#IntelCon2020

IntelCon
by Ginseg

When Cyber met Intel

José María Blanco Navarro
Jorge Alcaín Pro

Congreso Online de Ciberinteligencia
Julio 2020

Presentación

IntelCon by Ginseg

#IntelCon2020

José María Blanco

Licenciado en Económicas y en Derecho

Manager Oficina de Inteligencia y Prospectiva

jose-maria.blanco-navarro@prosegur.com

https://www.linkedin.com/in/jose-mar%C3%ADa-blanco-navarro-5b511137/

Jorge Alcaín Pro

Grado en Ingeniería Informática

PMO Europe Manager y Co-fundador de ChronosEye

jalcain@chronoseye.com

@jorgeapro

https://www.linkedin.com/in/jorgeapro/

IntelCon
by Ginseg

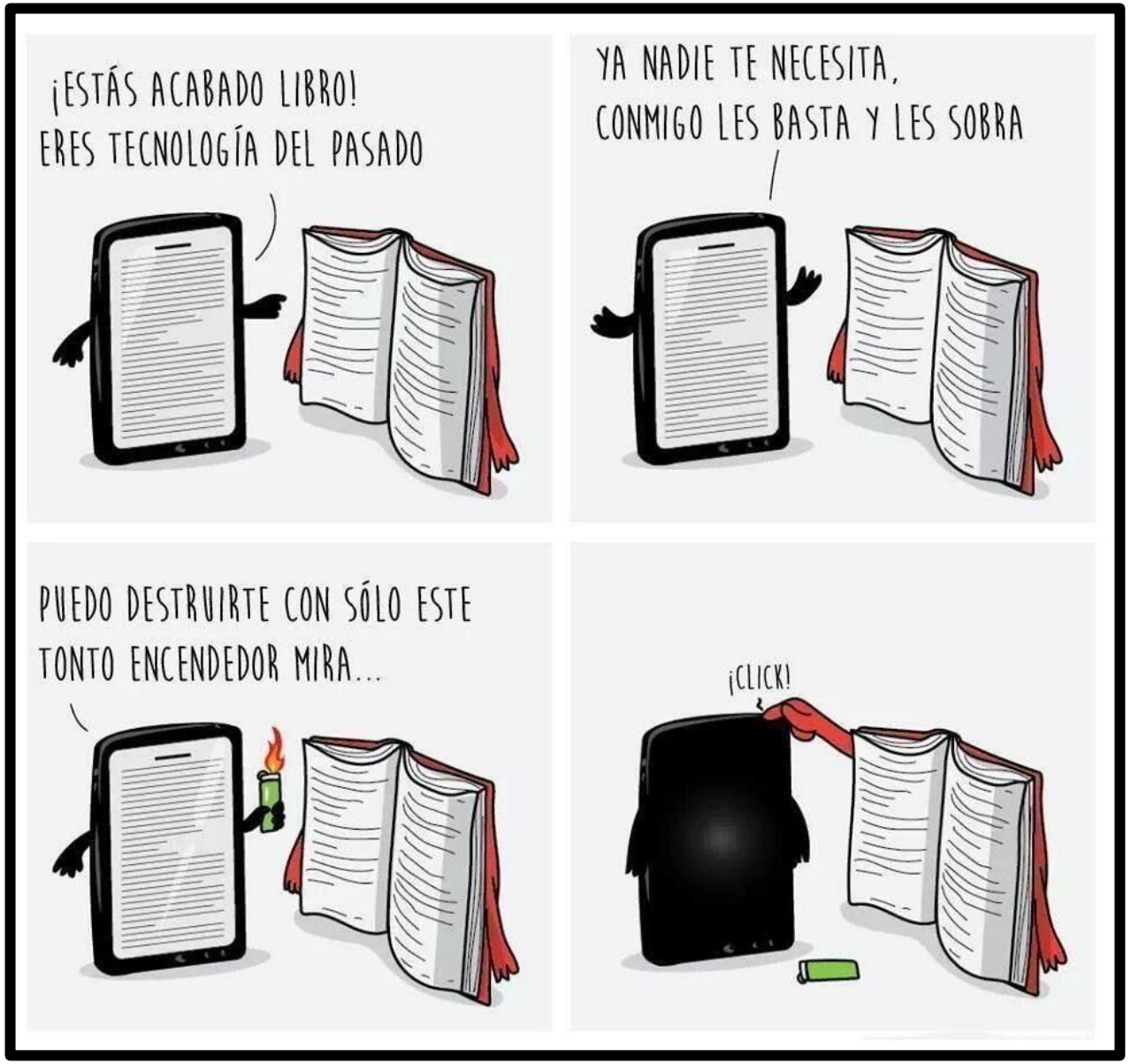
1

Hacia un Mundo Digital

Los analfabetos del siglo XXI no serán aquellos que no sepan leer o escribir, sino aquellos que no puedan aprender, desaprender y reaprender

Alvin Toffler

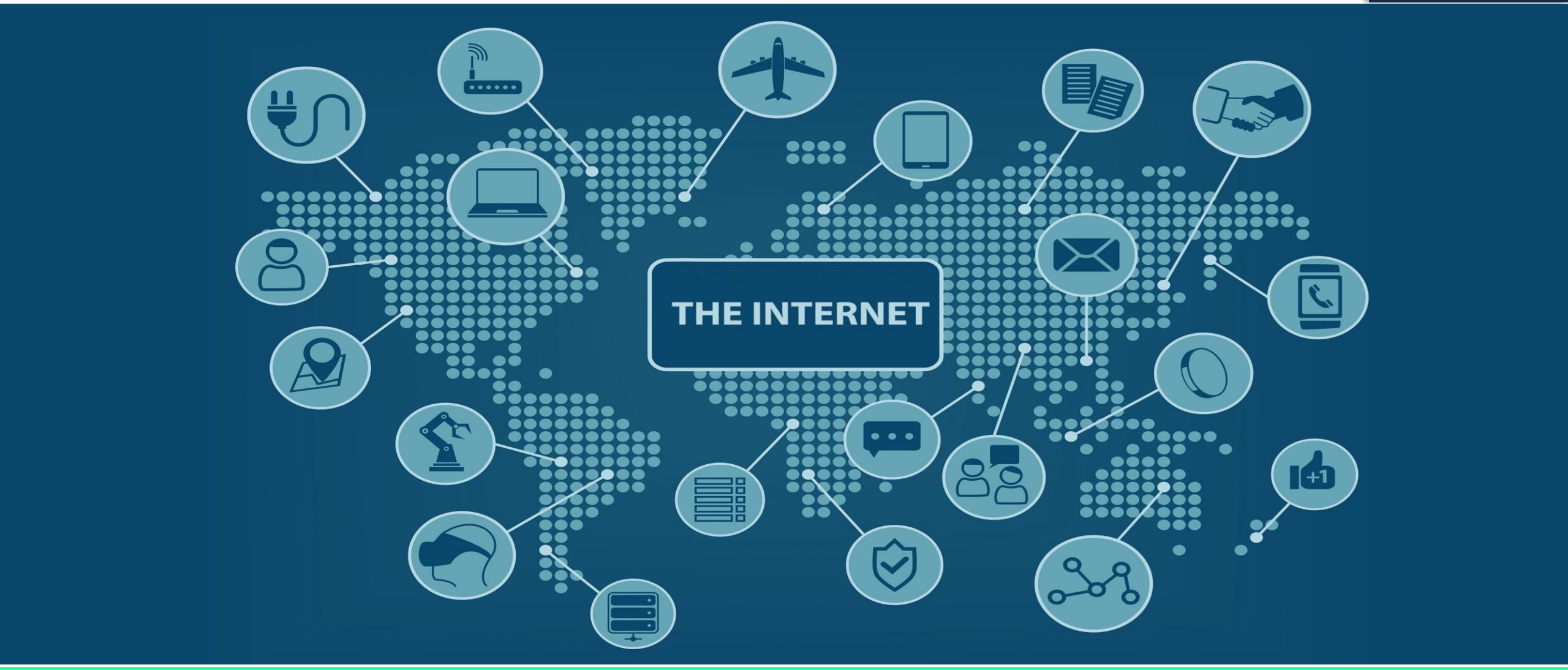
Primer paso: TRANSFORMACIÓN DEL DATO



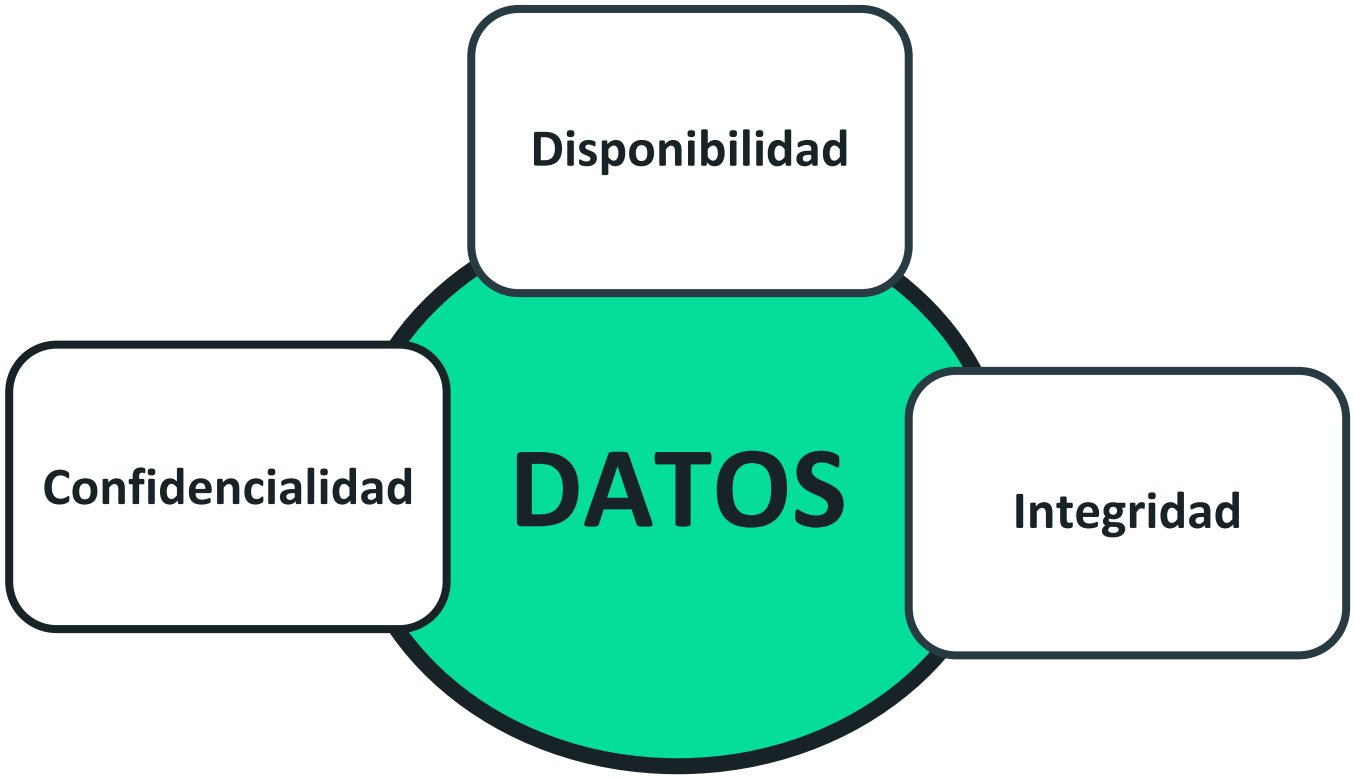
Segundo paso: INTERNET

IntelCon
by Ginseg

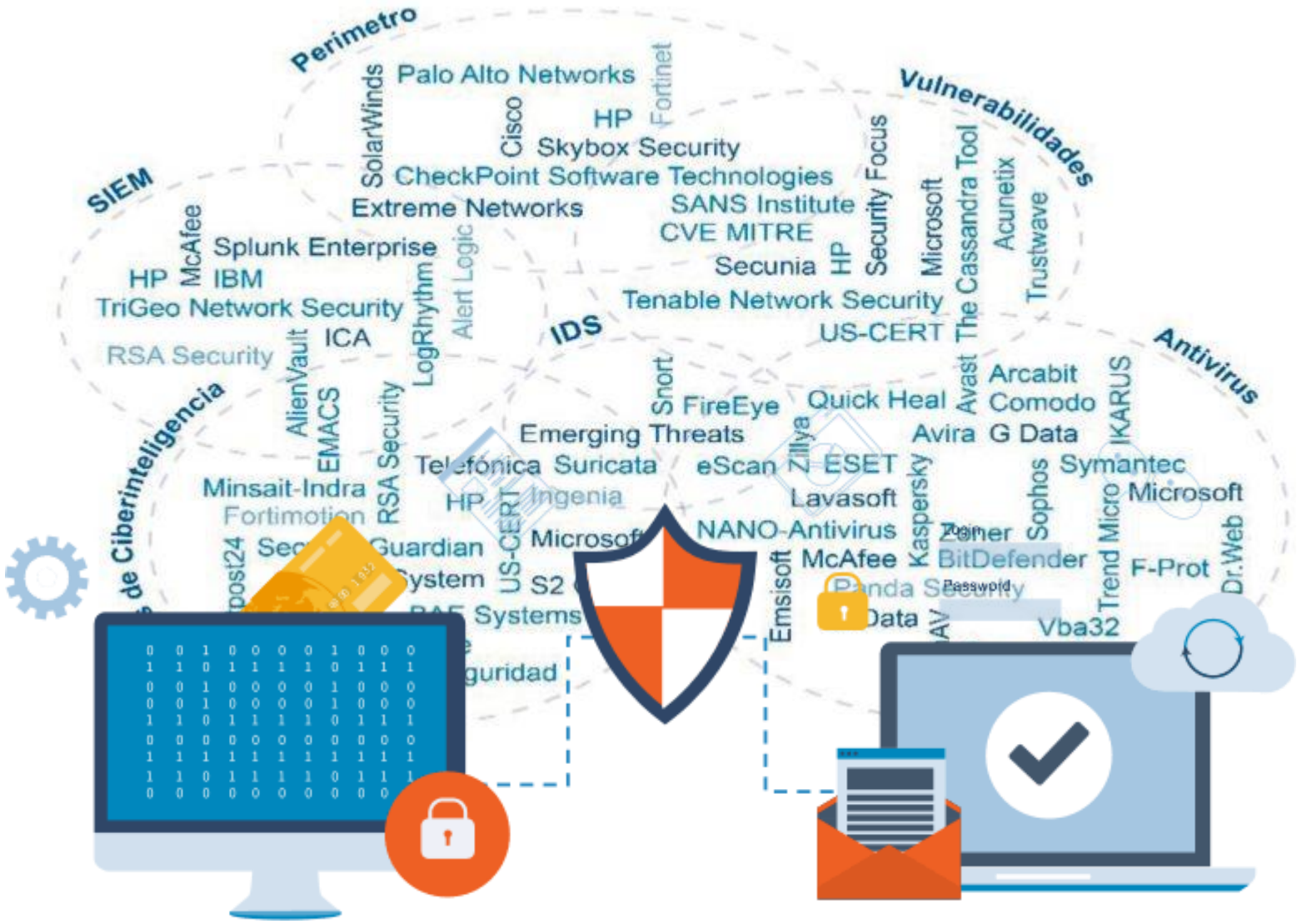
#IntelCon2020



¿Qué protegemos?



Tecnologías para protegerse



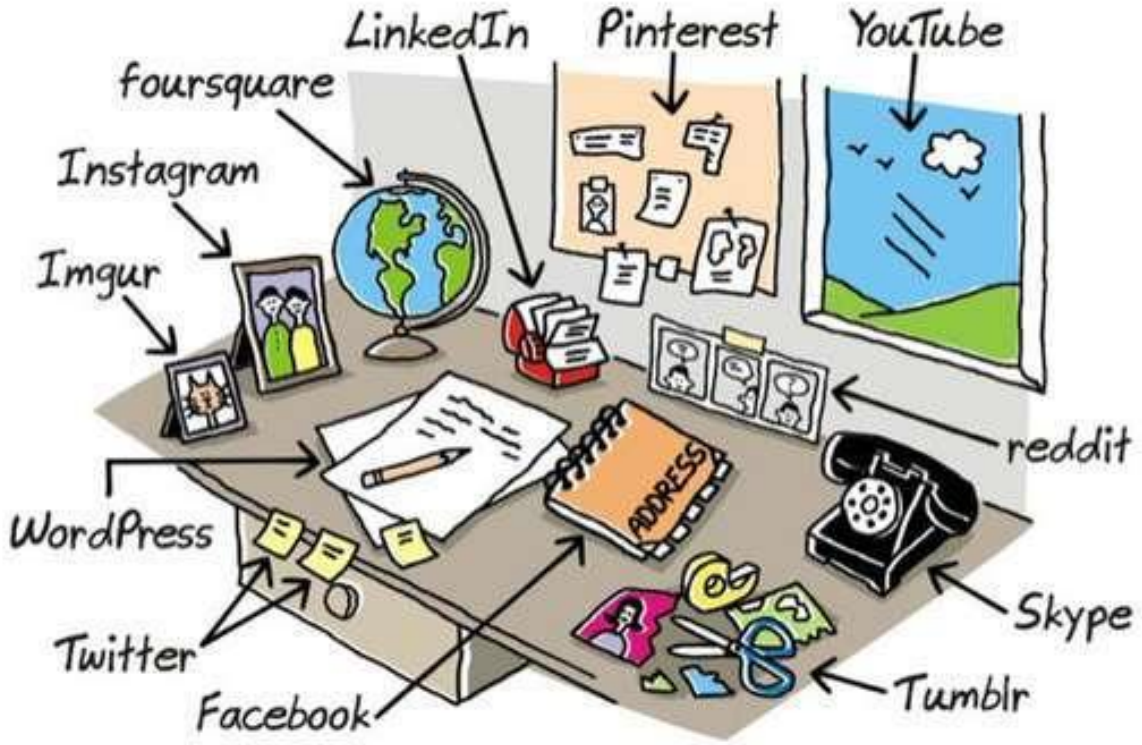
Interconexión

Comunicación Inmediata

IntelCon
by Ginseg

#IntelCon2020

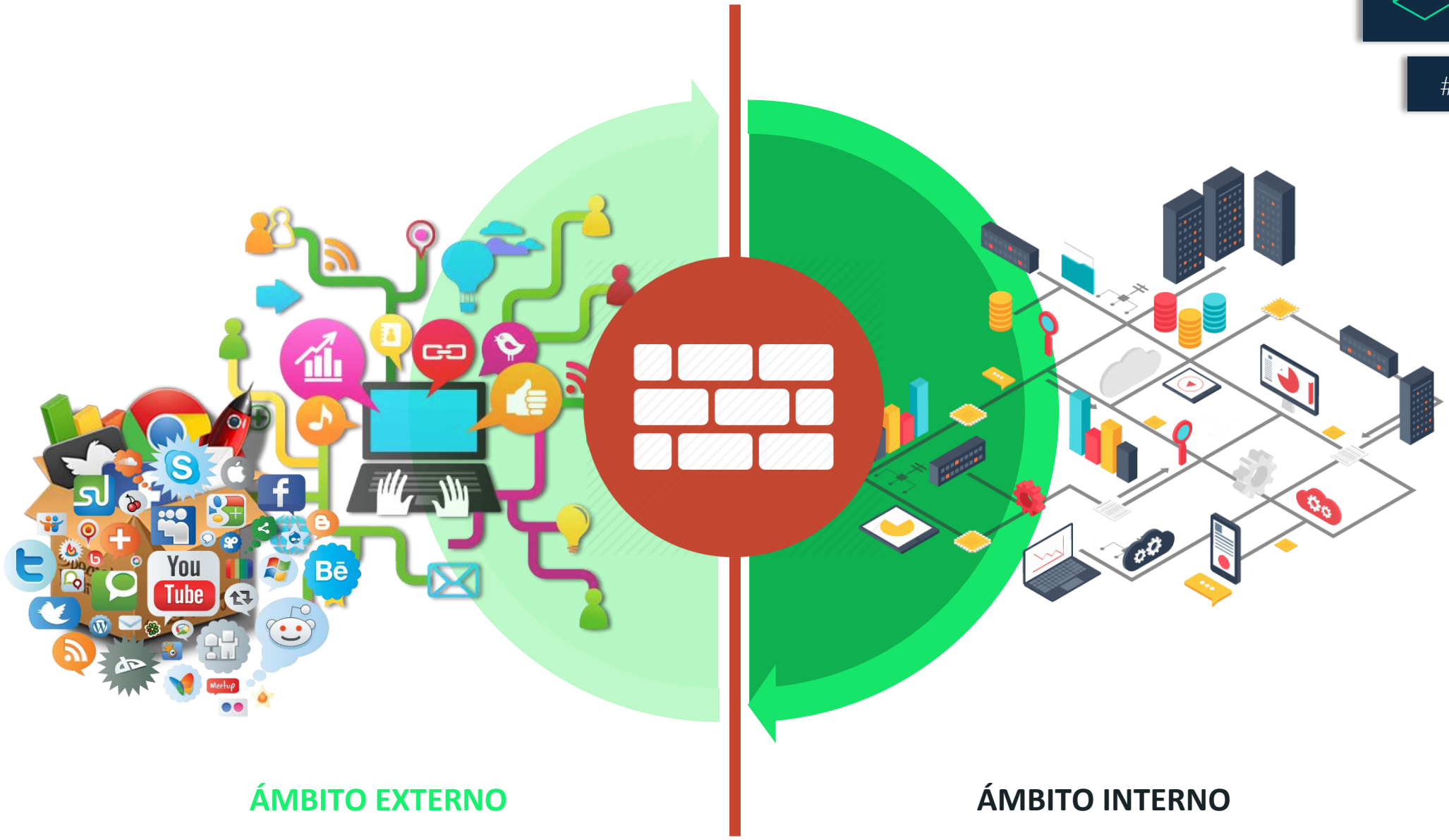
¿En qué nos hemos TRANSFORMADO?



¿Y cómo nos PROTEGEMOS AHORA?

IntelCon
by Ginseg

#IntelCon2020



ÁMBITO EXTERNO

ÁMBITO INTERNO

¿Y el FUTURO?

IntelCon by Ginseg

#IntelCon2020

IntelCon
by Ginseg

2
Hacia un concepto de Ciberinteligencia

El conocimiento si no se sabe aplicar es peor que la ignorancia

Charles Bukowski

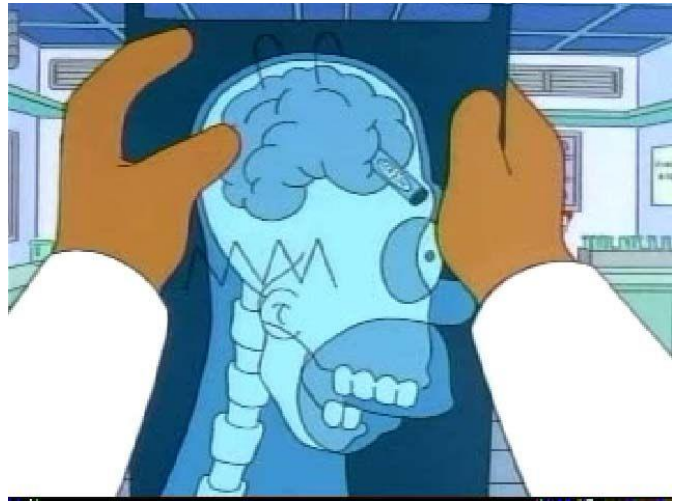
Diversidad de CONCEPTOS

"El **conocimiento sobre los ciber-adversarios y sus métodos**, además del conocimiento sobre la posición de seguridad de una organización sobre sus adversarios en el ciberespacio y sus métodos" *(RSA,2012)*

"Los **productos y los procesos del ciclo de inteligencia** para analizar las capacidades, intenciones y actividades – no sólo técnicas- de los potenciales adversarios y competidores en el ciberespacio" *(INSA, 2015)*

"La **adquisición y análisis de información** para identificar, seguir y predecir ciber-capacidades, intenciones y actividades que ofrezcan líneas de acción para apoyar la toma de decisiones" (Carnegie Mellon Software Engineering, 2013)

"**Conocimiento** de la superficie de ataque, sus objetos de mayor valor y objetivos, y cómo sus vulnerabilidades pueden ser explotadas; mantener un situational awareness sobre actores maliciosos; desarrollar técnicas y aplicaciones para contrarrestar, identificar y vigilar; en su versión más avanzada entender las motivaciones de los atacantes, su lenguaje, organización, comportamiento individual y grupal, con objeto de perfilar grupos, actores y campañas" *(Department of Homeland Security, 2012)*



¿Posibilidad de un CONCEPTO consensuado?

Proceso y producto de la obtención y análisis de datos e información en/sobre el ciberespacio, realizado por especialistas, y orientado a la toma de decisiones en forma, tiempo y lugar

Adaptación basada en definiciones de Javier Candau (CCN-CERT) y Manuel Torres Soriano (GESI)

Tipos de Ciberinteligencia

IntelCon by Ginseg

#IntelCon2020

ESTRATÉGICA

- Amplia en la obtención.
- Más allá del sector.
- Mira a medio y largo plazo.
- Amplia en identificar adversarios
- Analiza el entorno
- Menos técnica
- Vinculada a análisis de riesgos

TÁCTICA

- Donde las batallas se planifican y ejecutan
- Equipos de respuesta a incidentes
- Resiliencia y análisis forense
- Análisis del atacante: modus operandi, motivaciones, capacidades, etc.
- Carácter técnico

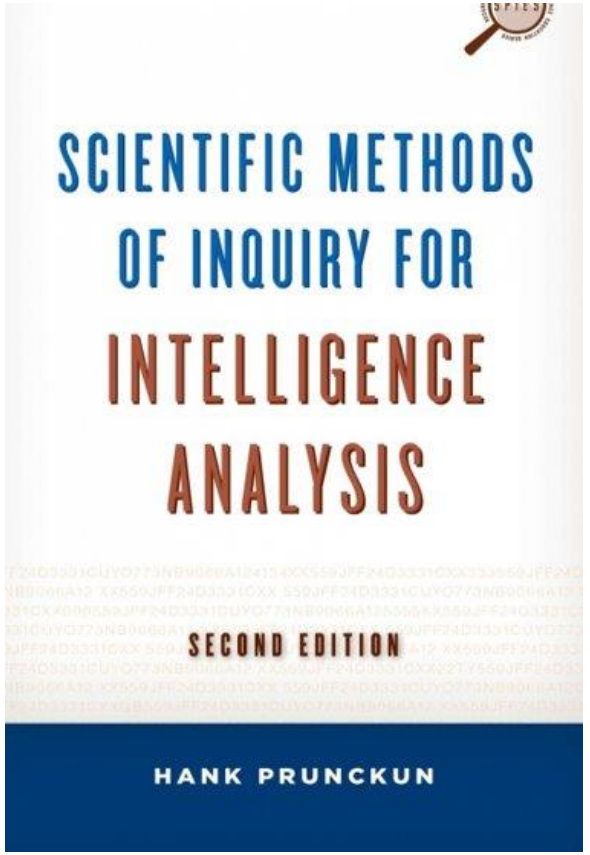
OPERACIONAL

- Orientada a los managers de IT, CIO, CISO.
- Apoyo a decisiones
- Foco en procesos y operaciones: negocio, clientes, proveedores…
- Análisis adversario técnico
- Combina tareas técnicas y no técnicas (vectores de mayor riesgo)

El detalle de la ciberinteligencia estratégica

CIBERINTELIGENCIA ESTRATÉGICA ad-hoc en cada empresa:

- La naturaleza e identidad
- Las decisiones que debe tomar
- El marco temporal y geográfico en el que actúa
- El alcance de la obtención de información.
- El carácter de los potenciales adversarios.
- El nivel de aptitudes técnicas para la función.

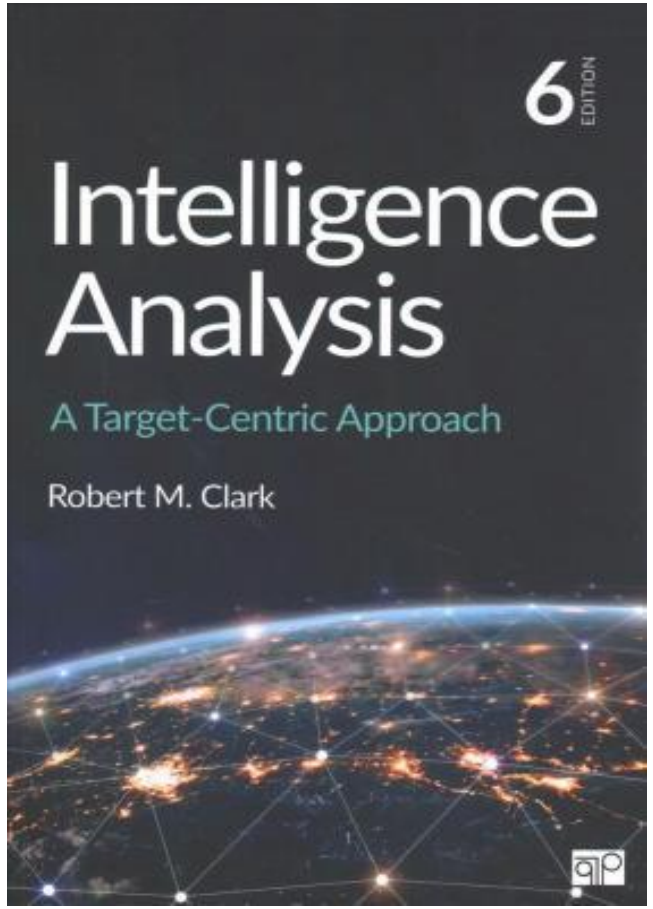


Requerimientos de información en ciberinteligencia estratégica

IntelCon by Ginseg

#IntelCon2020

- Qué información se precisa por el decisor
- Qué información se precisa sobre el entorno que configura el ámbito espacial y temporal
- Qué información se precisa sobre amenazas y riesgos para nuestra organización o nuestros clientes.
- Qué información se precisa sobre potenciales adversarios.
- Qué posición tiene la organización en seguridad
- Objetivos a proteger.
- Vulnerabilidades.
- Nivel de riesgo: bajo, medio o alto riesgo ciber.
- Qué valor tiene la información de la organización.
- Qué valor tienen los aspectos digitales en sus procesos.
- Qué requisitos legales tiene la información

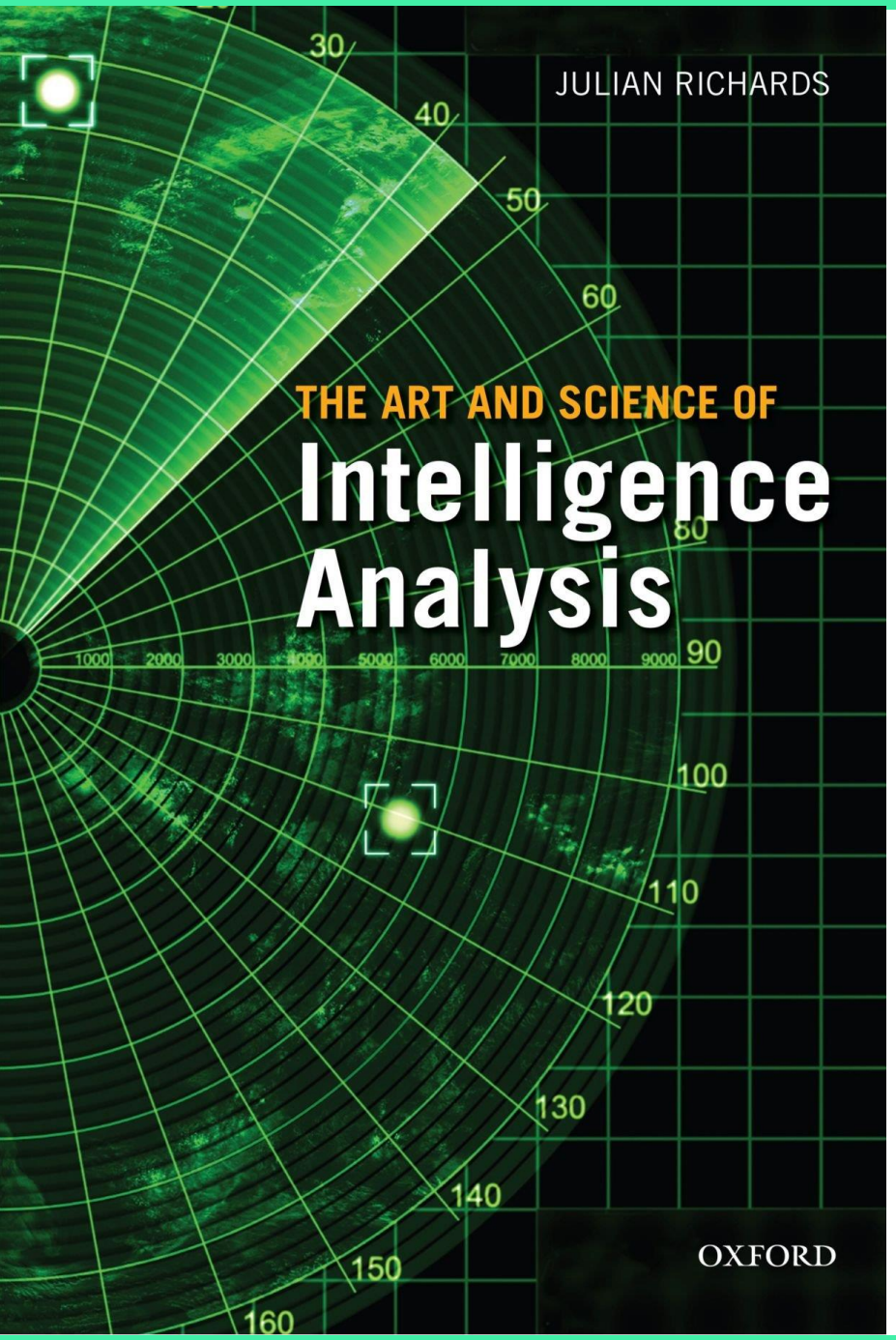


3

De Intel hacia Ciber

Vivimos en un mundo donde todas las guerras comenzarán como ciberguerras ... Es la combinación de piratería y campañas de desinformación masivas y bien coordinadas

Jared Cohen

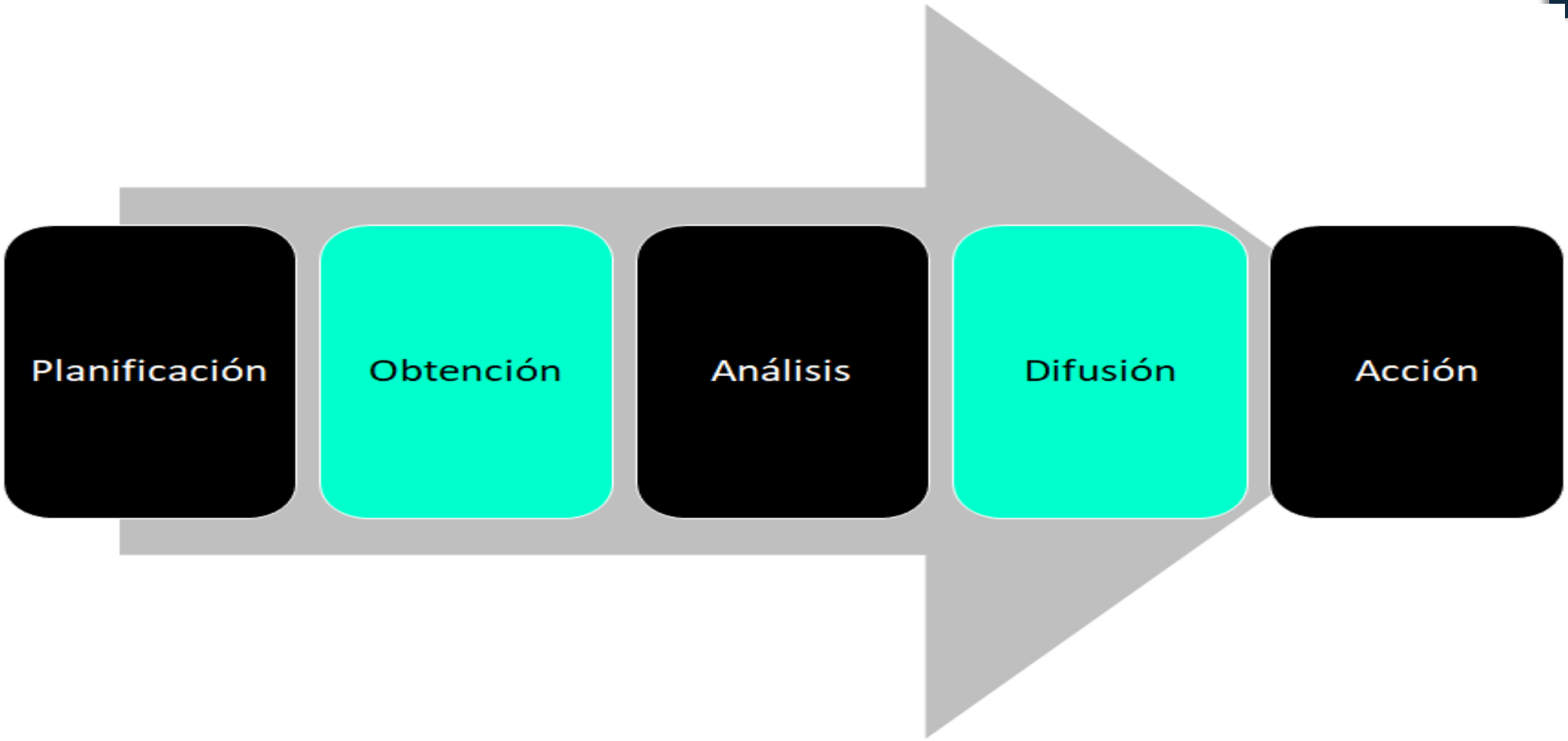


IntelCon
by Ginseg

#IntelCon2020

1	• Intereses a proteger
2	• Fundamentos y doctrina
3	• Ciclo de Inteligencia
4	• Trabajo con fuentes diversas
5	• Técnicas estructuradas de análisis
6	• Conocimiento sobre desinformación
7	• Prospectiva

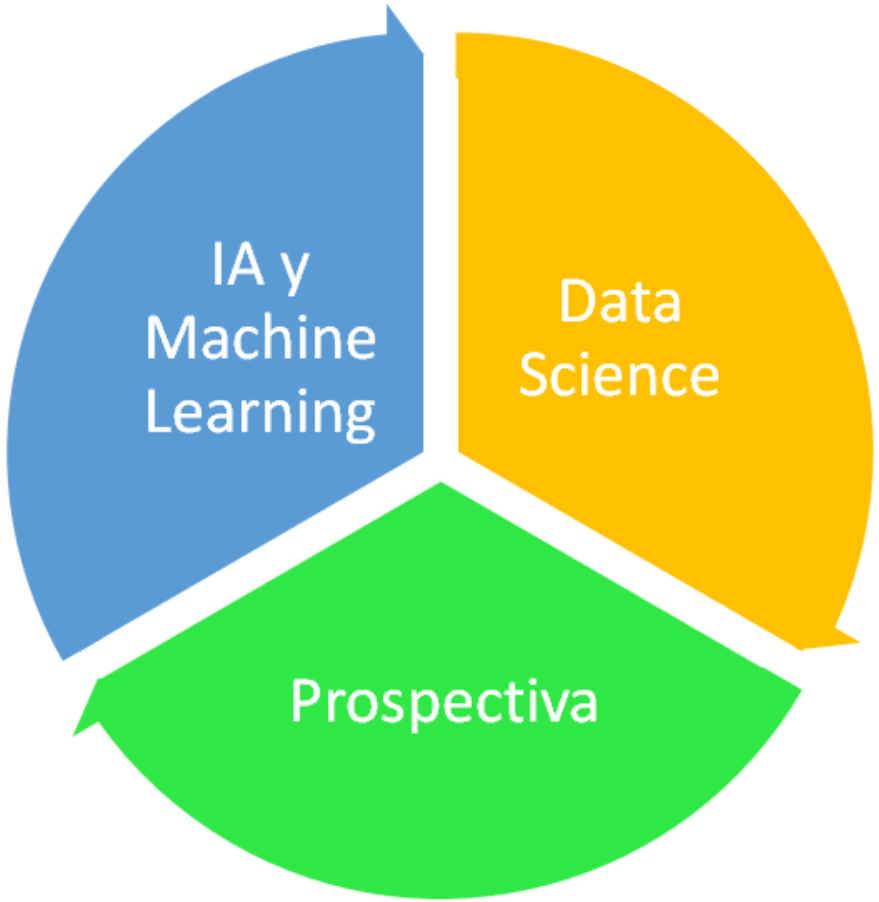
Proceso



Metodología

IntelCon
by Ginseg

#IntelCon2020



Identidad de objetivos

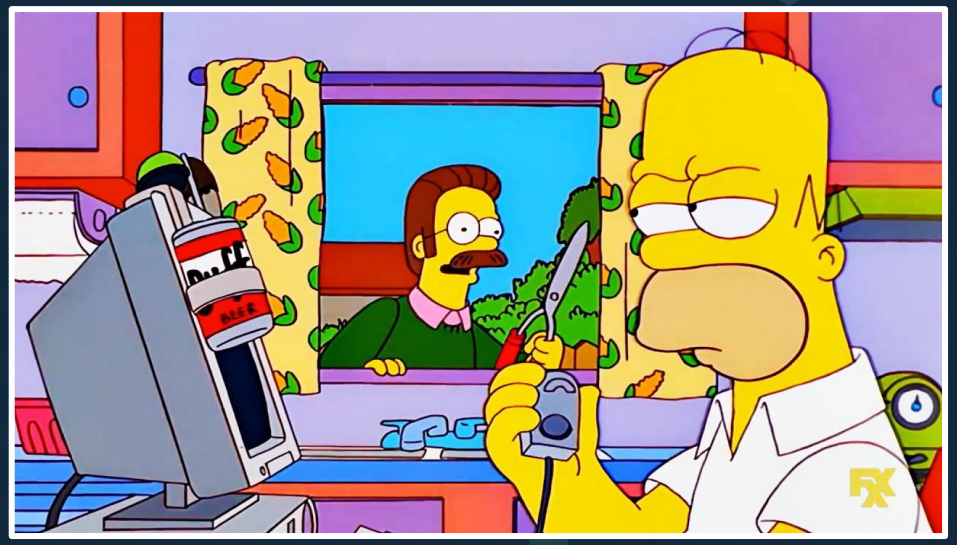
IntelCon
by Ginseg

4

De Ciber hacia Intel

Ser capaz de superar la seguridad no te convierte en un hacker, de la misma forma que hacer un puente a un coche no te convierte en ingeniero mecánico

Eric S. Raymond

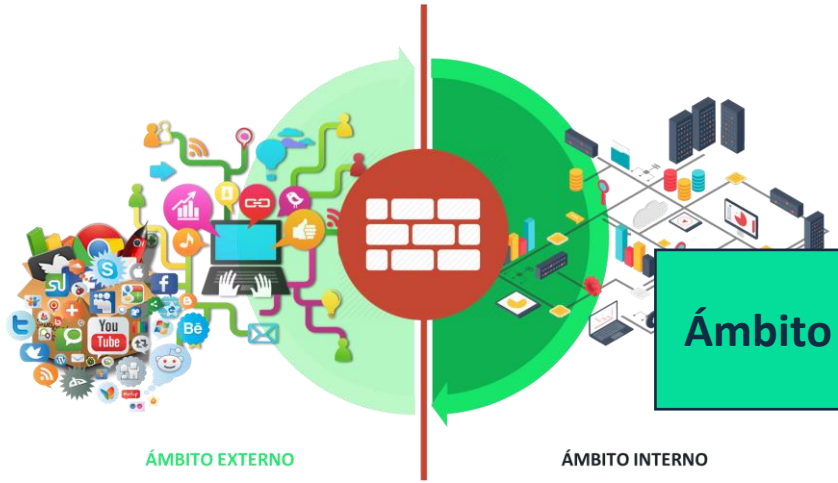


PRIMEROS PASOS de la Ciberinteligencia

IntelCon by Ginseg

#IntelCon2020

Activos de Información



Ámbito Externo

Nuevas Amenazas

Fugas de Información

Ingeniería Social

SIGUIENTES PASOS de la Ciberinteligencia

IntelCon
by Ginseg

#IntelCon2020

Herramienta de VISIÓN EN EL MUNDO DIGITAL

Herramienta de OBTENCIÓN DE INFORMACIÓN en la RED

IntelCon
by Ginseg

#IntelCon2020

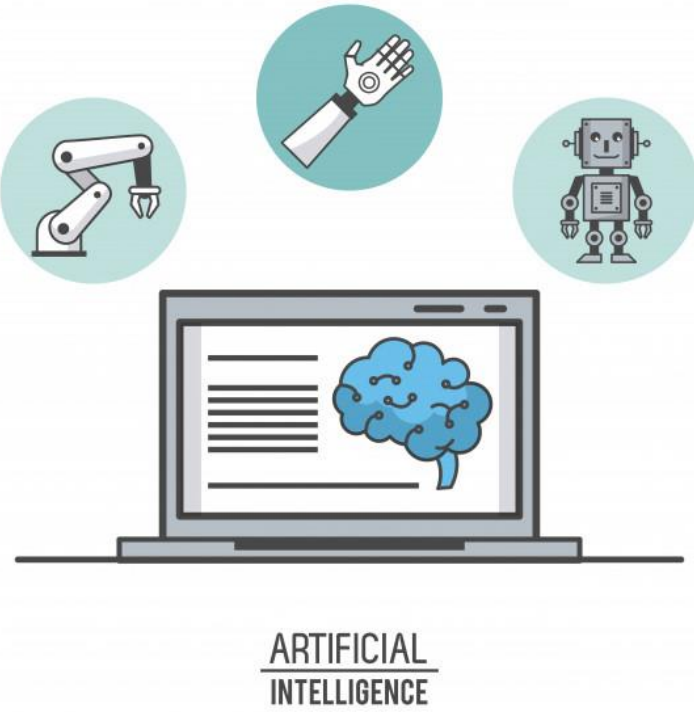
OPSEC

OPERATIONS
SECURITY

La ciberinteligencia se apoya en…

IntelCon
by Ginseg

#IntelCon2020

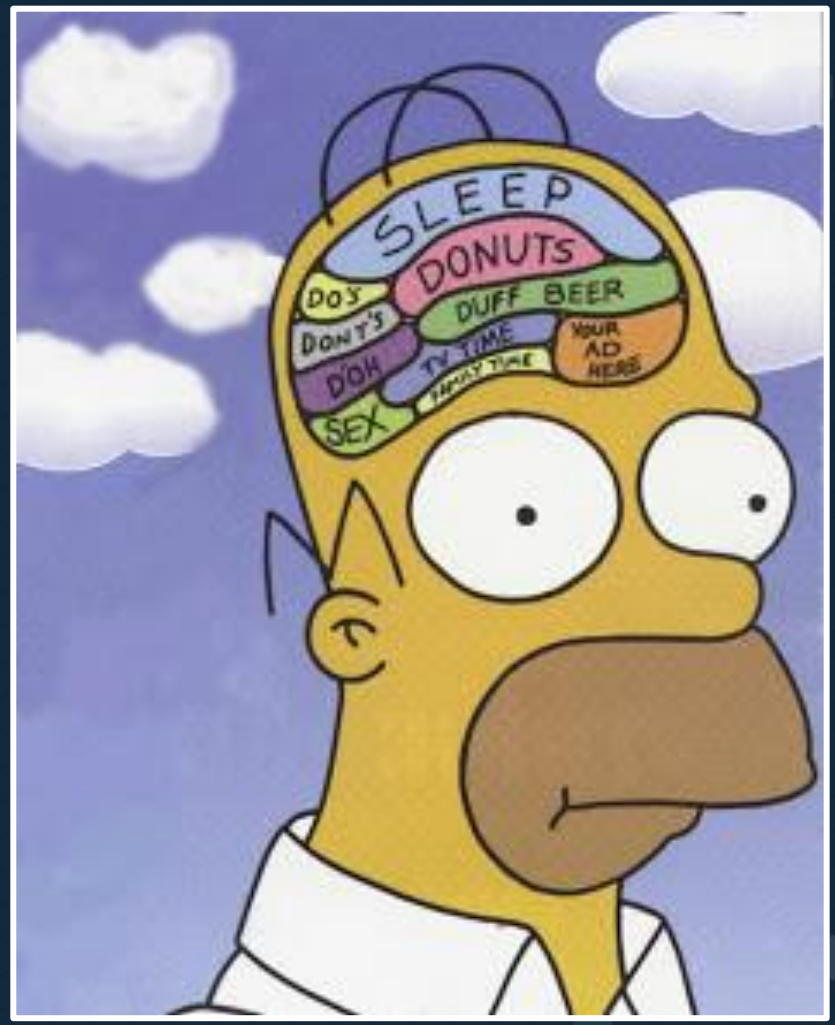


5

Describiendo los pasos…

"Es de sentido común elegir un método y probarlo.
Si falla, admitirlo francamente y probar con otro.
Pero, sobre todo, intentar algo.".

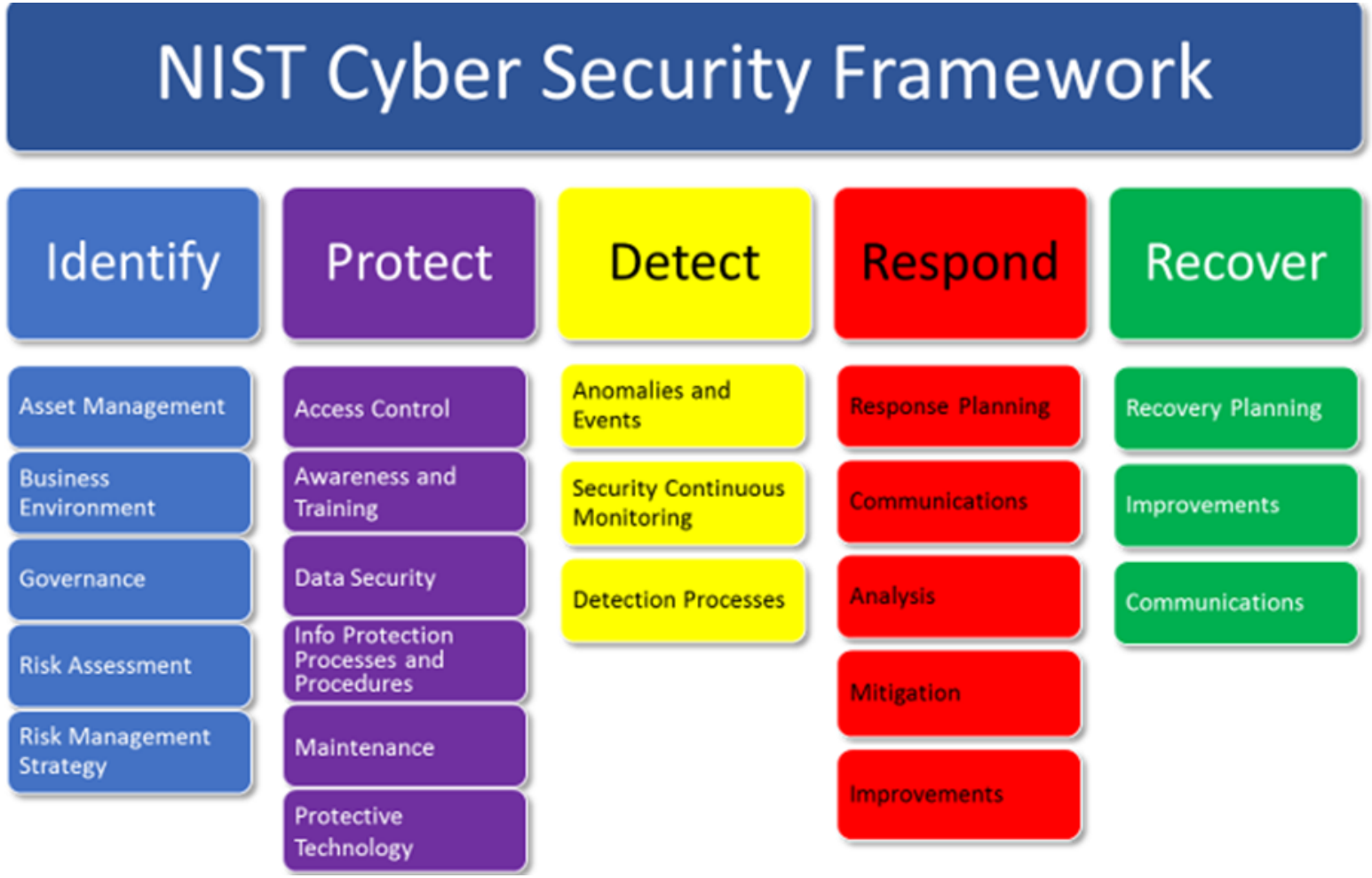
Franklin D. Roosevelt



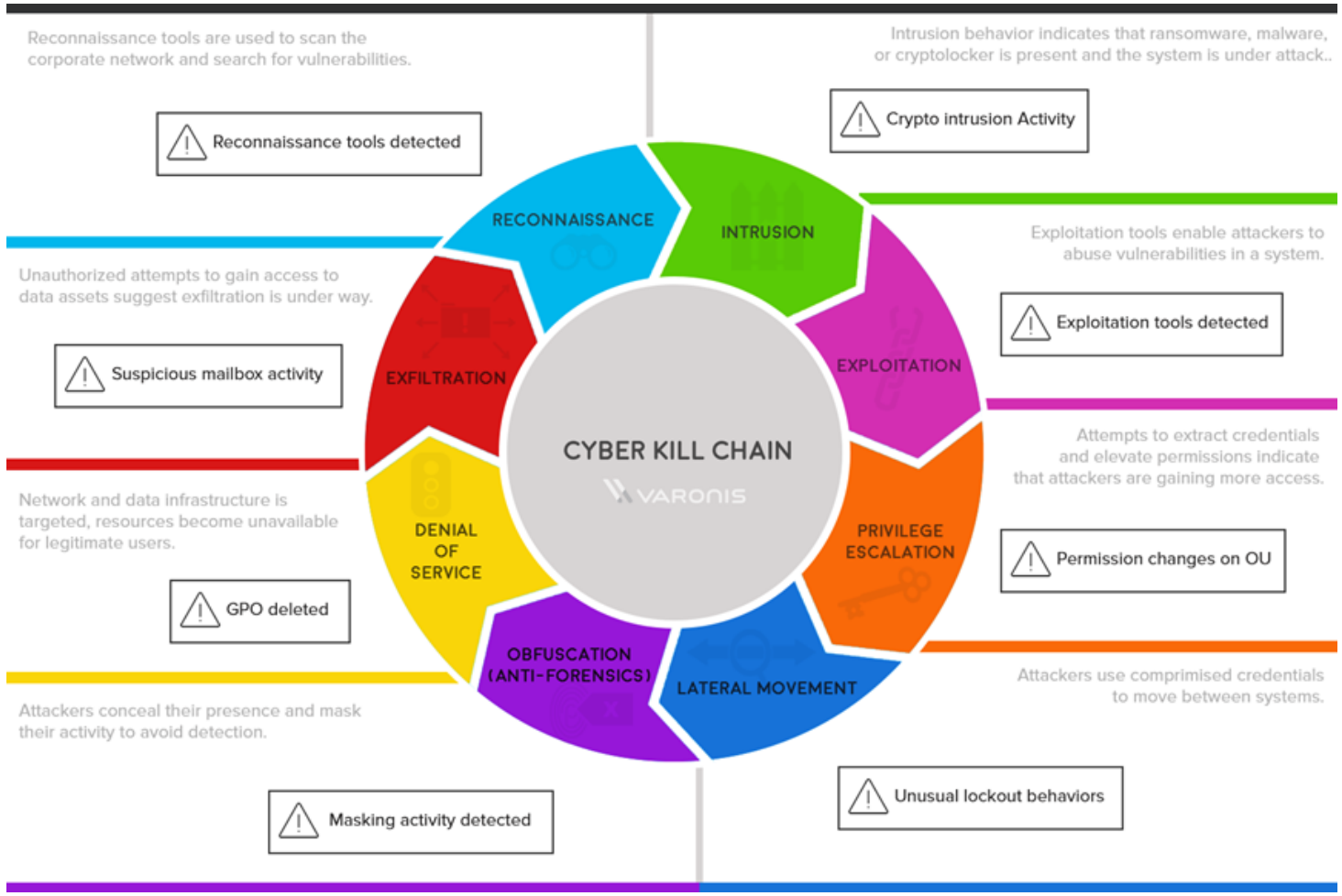
Basándonos ESTÁNDAR CYBER

IntelCon
by Ginseg

#IntelCon2020



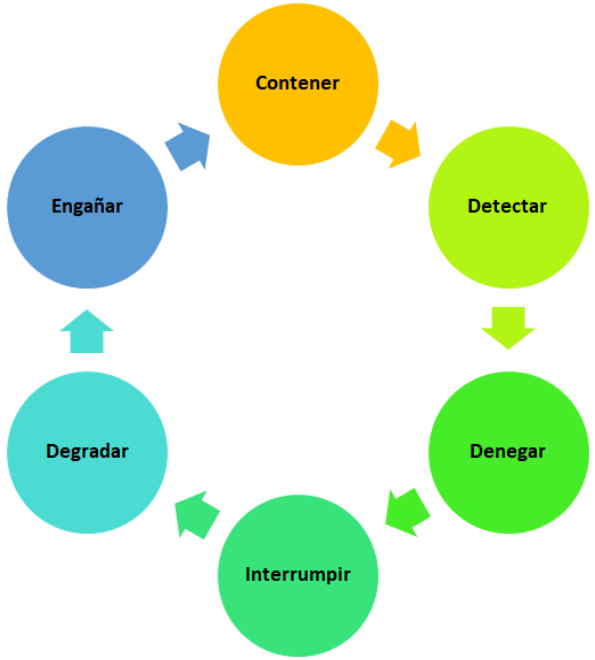
Basándonos ESTÁNDAR CYBER

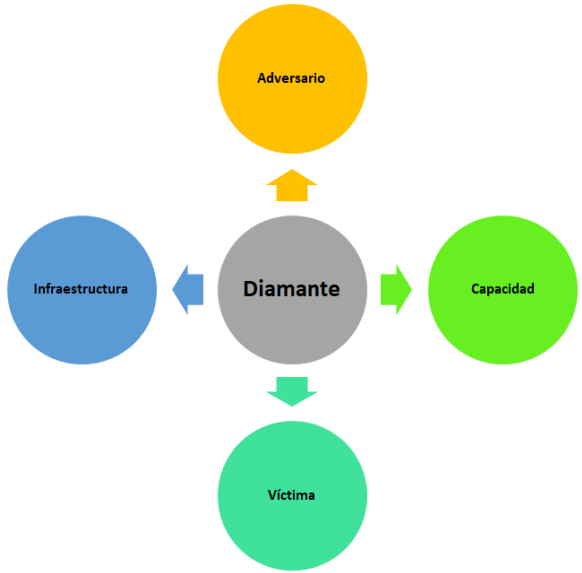


CASO PRÁCTICO Lucha contra la radicalización on line

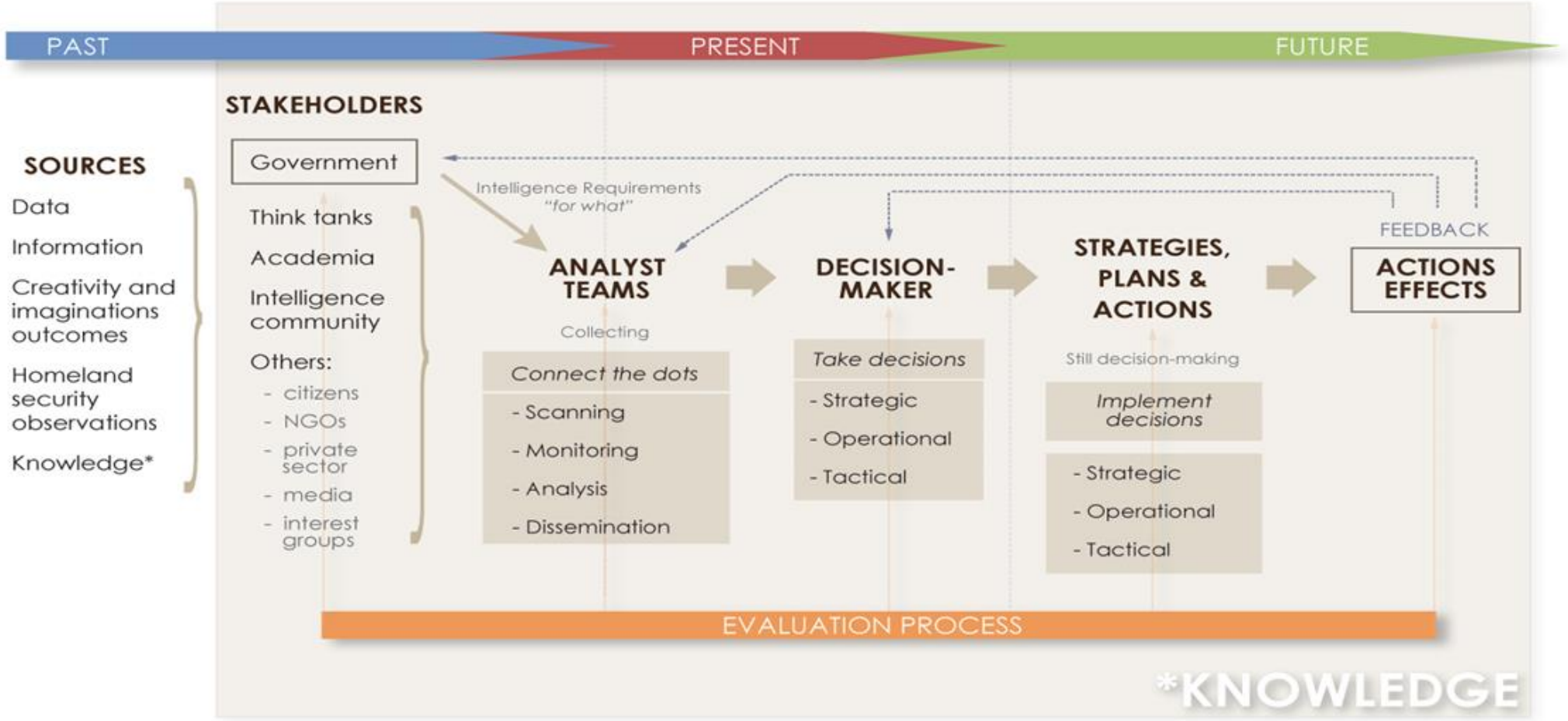
IntelCon by Ginseg

#IntelCon2020





MODELO integrador



Blanco, J.M. & Cohen, J., 2014

IntelCon
by Ginseg

6

Hacia un Mundo Inteligente

"Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología".

Bruce Schneier

VUCA: Entornos cambiantes

10 puntos para el FUTURO

IntelCon by Ginseg

#IntelCon2020

1. **Extrema convergencia entre el mundo físico y lógico**
2. **Prácticamente todos los riesgos para estados, organizaciones, empresas e individuos pueden tener aspectos tanto físicos como lógicos.**
3. **Desde ambas inteligencias se trata de proteger los mismos intereses: personas, infraestructuras, imagen y marca, datos e información, patrimonio y continuidad de negocio.**
4. **INTEL no es una ciencia. Debe ser desarrollada en muchos ámbitos**
5. **La INTEL precisa pragmatismo, uso de cualquier fuente o metodología que sea ÚTIL para apoyar toma de decisiones. NO DEBEMOS SER DOGMÁTICOS**
6. **La INTEL recoge marcos y metodologías de muchas disciplinas ajenas, de las ciencias sociales**
7. **Las 2 INTEL precisan de aproximaciones cuantitativas y cualitativas, para abordar la complejidad de los riesgos de nuestro mundo. IA, Machince learning, data science como aproximaciones muy relacionadas**
8. **La INTEL debe ser HOLÍSTICA. Para conocer el ciberespacio es preciso conocer el mundo físico y viceversa. Geopolítica, estrategia, conocimiento de las organizaciones, etc...**
9. Prospectiva. Ir más allá del cortoplacismo, de lo inmediato. ANTICIPAR
10. **MUNDO COMPLEJO. TENDREMOS CISNES NEGROS. ANticipar (ciberinteligencia) + Resiliencia (FDIR). No compartimentar la Inteligencia**

#IntelCon2020

IntelCon
by Ginseg

Gracias por la atención

Congreso Online de Ciberinteligencia | Julio 2020