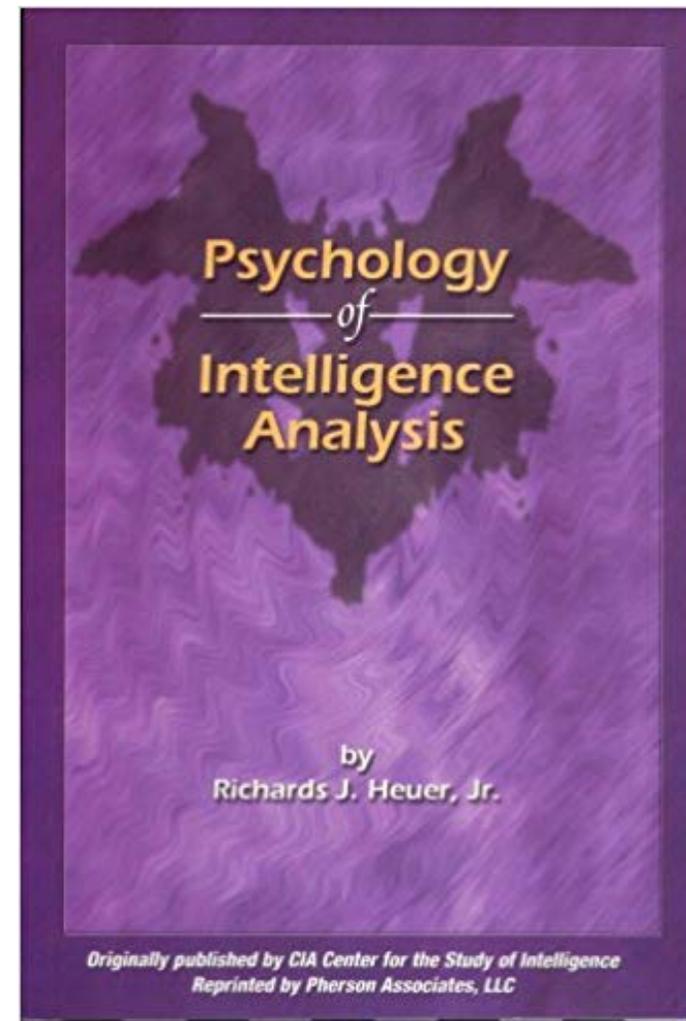


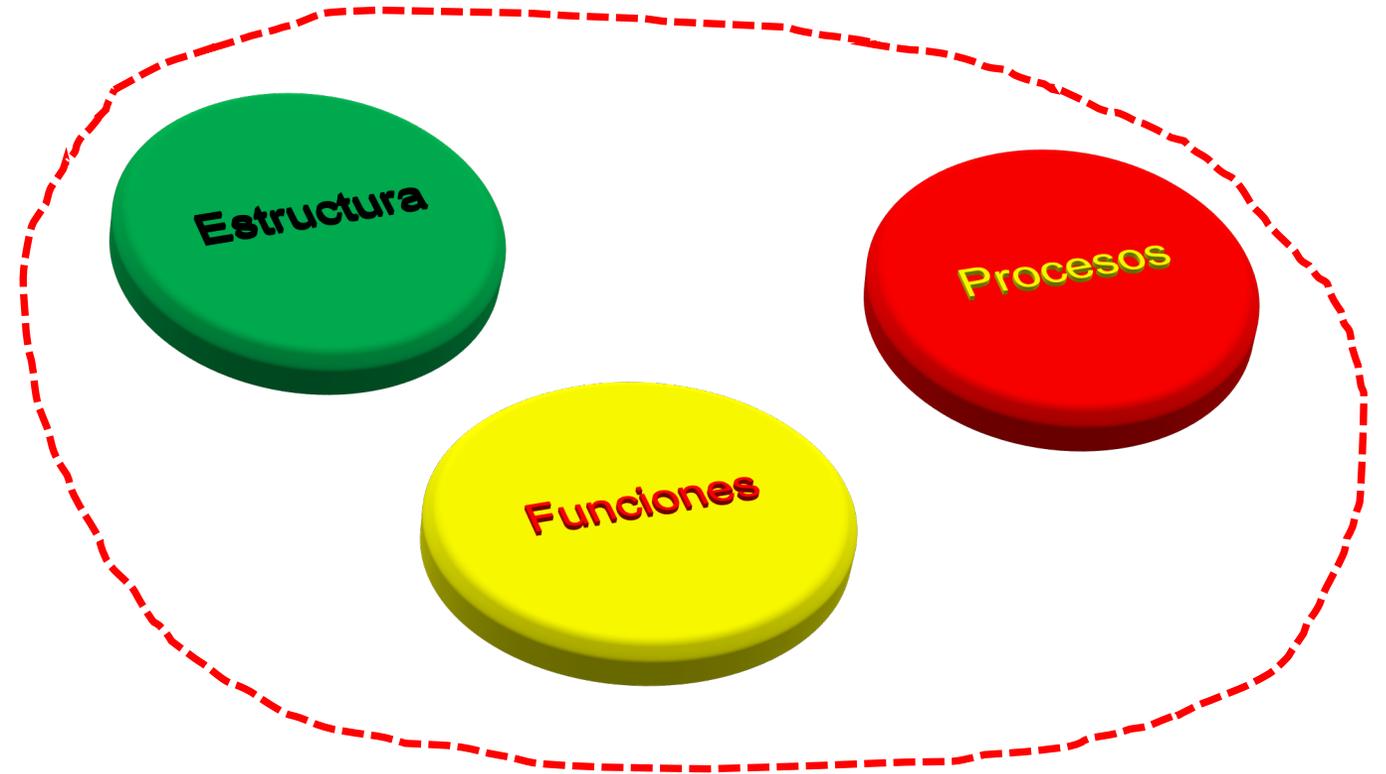
Los analistas de Inteligencia deberían ser conscientes de su proceso de razonamiento.

Deberían pensar en cómo hacen los juicios y llegan a conclusiones, no sólo en los propios juicios y conclusiones.

*Richards J. Heuer, Jr.*

*Psychology of Intelligence Analysis (1999)*





## Elementos Fundamentales de una Red

### Cómo son

*Relaciones y Nodos de Red*

*Cuáles son los Nodos*

*Dónde están los Nodos*

*Cómo son las Relaciones*

*Cómo es la Estructura  
General de la Red*

**ESTRUCTURA**

### Qué hacen

*Relativo a Acciones,  
Personal y Recursos*

*Valor de sus Acciones  
para el conjunto de la Red*

*Cómo le afecta un  
Problema de Funcionamiento*

**FUNCIONES**

### Por Qué y Cómo operan

*Por qué se establecieron  
las Relaciones*

*Qué Beneficios Comunes  
obtienen los Nodos*

*Quién Manda*

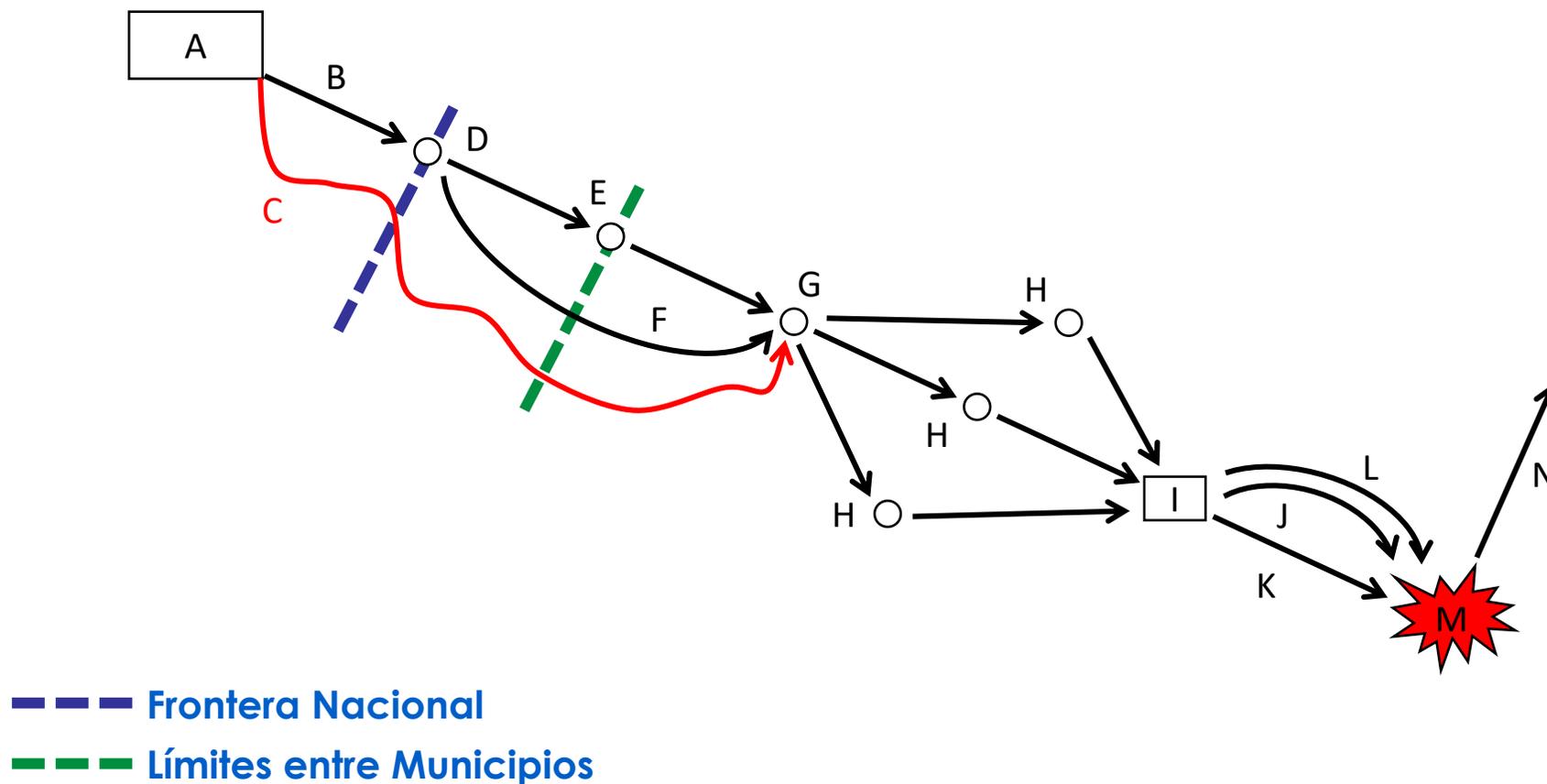
*Quién Coordina  
las Acciones*

*Cómo se toman Decisiones*

**PROCESOS**

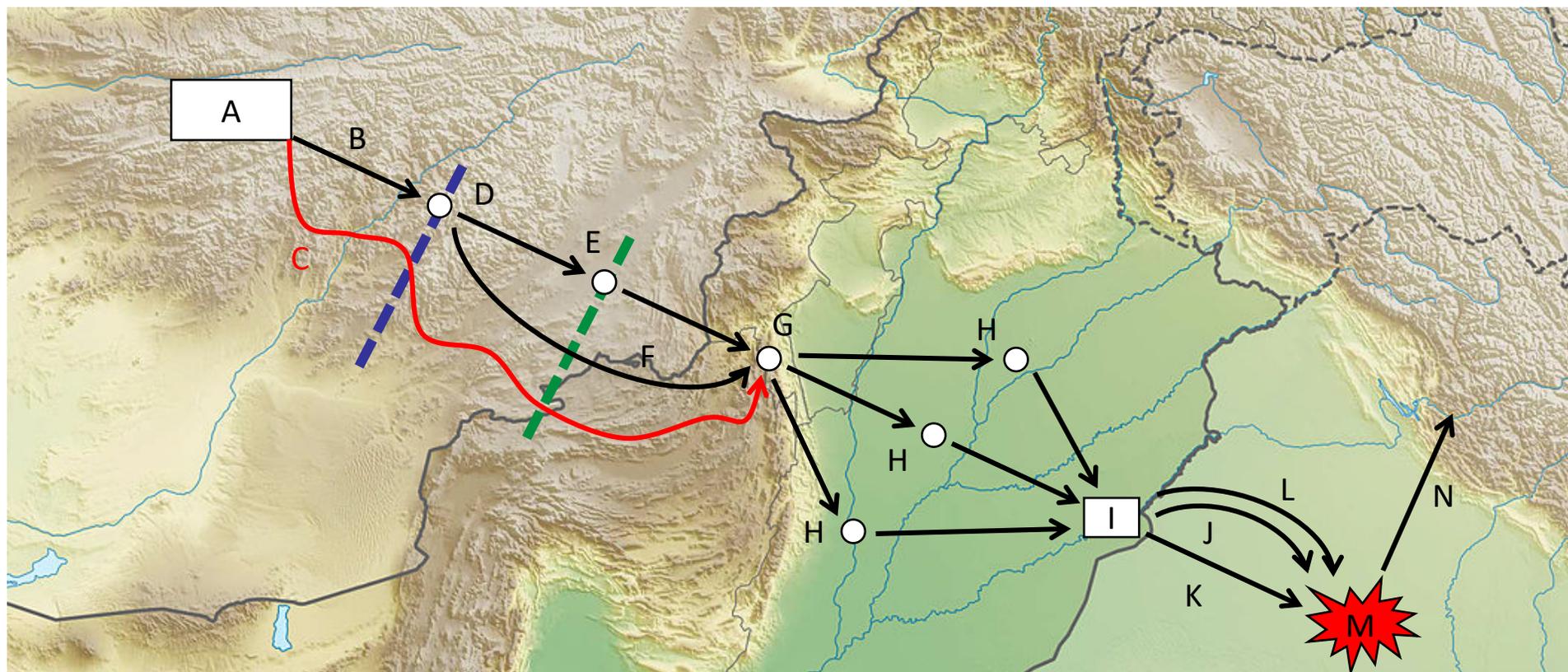
## Modelo de Red Tareas /Actividades

### Patrones de Red & Secuencia de Actividades



## Modelo de Red Tareas /Actividades

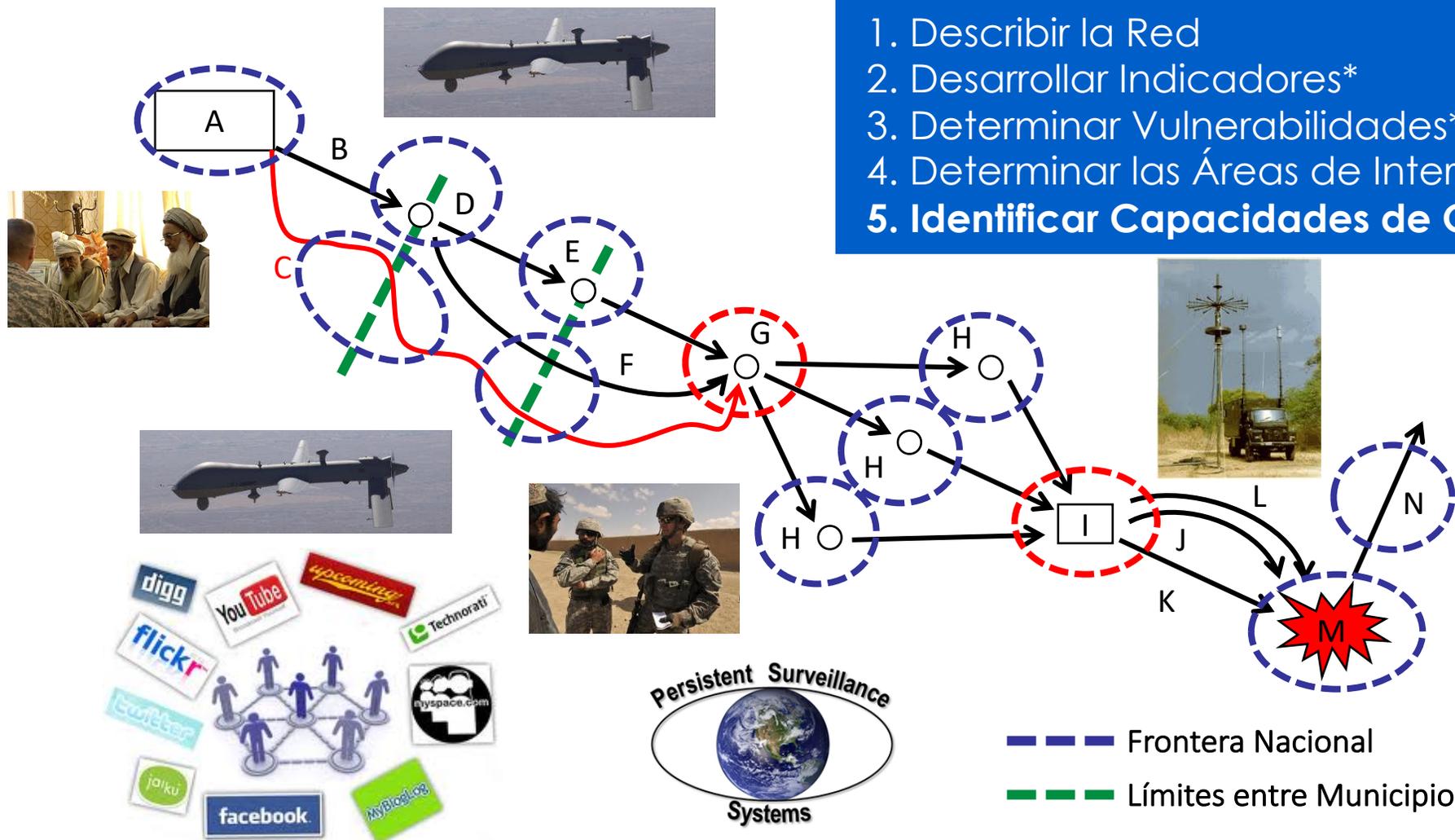
*Patrones de Red & Secuencia de Actividades*

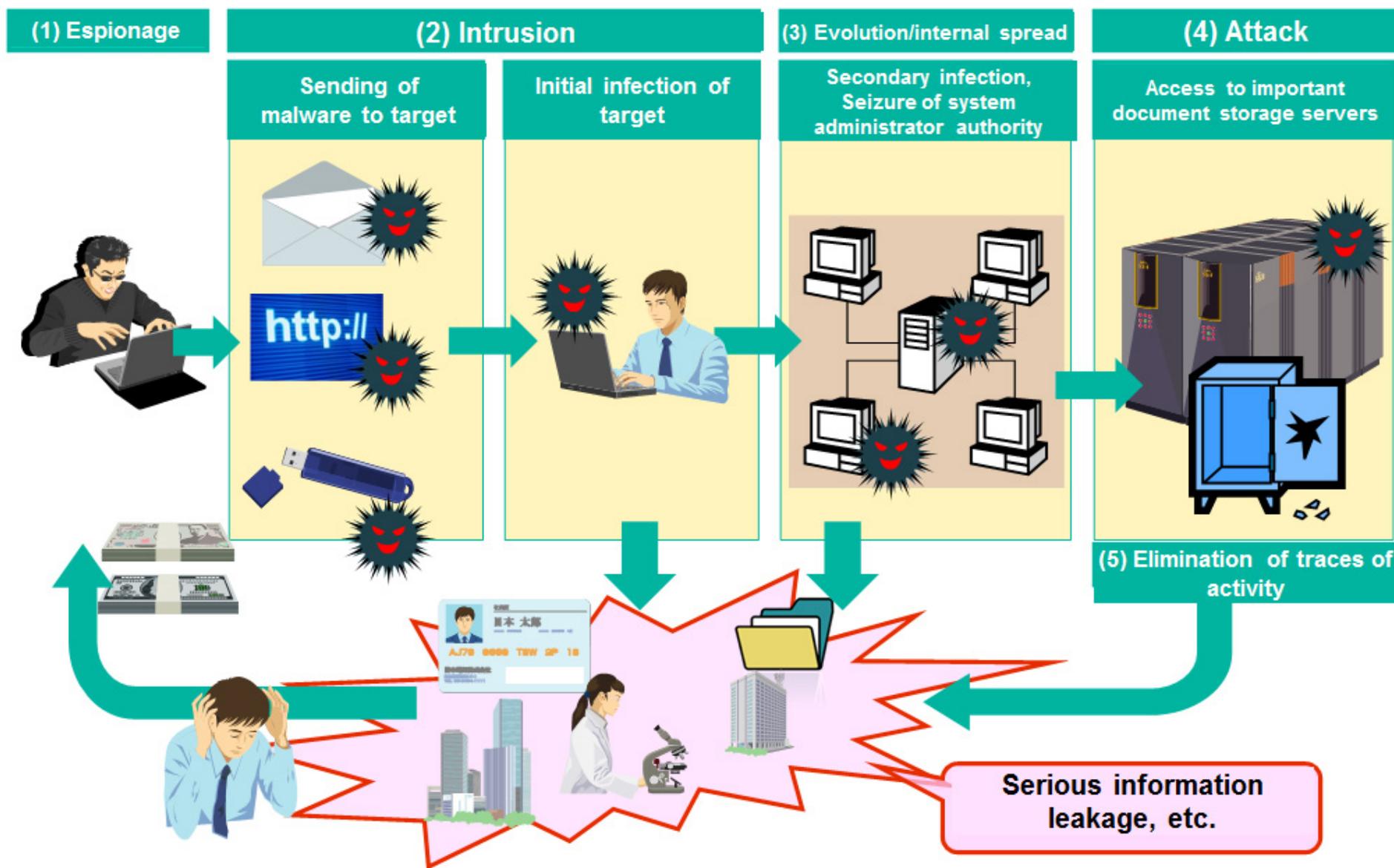


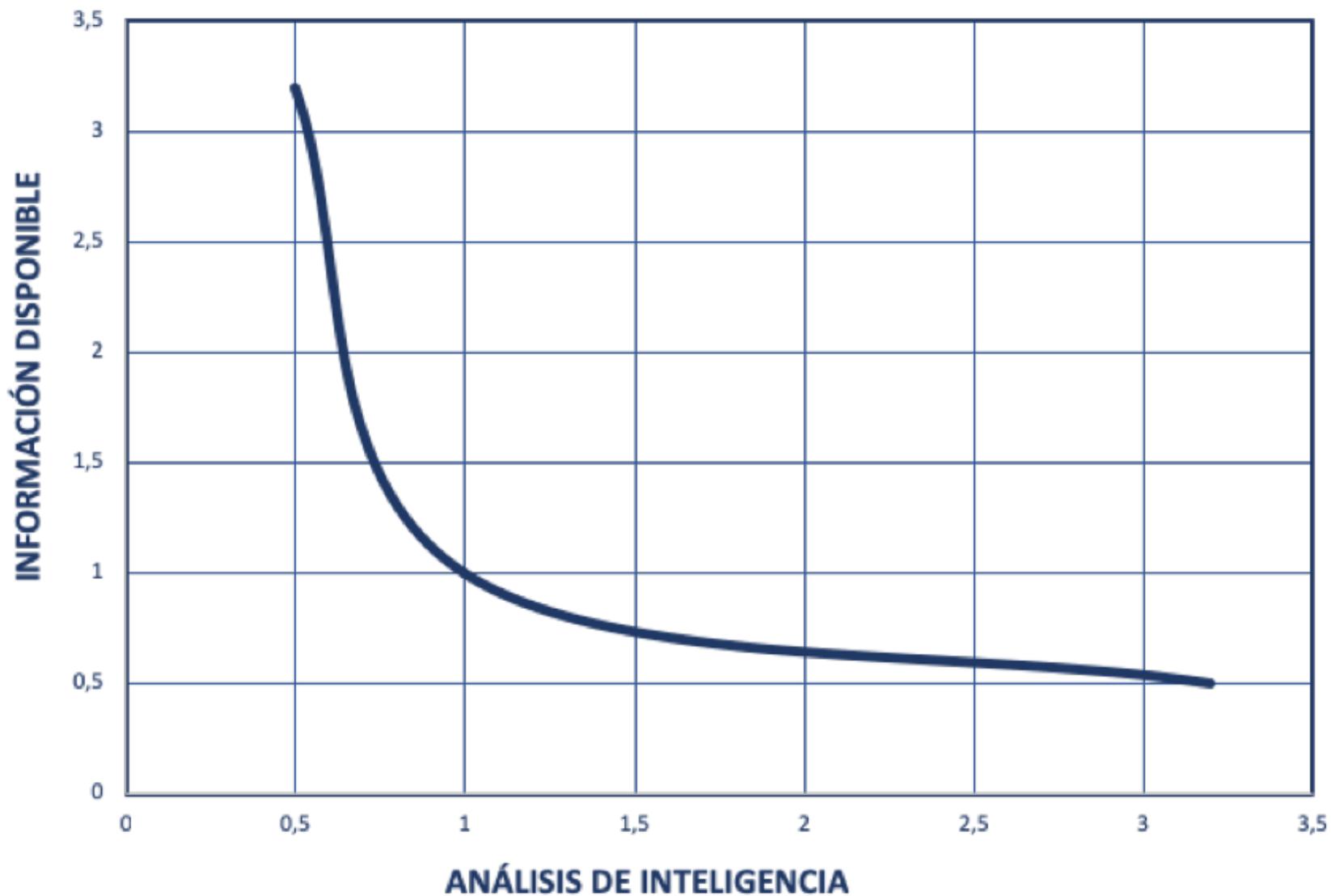
- — Frontera Nacional
- — Límites entre Municipios

## Proceso de elaboración del modelo de actividades & tareas de una red

1. Describir la Red
2. Desarrollar Indicadores\*
3. Determinar Vulnerabilidades\*
4. Determinar las Áreas de Interés
5. **Identificar Capacidades de Obtención**









# Generación de Hipótesis Basadas en Eventos Pasados

04-03-2018- Envenenamiento del antiguo oficial del GRU, Serguei Skripal y su hija Yulia en Salisbury



Ante esta imagen ¿Qué hipótesis pueden ser generadas inmediatamente?



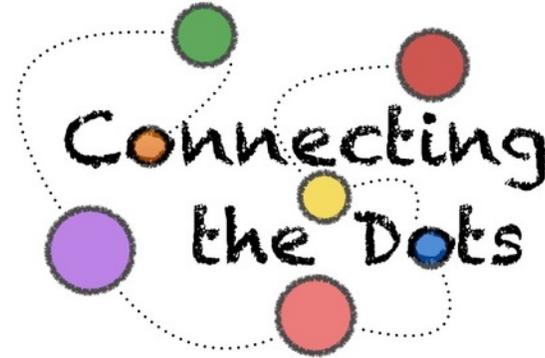
Colonel Chepiga

Imagine que nuestra hipótesis supone que las dos personas que aparecen en la cámara de vigilancia fueron los que envenenaron a Skripal y su hija.

Hasta el momento, los datos sugieren que estuvieron en las proximidades antes del envenenamiento.



*Si nuestra hipótesis es válida, ¿que otras clase de evidencias podemos esperar encontrar?*



**Hipótesis**

Los dos hombres son agentes rusos

**Supuestos**

Los pasaportes eran casi consecutivos. Emisión 2009.

Es muy improbable que los obtuvieran por los cauces normales

Reservaron vuelos de vuelta dos días consecutivos el 3 y el 4 de marzo

Improbable que fueran turistas

МЕЛКО УТЕХИНСКИ	353 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 24:08	ИПРЕД.0
МЕЛКО УТЕХИНСКИ	353 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:20	ЛОУЧЕВ(0)
МЕЛКО УТЕХИНСКИ	353 15-23 03 2009 01	3288-01	03 03 2009 24:00	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:00	МЕЛКОУТЕХИНСКИ(0)
МЕЛКО УТЕХИНСКИ	353 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:00	ОМПИТЕ.МЕЛКОУТЕХИНСКИ(0)
ВОИНИЦА ИГОРЬ	354 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 24:08	ИПРЕД.0
ВОИНИЦА ИГОРЬ	354 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:20	ЛОУЧЕВ(0)
ВОИНИЦА ИГОРЬ	354 15-23 03 2009 01	3288-01	03 03 2009 24:00	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:00	МЕЛКОУТЕХИНСКИ(0)
ВОИНИЦА ИГОРЬ	354 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:00	МЕЛКОУТЕХИНСКИ(0)
ВОИНИЦА ИГОРЬ	354 15-23 03 2009 01	3288-01	03 03 2009 23:42	ПРЕДПРИЯТИЕ ИНОСРЕДСТВАМИ ГОСУДАРСТВЕННОЙ	03 03 2009 23:00	ОМПИТЕ.МЕЛКОУТЕХИНСКИ(0)

**Evidencias**

Grabación de dos hombres caminando uno al lado del otro

Los dos hombres abandonaron el país a las pocas horas del envenenamiento

## Hipótesis Explicatorias      Probabilidad de las Hipótesis

¿Qué hipótesis podrían explicar estas observaciones?

¿Qué evidencia apoya cada hipótesis?

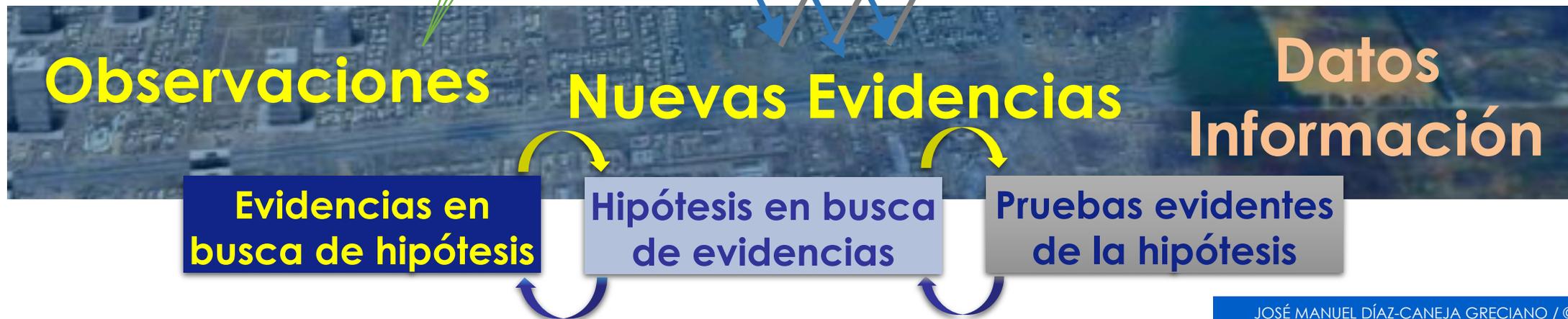
¿Cual es la probabilidad basada en las evidencias de cada hipótesis?



Data-driven

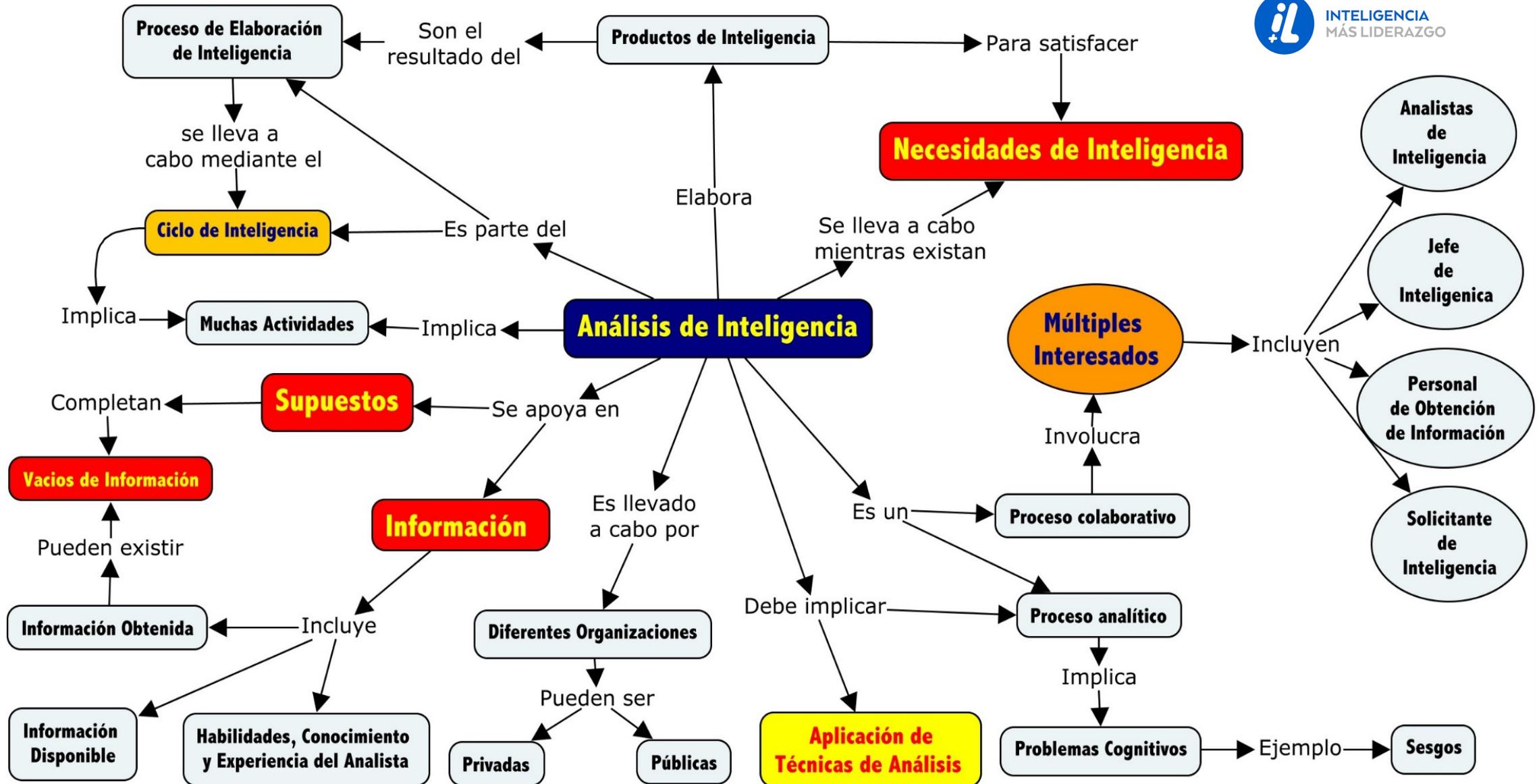


Hypothesis-driven













# ¿Qué es una técnica de análisis estructurado?

JUICIO DE  
EXPERTO

Proceso de razonamiento individual basado en el estudio de evidencias, historia, casos y analogías.

**ANÁLISIS  
ESTRUCTURADO**

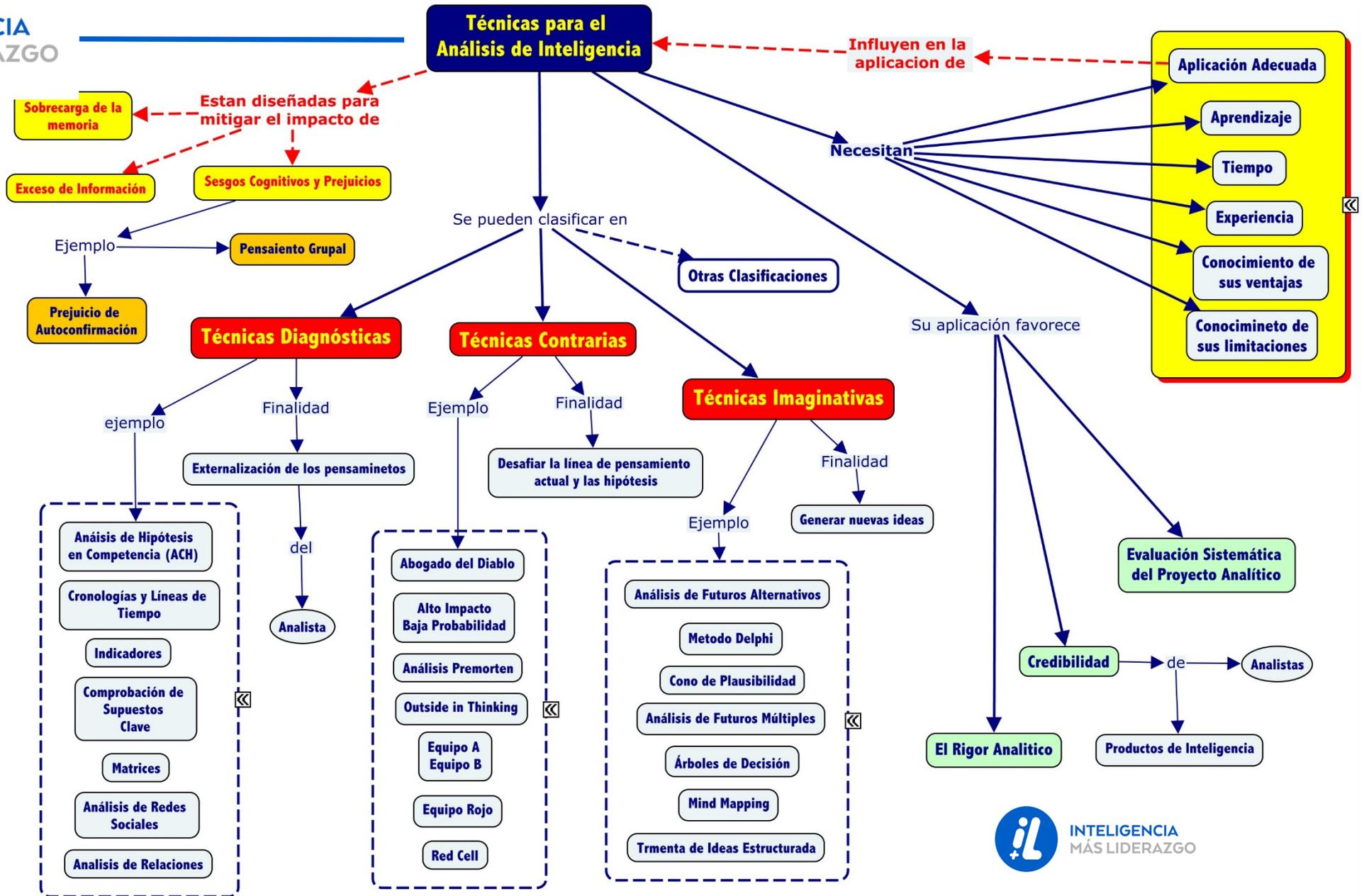
Proceso de análisis por pasos que permite externalizar el pensamiento del analista, su revisión y discusión.

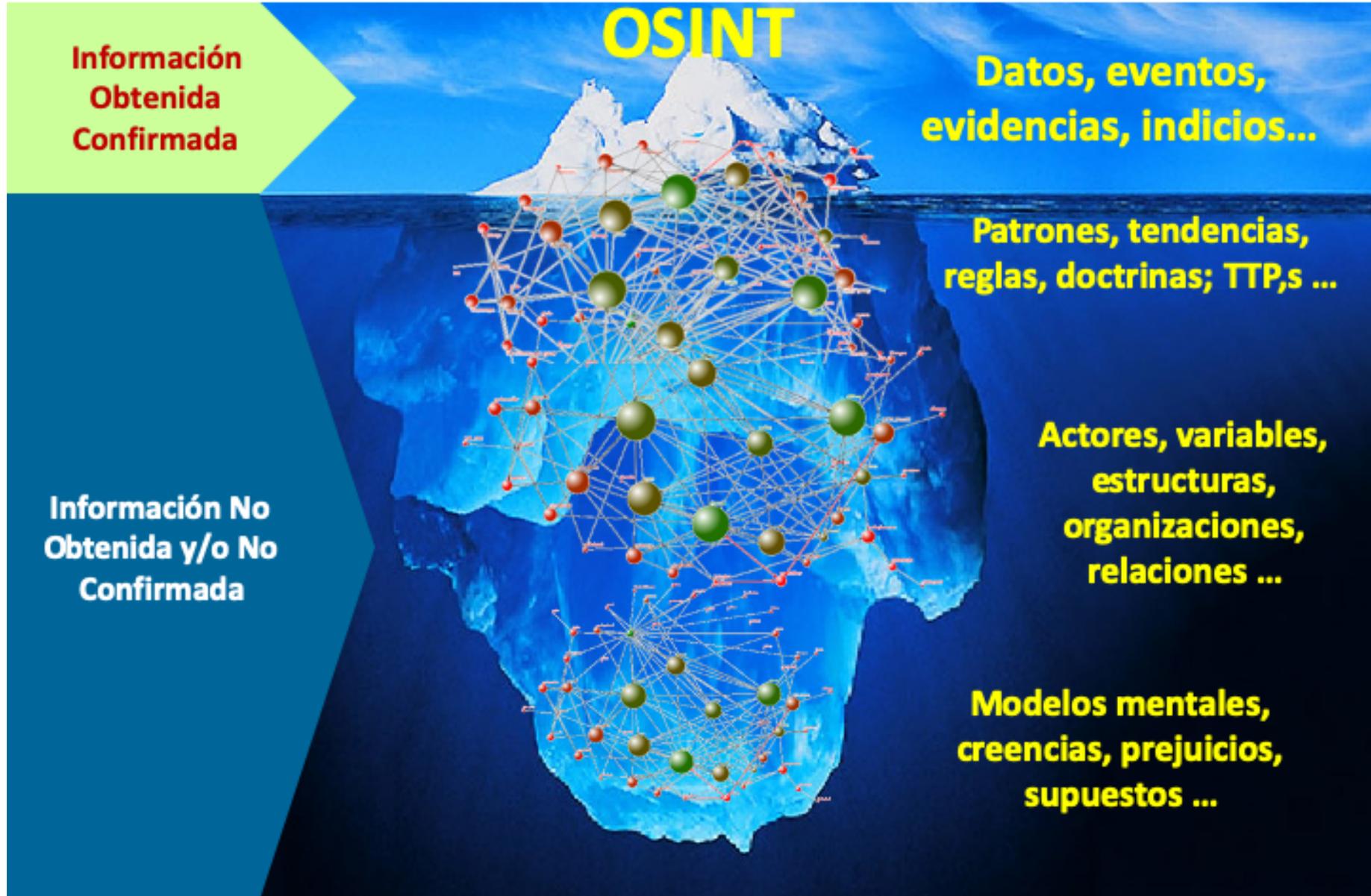
MÉTODOS  
CUANTITATIVOS  
USANDO DATOS  
GENERADOS  
POR EXPERTOS

Proceso de razonamiento basado en datos generados por expertos o métodos de simulación cuando no se dispone de datos empíricos.

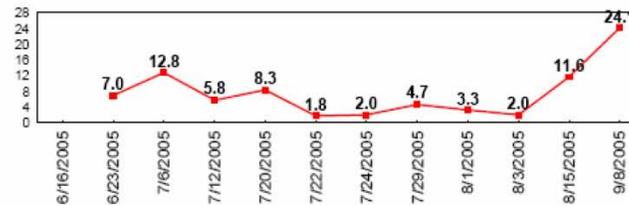
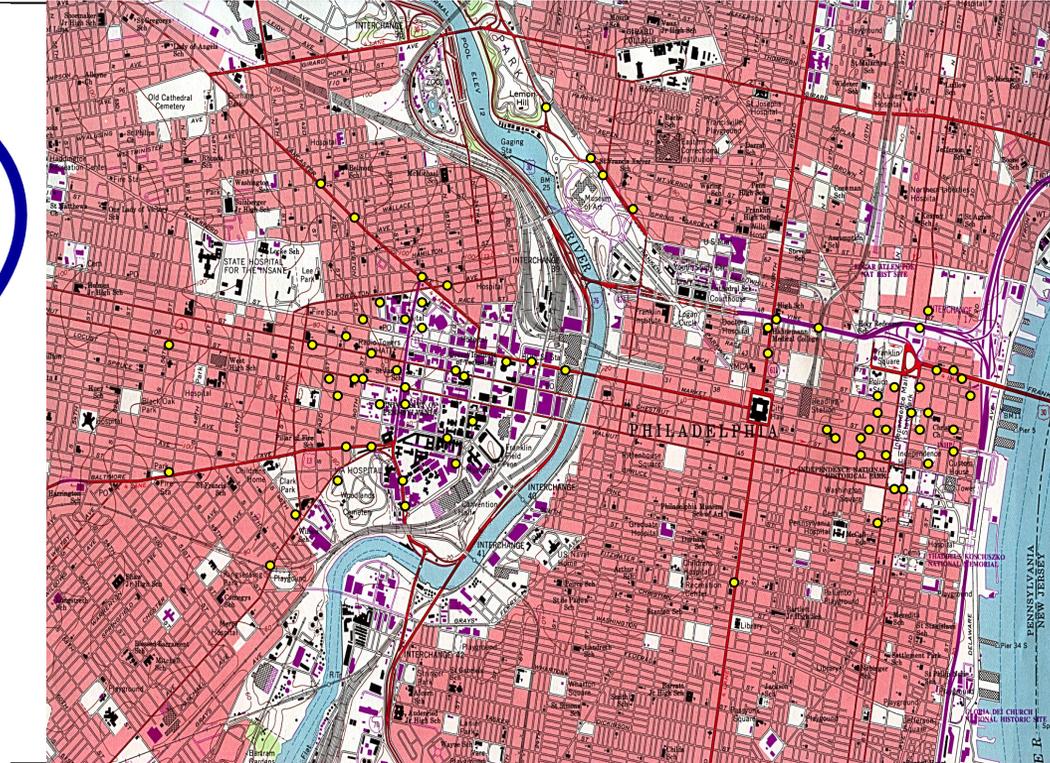
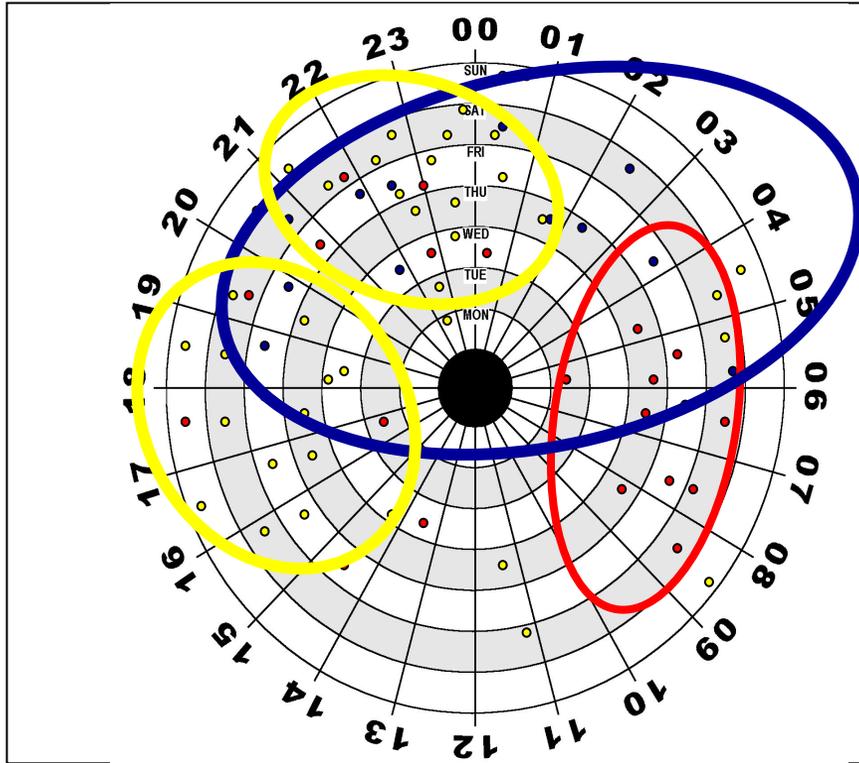
MÉTODOS  
CUANTITATIVOS  
USANDO DATOS  
GENERADOS  
POR EXPERTOS

Proceso de razonamiento basado en datos empíricos.



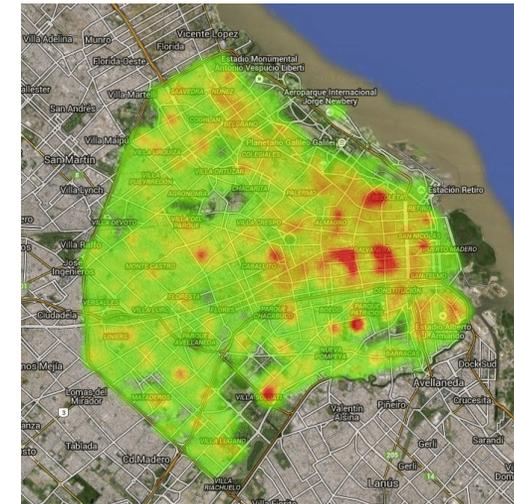
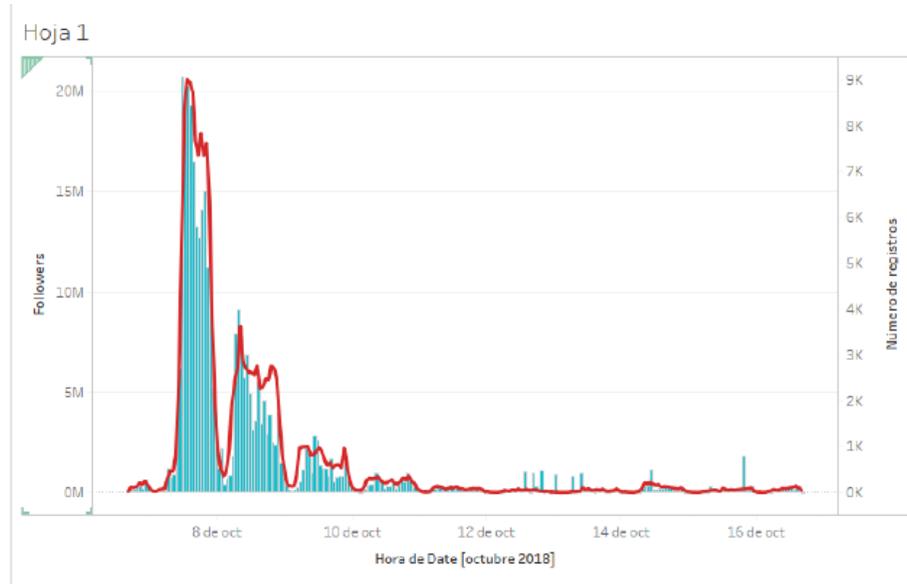


## PATRONES / RUTINAS Representación visual de datos

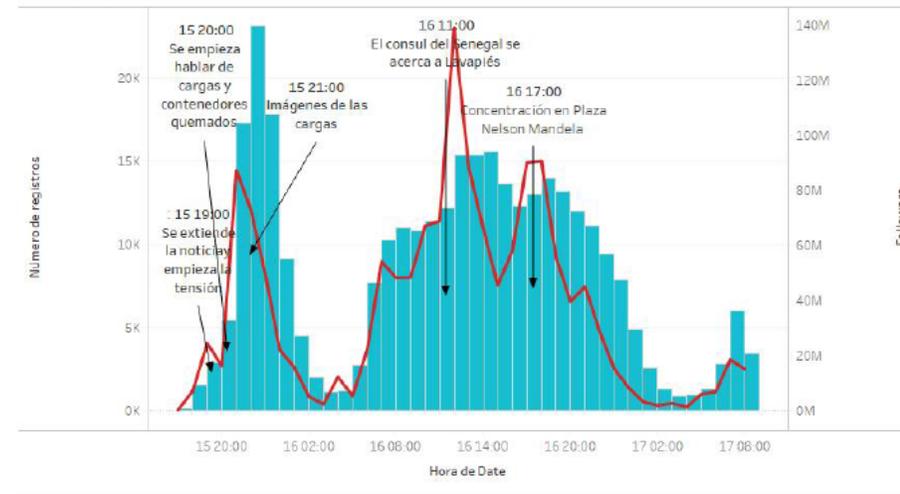
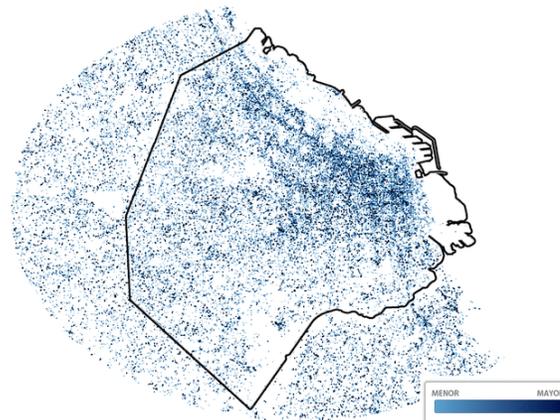




## ANÁLISIS DE INTERVALOS



### Hechos destacables



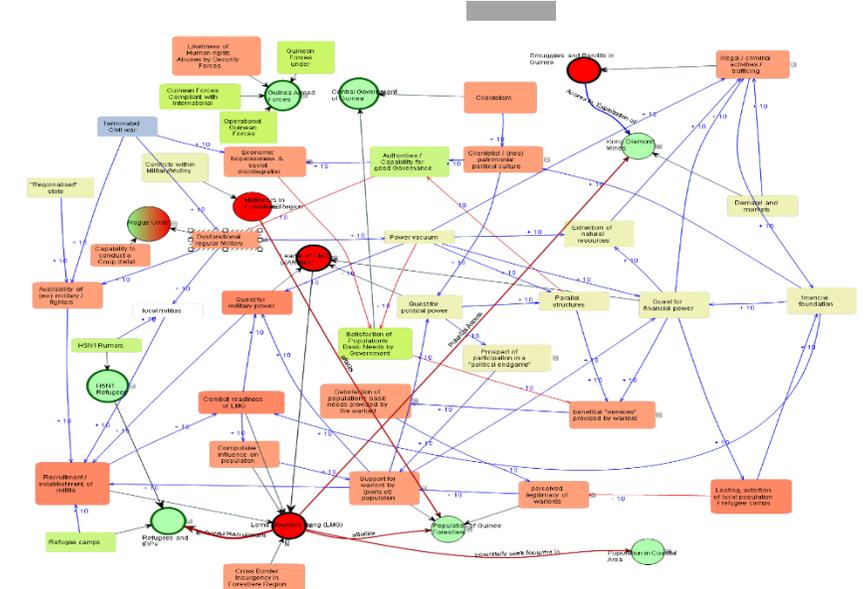
## ACH

Classification	H	Type	Credibility	Relevance	H. 1	H. 2	H. 3	P
Project Title:								
Available Matrices:								
EB Evidence Notes:								
	E6	Assumption that failure to retaliate would be unacceptable loss of face for Saddam.	Analyst Assumption	MEDIUM	MEDIUM	I	C	C
	E5	Iraqi ambassadors instructed to take increased security precautions.	COMINT	MEDIUM	MEDIUM	I	C	C
	E4	Increase in frequency/length of monitored Iraqi agent radio broadcasts.	COMINT	MEDIUM	MEDIUM	I	C	C
	E3	Assumption that Iraq would not want to provoke another US attack.	Analyst Assumption	MEDIUM	MEDIUM	C	C	I
	E2	Absence of terrorist offensive during the 1991 Gulf War.	Absence of Evidence	MEDIUM	MEDIUM	C	C	I
	E1	Saddam public statement of intent not to retaliate.	Leadership Statement	MEDIUM	MEDIUM	C	C	C

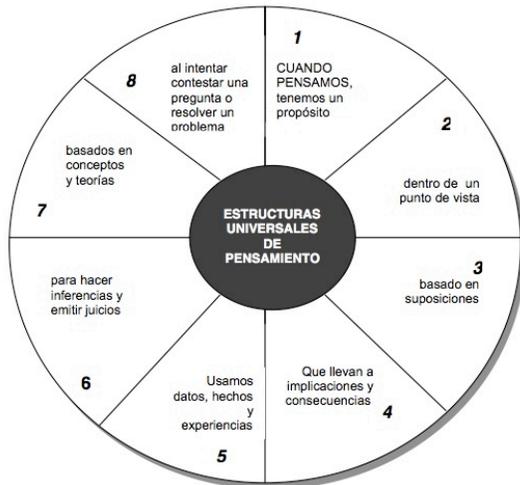
## SWOT/DAFO



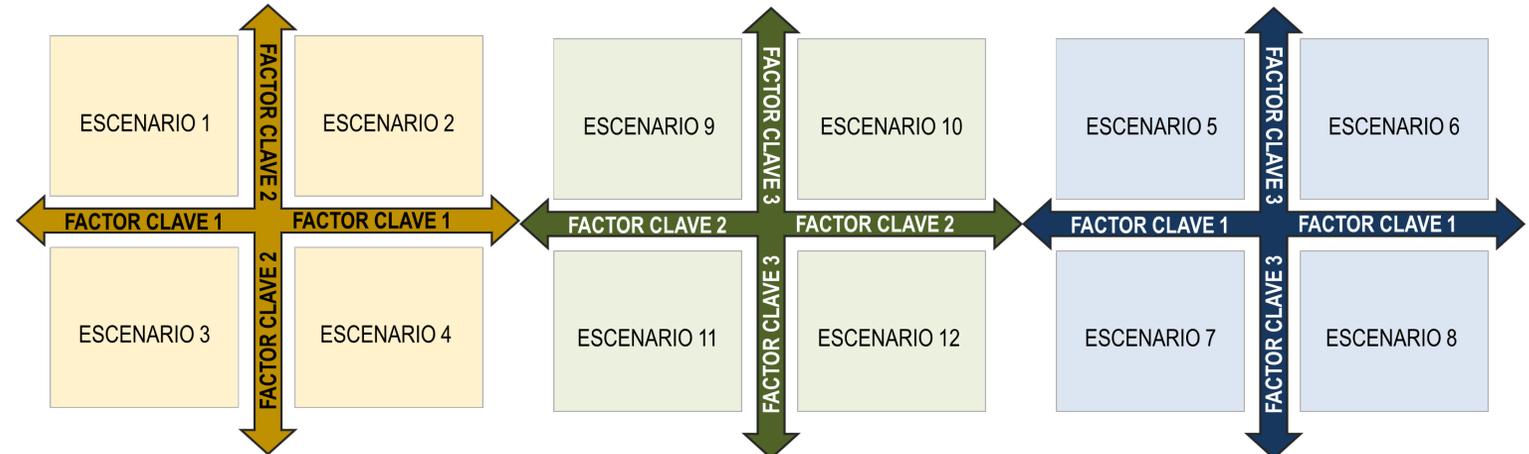
## Diagramas de Influencia



## Pensamiento Crítico

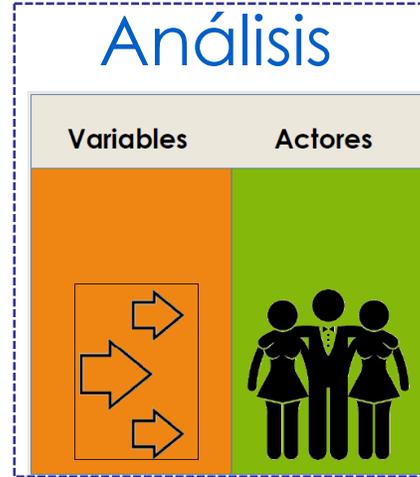
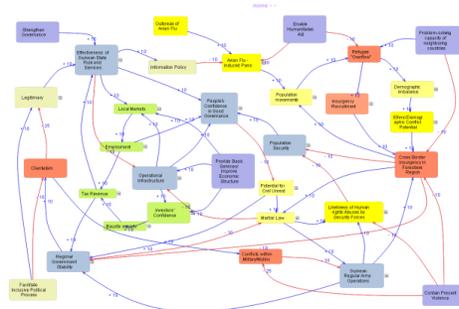


## Escenarios e Indicadores





# Procesos de Análisis ¿Dónde estamos?

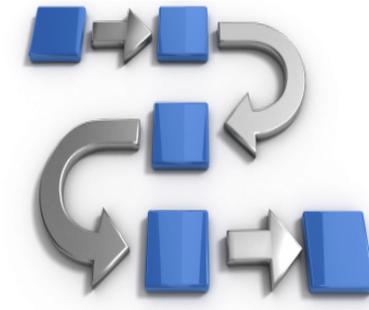
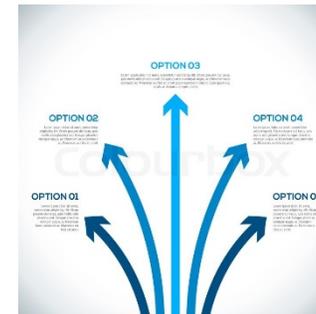


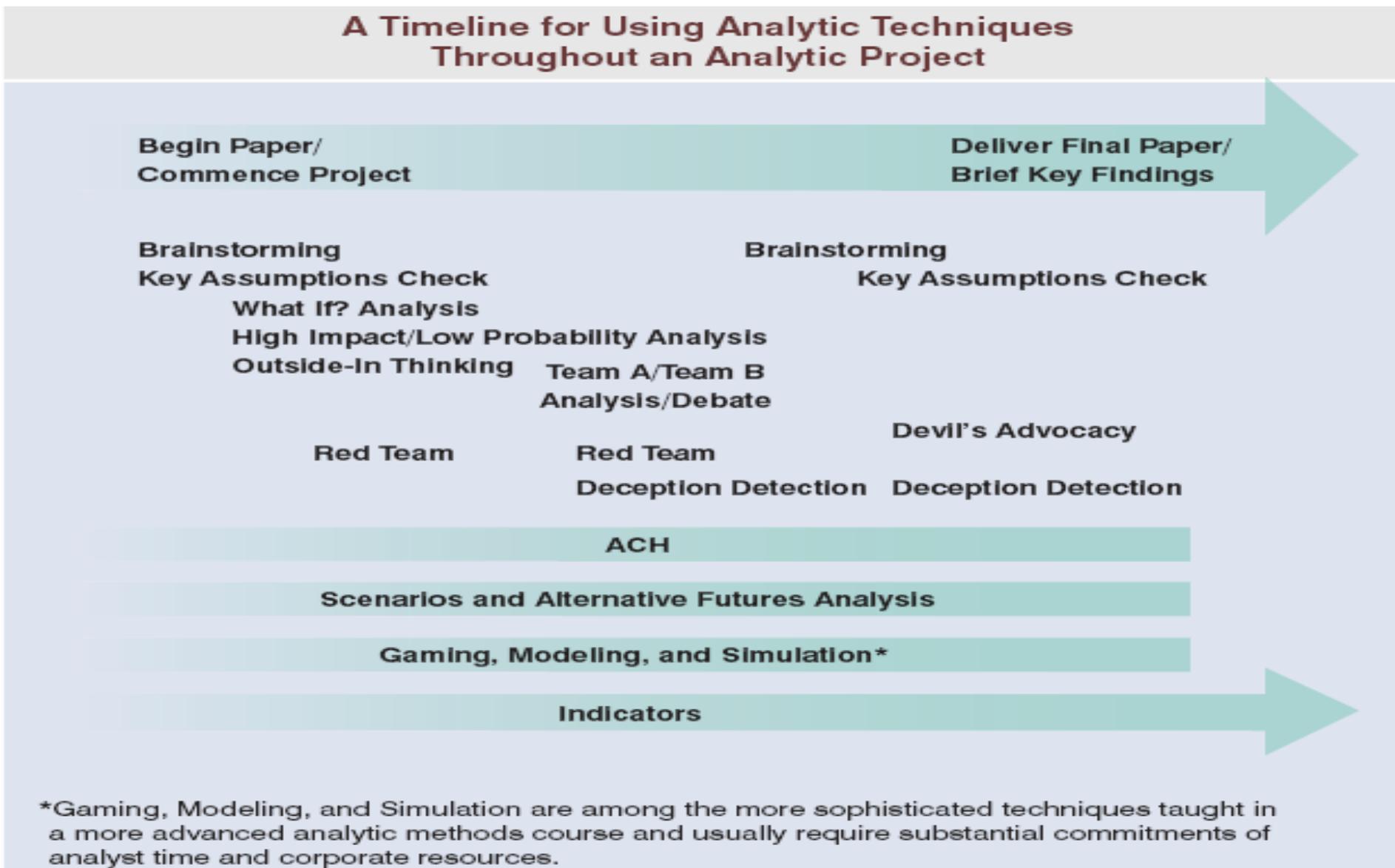
## Variables Clave

	variables	A	B	C	D	E	F	G	H	I	J	K	L	M	Mobilidad
1	A Enfrentamientos en la zona este	0	3	2	3	3	2	0	2	3	3	3	0	2	26
2	B Asentamientos de milicias extranjeras	3	0	3	2	3	1	2	2	3	3	3	1	3	29
3	C Refugiados	2	3	0	1	2	3	0	0	1	2	2	0	3	19
4	D Desplazados	0	1	1	0	1	3	0	0	0	0	1	0	3	10
5	E Estabilidad y seguridad territorial	3	3	3	3	0	1	3	2	1	3	3	3	3	21
6	F Transmisión de enfermedades infecciosas	0	1	3	3	1	0	0	1	0	0	0	0	3	12
7	G Control de los recursos hídricos	0	1	1	0	1	0	0	3	2	0	2	3	1	14
8	H Estabilidad política	2	2	2	2	2	1	1	0	3	2	2	1	1	21
9	I Desarme y desmovilización	3	3	2	3	3	2	2	2	0	3	3	0	3	29
10	J Explotación ilícita de recursos naturales	3	2	2	2	3	0	0	2	3	0	3	0	2	22
11	K Suministro ilegal de armas	3	3	2	3	3	2	2	2	3	3	0	0	3	29
12	L Exportación de energía hidroeléctrica	0	1	0	0	2	0	3	1	1	0	1	0	0	9
13	M Ayuda humanitaria	0	0	3	3	2	3	0	1	2	0	0	0	0	14
	Dependencia	19	23	24	25	26	18	13	18	22	19	23	8	27	



## Escenarios de Futuro







## El Sueño del Clavo y el Riesgo de Martillo

Ignorar que el martillo existe cuando encontramos un clavo suelto

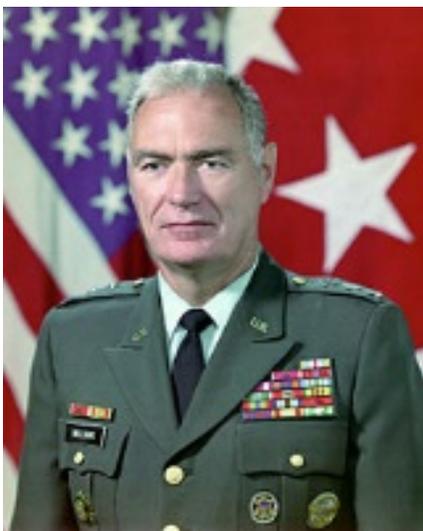
Debido a que conocemos el uso del martillo terminar por creernos que todos los problemas se asemejan a un clavo



**El sueño del clavo**

**El riesgo del martillo**

“Comprender las necesidades del consumidor y las fuentes disponibles permite que un analista elija la metodología correcta para obtener respuestas útiles.”

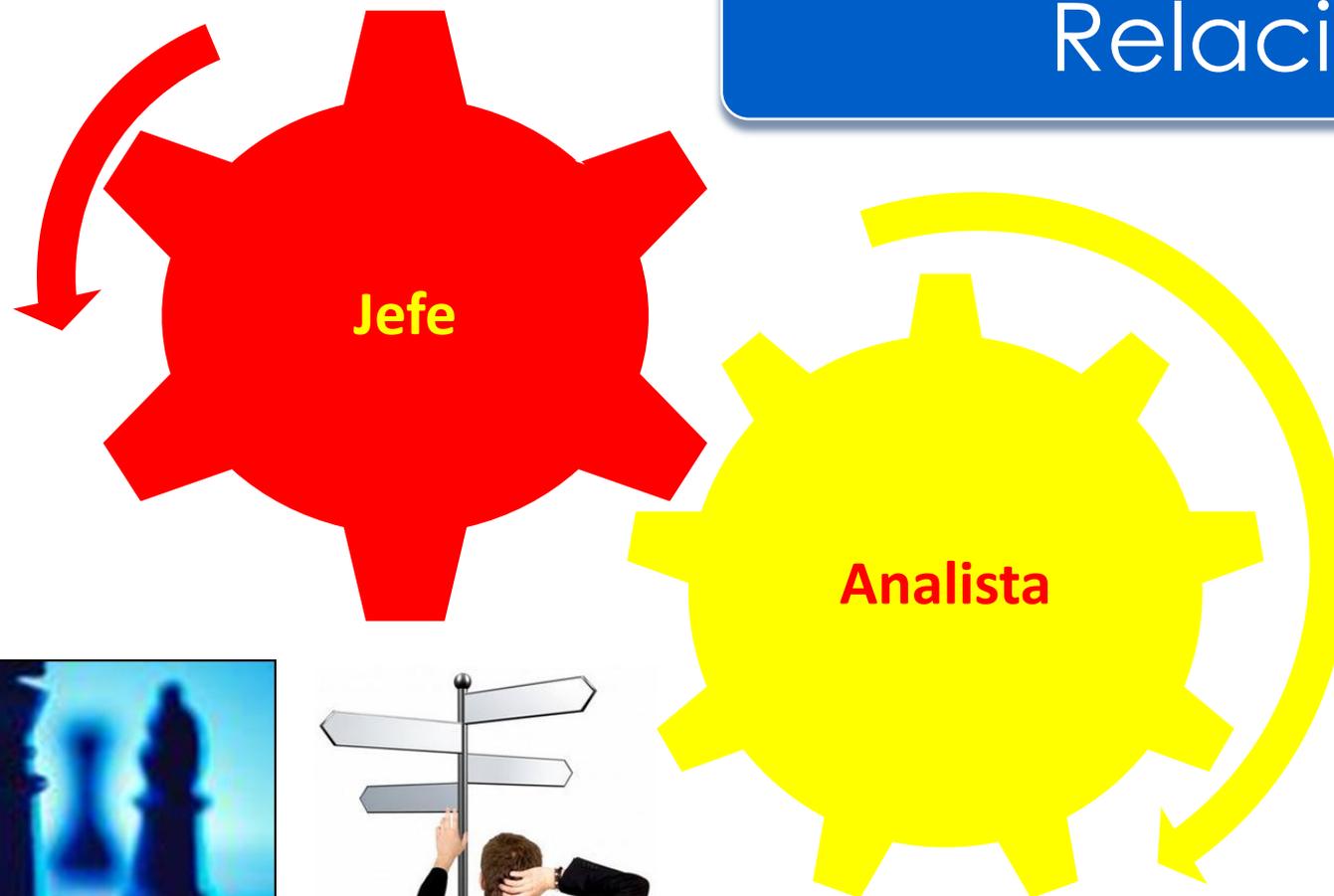


James A. Williams, LTG, U.S. Army (Ret.)  
Former Director, Defense Intelligence Agency



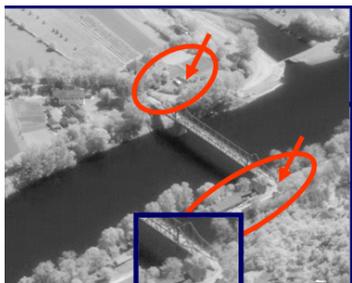


## Relación





Todas las conclusiones a las que se llega en el análisis de inteligencia poseen cierto grado de incertidumbre



Nunca tenemos todos los datos necesarios.

Las evidencias muchas veces son incompletas.



El proceso de análisis examina como las evidencias, argumentos y conclusiones coexisten.



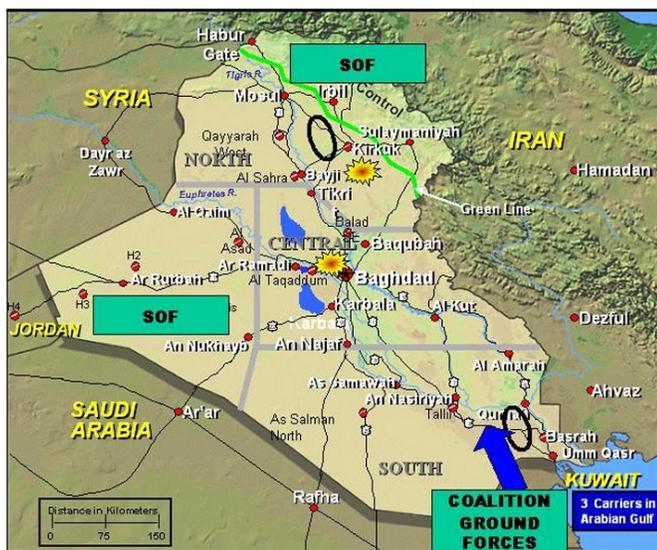
## ¿Qué necesita saber?

*Para evitar malentendidos y asegurar que existe una comprensión clara y común de lo que es real y lo que es supuesto, el Jefe debe ser informado de:*

*"lo que se sabe y por qué se sabe,*

*lo que se supone y por qué se supone,*

*lo que no se sabe y lo que se está haciendo al respecto".*





INTELIGENCIA  
MÁS LIDERAZGO

¿Preguntas?

JOSÉ MANUEL DÍAZ-CANEJA GRECIANO



[jmdiazcaneja@inteligenciayliderazgo.com](mailto:jmdiazcaneja@inteligenciayliderazgo.com)



[www.linkedin.com/in/jose-manuel-diaz-caneja](http://www.linkedin.com/in/jose-manuel-diaz-caneja)



[@JDiaz\\_Caneja](https://twitter.com/JDiaz_Caneja)



Formación en Inteligencia por [iL Inteligencia más Liderazgo](#) esta protegida por una licencia [Creative Commons](#)

[Reconocimiento - No Comercial - Compartir Igual 4.0 Internacional](#)



ARE YOU FIT TO SERVE?

