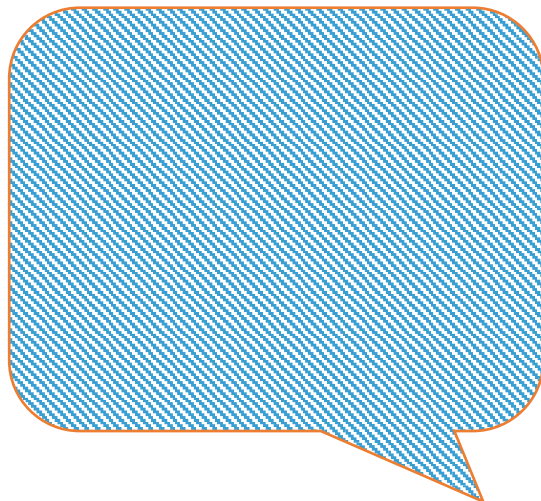




Los malos también saben de OSINT

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL

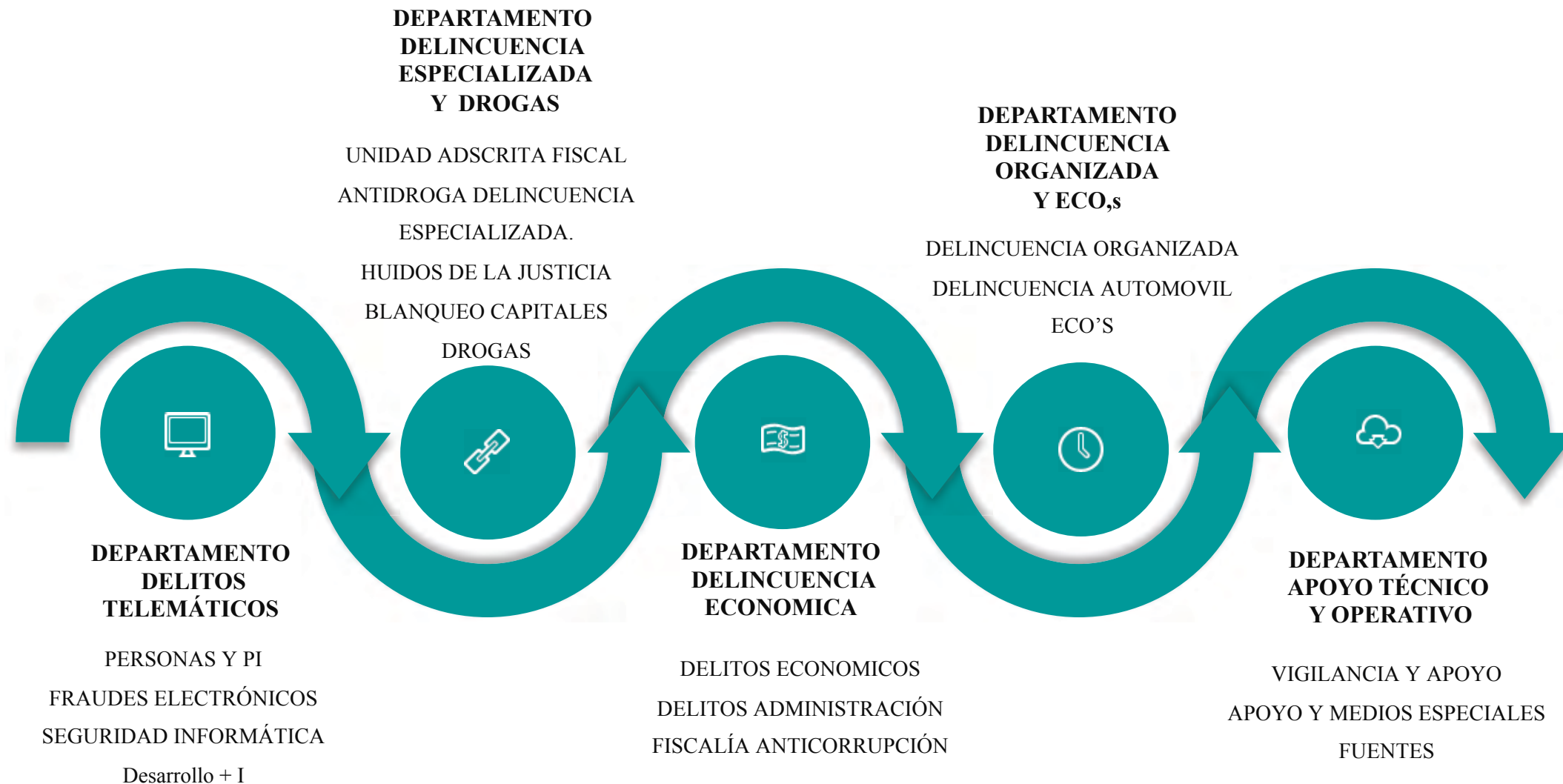


- César Lorenzana & Javier Rodríguez
- Guardia Civil
- delitostelematicos@guardiacivil.org

Índice

1. **Quiénes somos**
2. **Kill Chain Attack Model.**
3. **Caso real.**
4. **Recomendaciones**
5. **Preguntas**







DEPARTAMENTO DELITOS TELEMATICOS

Atención al Ciudadano



- RR.SS. y MCS
- Consejos y Alertas
- Informes y Notificaciones

Investigación Delitos



- Ataques a Sistemas
- Fraudes y Estafas
- Abusos, Amenazas, Extorsiones, y otros...

Apoyo Técnico Especializado



- *Diseño de herramientas*
- *Adquisición de evidencias*
- *Análisis Soportes & Datos*



AGENTES EXTERNOS, GRUPOS ORGANIZADOS, ACTORES SOLITARIOS,..... PROFESIONALES



CENTRADO EN OBEJTIVOS COMERCIALES/ECONÓMICOS



AMENAZA ECONOMICA REAL PARA EMPRESAS ESTRATEGICAS



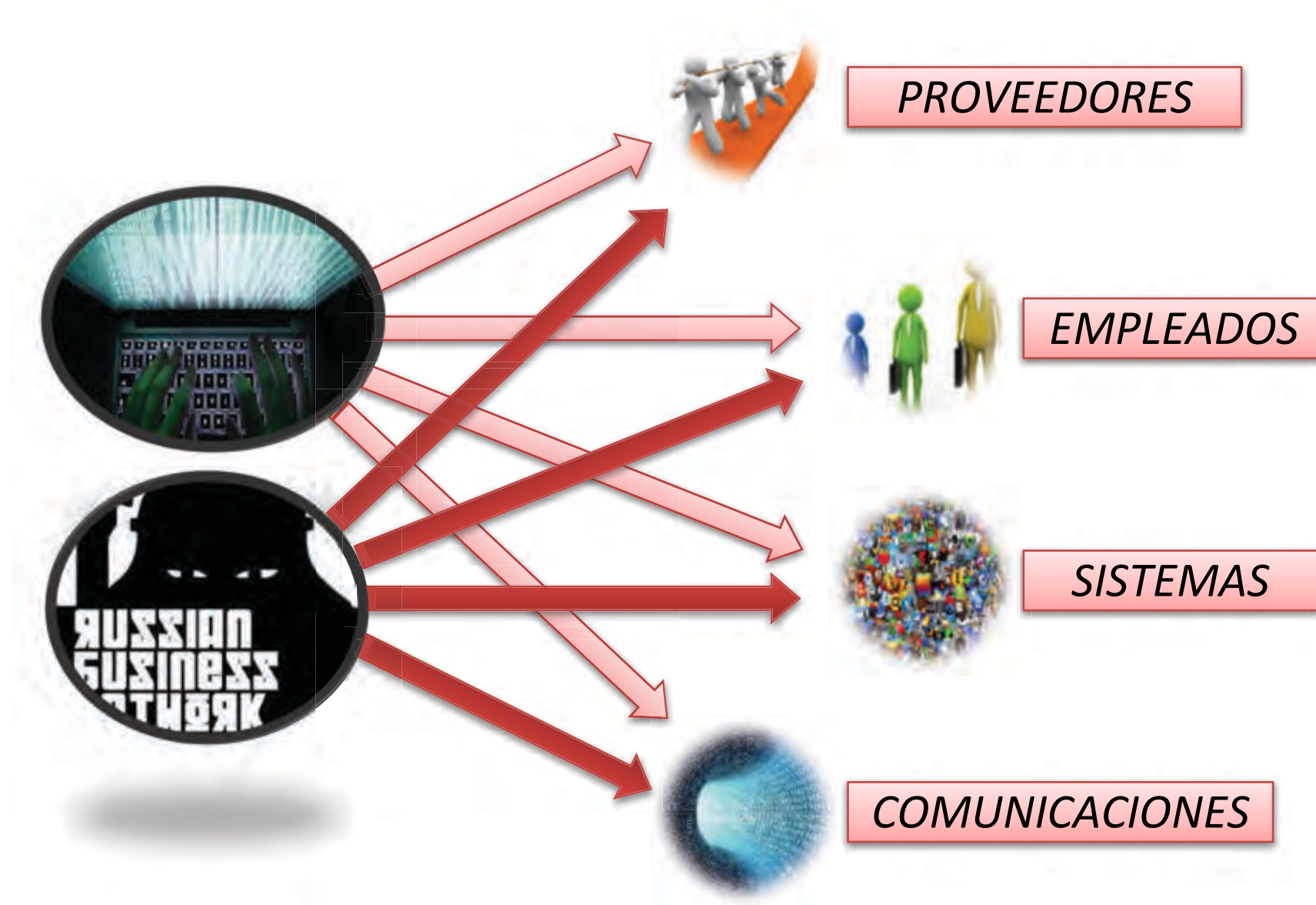
FINANCIADO POR GOBIERNOS.....NO SIEMPRE EJECUTADO POR ELLOS

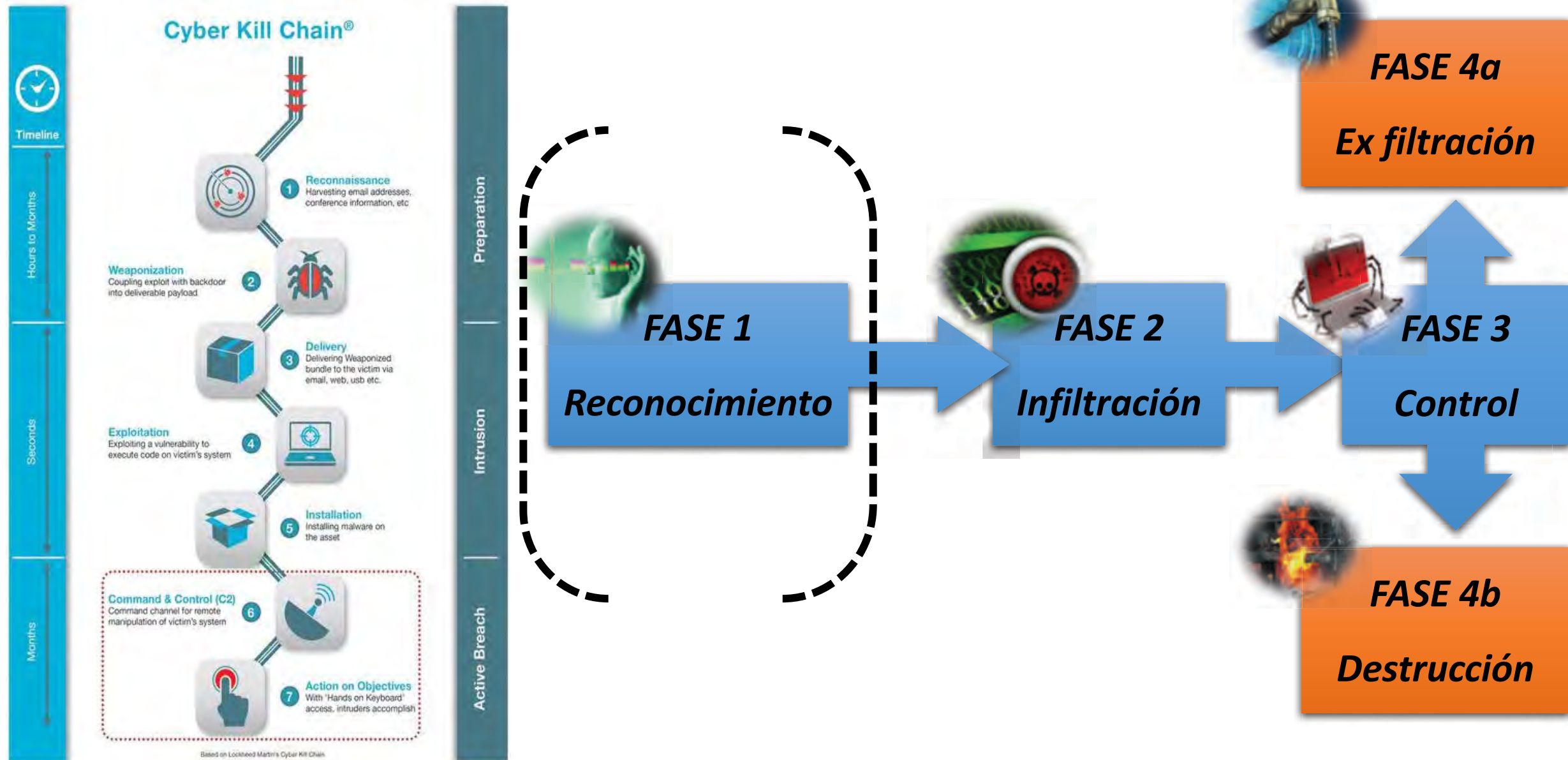


CENTRADO EN OBJETIVOS ESTRATEGICOS.... NO ECOMOMICOS

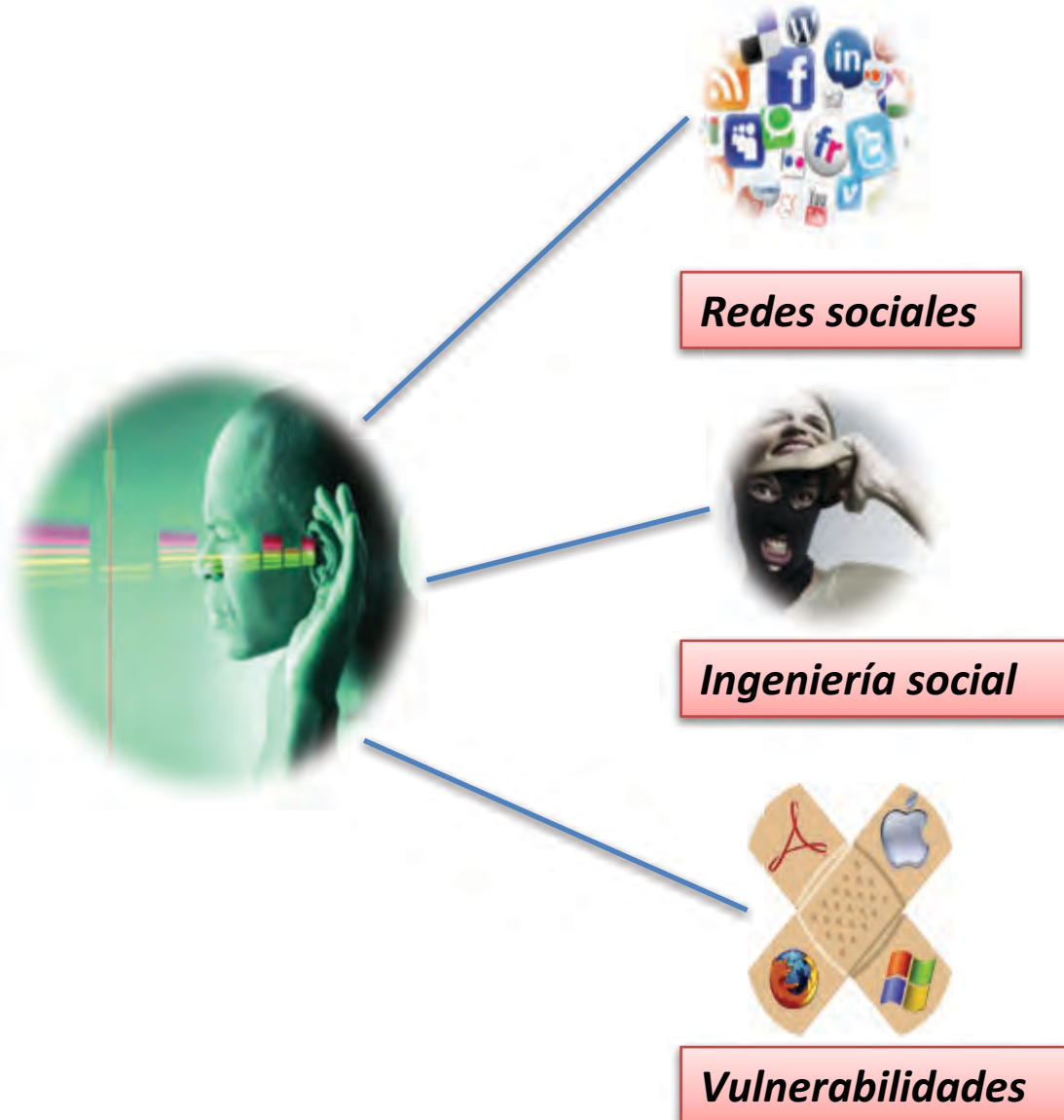


SIEMPRE HA EXISTIDO..... AHORA USAN INTERNET



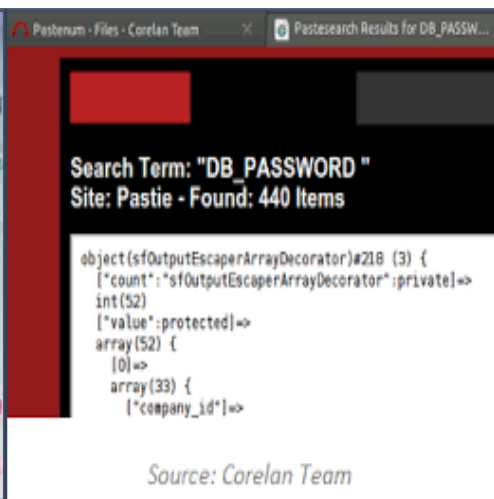


© **FASE 1 - RECONOCIMIENTO**

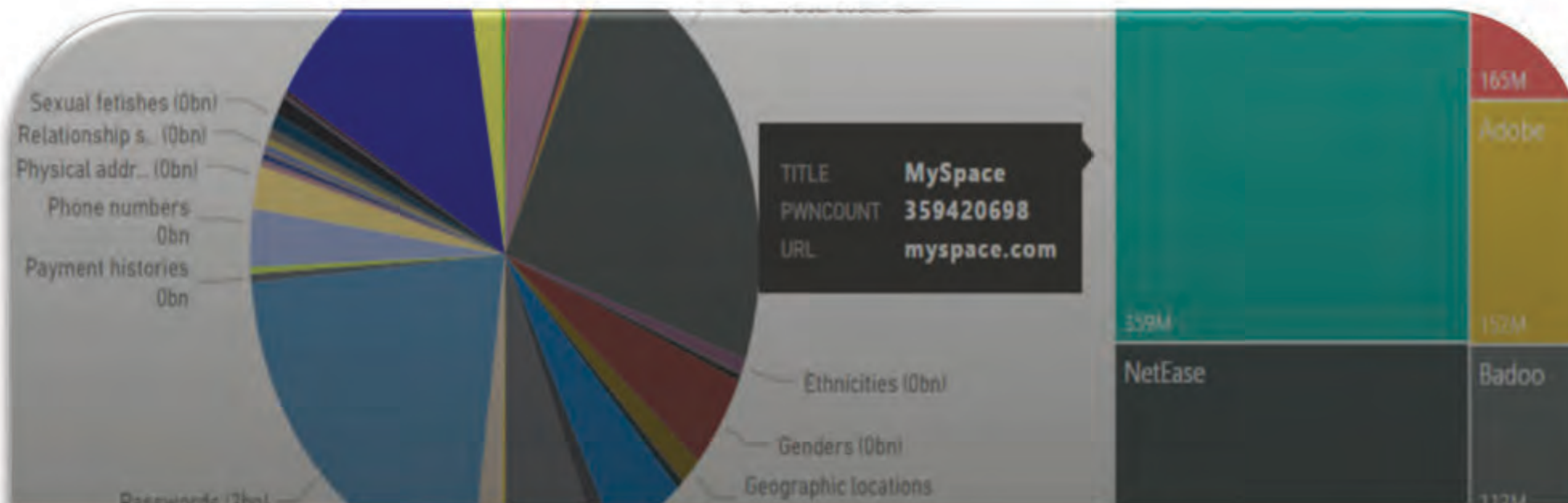


- Obtención de información del objetivo.
- Técnicas clásicas de recolección.
 - Detección de infraestructura.
 - Software/Hardware que posee.
 - Recolección emails.
 - Investigación focalizada a trabajadores departamento TI
- En algunos casos: desplazamiento a sedes empresa investigación WIFI (SIGINT)
- **Database leaks.**
- **SOCMINT**

© FASE 1 – RECONOCIMIENTO -> DATABASE LEAKS

				
Bases de datos de proveedores de servicios que han sido sustraídas y expuestas.	Sitios webs “especializados” en fugas de información ••HavelBeenPwned ••LeakedSource ••BreachAlarm	Sitios webs orientados a la publicación de información ••PasteBin ••AnonPaste ••WikiLeaks	Publicación de DataSets y "leaks" mediante Torrents	Uso de buscadores genéricos para obtener información: ••Por cuenta de correo electrónico/alias. ••Por dominio.

© FASE 1 – RECONOCIMIENTO -> ***DATABASE LEAKS***



Here's 1.4 billion records from Have I been pwned
for you to analyse

© **FASE 1 – RECONOCIMIENTO -> DATABASE LEAKS**



**EMAILS
CORPORATIVOS**



**CUENTAS EN SITES
PROFESIONALES**

StratForce - Importante en Intel
Webs trading - Importante para CFO



EXTRA....

Passwords
Teléfonos
Direcciones físicas

¿Qué podemos encontrar?

© FASE 1 – RECONOCIMIENTO -> **SOCMINT Social Media Intelligence**



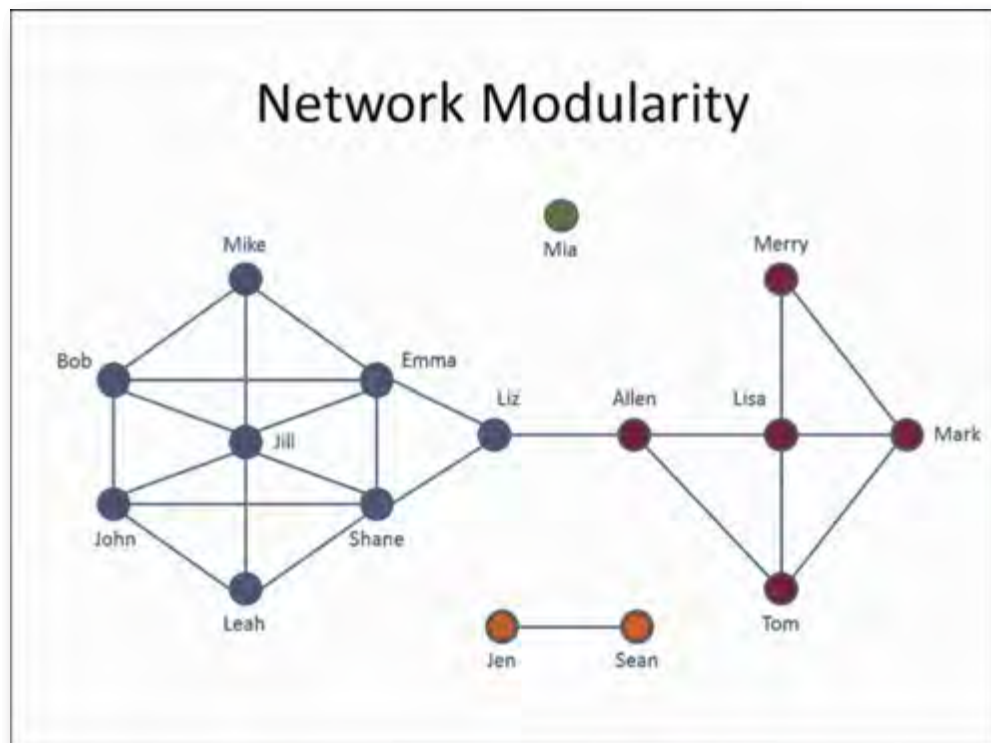
Obtención de información en redes sociales que, mediante su análisis, puedan producir inteligencia

Objetivo:

- Red estructurada de contactos.
- Red de comportamiento.
- ¿Quién dice qué, a quien, porqué canal y con que objetivo?.
- Se apoya en el SNA – Matemáticas discretas

© FASE 1 – RECONOCIMIENTO -> *Social Media Intelligence*

SOCMINT - SNA



Aplicando diversos algoritmos, detectar personal influyente.

Detección de “grupos” de personal de una empresa.

Conexiones entre esos grupos.

Existe multitud de software para realizarlo.

OJO, esto no es Big Data!

© FASE 1 – RECONOCIMIENTO -> ***SOCMINT Social Media Intelligence***



**Social Media
Intelligence**

....

¿Resultados?

Conocimiento de buscadores RRSS.

Cierta facilidad para obtener información a través de sistemas automatizados.

Apoyo de herramientas basadas en grafos.

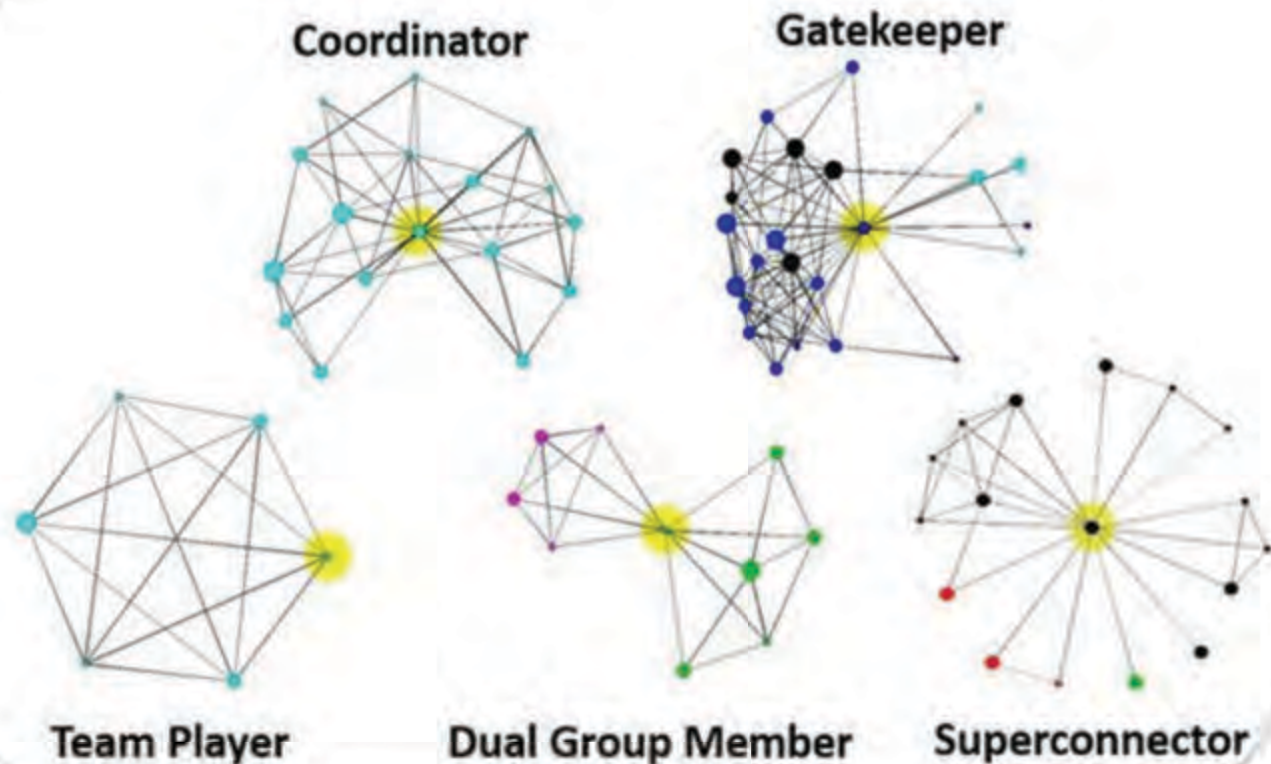
Permite la posibilidad de visualizar mucha información de forma fácil y clara.

Permite identificar a miembros clave de una organización.

© FASE 1 – RECONOCIMIENTO -> *Social Media Intelligence*



Un ejemplo real y conocido.....



Ataque RSA (año 2011, selección de objetivos)

Selección de empleados de bajo nivel, pero bien conectados con nivel de toma de decisiones Un conocimiento de la organización, permite maximizar la ventana de oportunidad.

© DATABASE LEAKS



Objetivo: Empresa servicio.es



DROPBOX LEAK => Hasta 60 cuentas asociadas al dominio *@servicio.es*

EL CONOCIMIENTO DE LA NOMENCLATURA DE LOS EMAILS PERMITE REALIZAR UN ESTUDIO DEL PERSONAL DE LA EMPRESA.

ASOCIACIÓN DE IDENTIDAD
cargo/responsabilidad -> email.

- Fuentes: prensa, noticias.
- LinkedIn.
- Facebook.

PATRÓN GENERACIÓN emails corporativos
Nombre+.+dos iniciales del primer apellido@servicio.es

© RECONOCIMIENTO -> NIVELES DIRECTIVOS



OBTENCIÓN EMAILS (LEAK O PREDICCIÓN)

Identificados 4 Miembros del Consejo de Administración

TODOS con perfil en FACEBOOK

Estudio de perfiles y relaciones

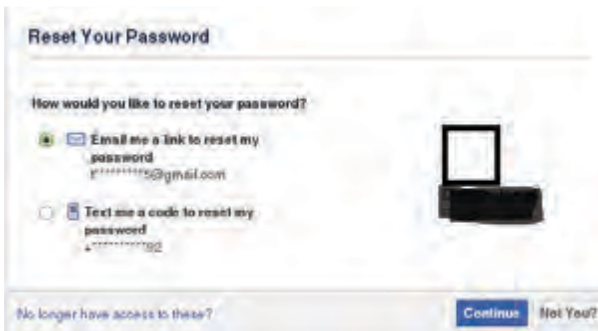
Identificado el CEO y el CFO

Obtención de información y relaciones familiares

Nuevos Perfiles para Analizar

Colegios/Universidades

Modelo Smartphone



© FASE 1 – RECONOCIMIENTO -> **FACEBOOK SEARCH TECHNIQUES**

Permite búsqueda dentro de los perfiles.

- Eventos/Sitios.
- Fotos subidas/comentadas/taggeadas.
- Grupos/likes.
- Amigos en común con otros perfiles y desde cuando, etc.

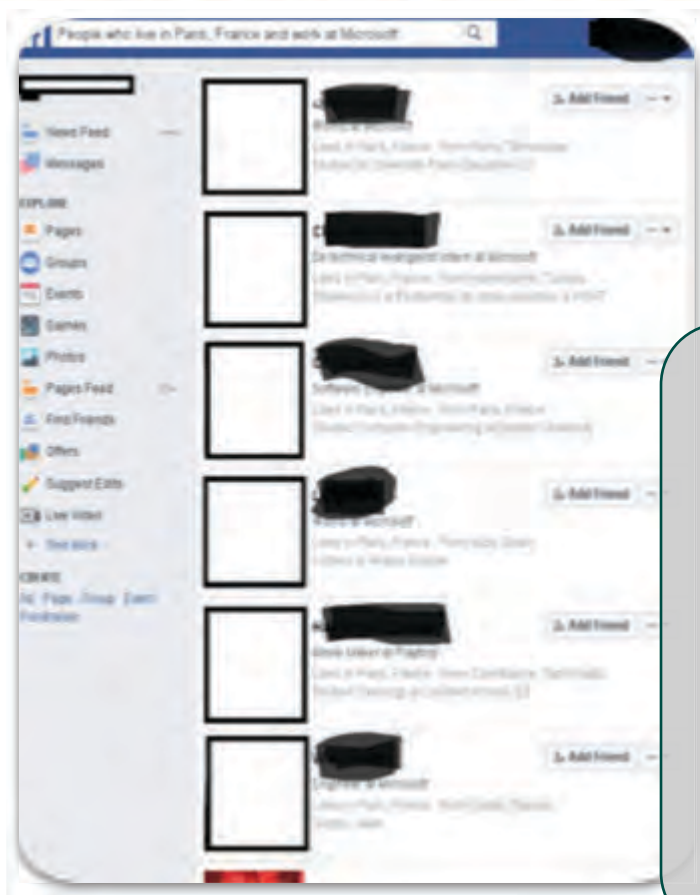
URL: www.facebook.com/search/FID/+query

Obtiene información incluso en perfiles que poseen configuración de privacidad alta.

Bajo ratio de detección de este tipo de prácticas por Facebook.

© **FACEBOOK SEARCH TECHNIQUES**

USO DE BÚSQUEDAS SEMÁNTICAS



- Personas **que trabajan** en servicio.es y viven en Madrid.
- Personas que viven en Madrid **con familiares que trabajan** en servicio.es.
- Personas que **han trabajado** en servicio.es
- Colegios donde **han estudiado** las personas **que trabajan** en servicio.es
- Las posibilidades son enormes

© RECONOCIMIENTO -> PLANTILLA DE SERVICIO.ES



Identificación de perfiles en redes sociales.
Las que mediante leaks pueden ser “vulnerables”.



Obtención de grupos de interés para la plantilla
Nuevos productos, ERE's, grupos genéricos de trabajadores, etc.



Canales de WhatsApp/Telegram (muy de actualidad)
Obtención de números de teléfono.
Genera una importante posibilidad de ataque.



Al tener este conocimiento, posibilidad de crear avatares para
obtención de información (Virtual HUMINT)



© RECONOCIMIENTO -> GRAFOS DE RELACIONES

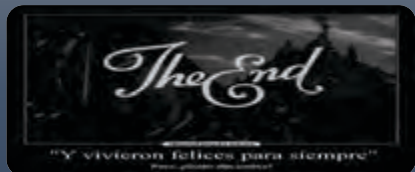


Red estructurada (contactos) y de comportamiento
Identificados los “C-Level members”, sus relaciones
personales/profesionales y si éstas son vulnerables

Señalados los trabajadores con servicios corporativos que pueden ser
accedidos, y su rol en la empresa/organización.

“Mapa interno” bastante completo, que genera nuevas oportunidades
para un atacante mediante ataques laterales.

© RECONOCIMIENTO -> NIVELES DIRECTIVOS



¿El Resultado? (AFAIK)

- Se localizó el perfil en RRSS de un familiar del CEO.
- Se simuló un email del un centro de estudios de este familiar al CEO, con un link especialmente diseñado.
- Y

© AUTOMATIZACION DEL PROCESO



PROS

- Sencillo de automatizar y mantener (python+selenium+db+db_grafos)
- Herramientas de análisis “free” (NodeXL, Netdraw, Gephy, etc.).
- Generación de inteligencia y conocimiento.
- Baja probabilidad de ser detectado.
- Facebook de vez en cuando actualiza sus medidas de privacidad.
 - Pero **no** avisa al usuario de que está siendo objeto de estas actividades.



CONTRAS

- Es un **abuse** del servicio (pero eso al “malo” le da igual).
- Facebook de vez en cuando actualiza sus medidas de privacidad.
 - Pero **no** avisa al usuario de que está siendo objeto de estas actividades.
- Hace falta un analista experto en SNA (“Social Network Analysis”).



CONTRAMEDIDAS

© **RECOMENDACIONES Y PROCEDIMIENTOS**

- Evitar patrones y estructuras regulares en la generación de correos o id's. *Especialmente en altos directivos*

**EVITAR
PATRONES
RECONOCIBLES**

- Incorporar a los sistemas de alerta temprana la detección y análisis datos "robados". *Especialmente los NO relacionados con la entidad*

**REVISAR
PUBLICACIONES
DE "LEAKS"**

- Si se detectan cuentas comprometidas..... Utilizarlas como señuelos para identificar posibles "atacantes"

**LEAK
=
OPORTUNIDAD**



© CONTRAMEDIDAS Y REACCIÓN

**CREACIÓN
PERFILES
ATRATIVOS**

- *Mediante una biografía y un timeline especialmente diseñado, se insertan links controlados y auditados.*

**MANTENER
PERFILES
“SEÑUELO”**

- *Los avatares deben ser **atractivos y sostenibles**. Además deben actualizarse de forma regular con datos “creíbles”.*

**CONTROL DE
“VISITANTES”**

- *Se debe disponer de un sistema que monitorice: IP's, SO's, UserAgent, Plugins,...etc.*



Honeypot

© **CUANDO TODO LO DEMÁS FALLE.....**



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

