

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Ciberdelincuencia Organizada

Caso Práctico: Inteligencia económica, o como “perder”
proyectos internacionales



Teniente Coronel
Juan Antonio
Rodriguez Alvarez De Sotomayor

**Jefe del Departamento de Delitos
Telemáticos.**

Unidad Central Operativa (UCO)

GUARDIA CIVIL

jsotomayor@guardiacivil.es

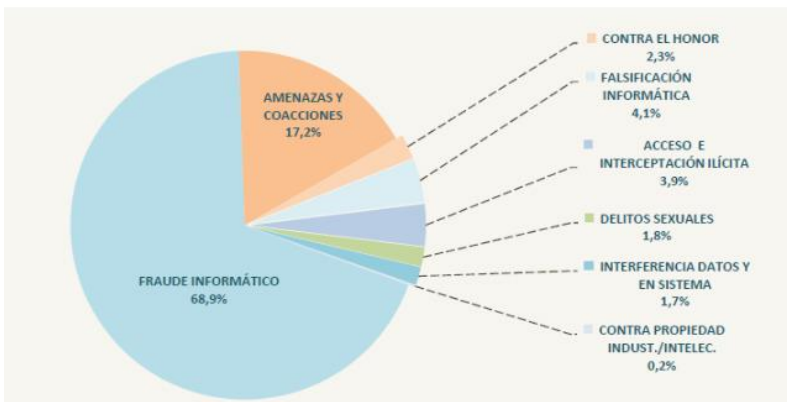


CIBER DELINCUENCIA ORGANIZADA

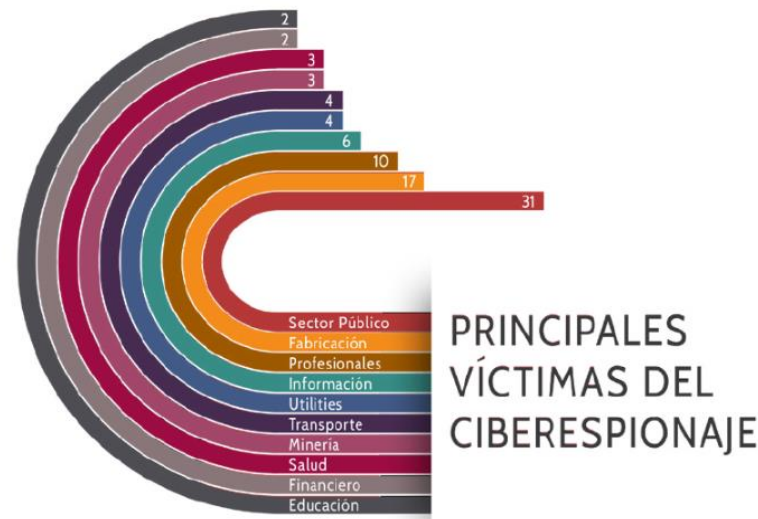
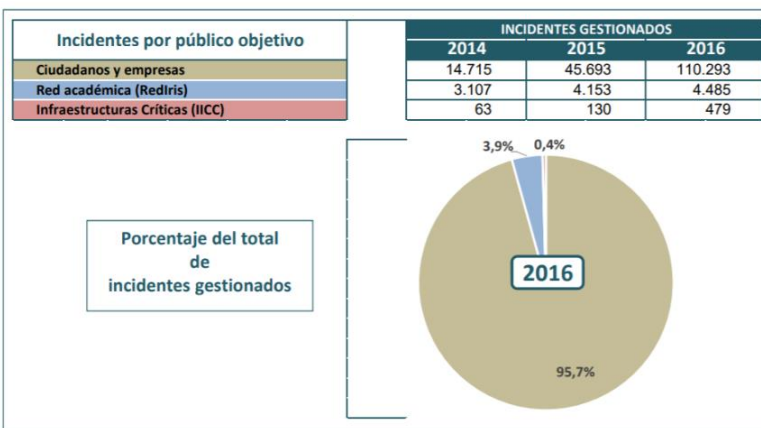
AMENAZA CON ENTIDAD PROPIA



HECHOS CONOCIDOS	2013	2014	2015	2016
ACCESO E INTERCEPCIÓN ILÍCITA	1.805	1.851	2.386	2.579
AMENAZAS Y COACCIONES	9.064	9.559	10.112	11.473
CONTRA EL HONOR	1.963	2.212	2.131	1.524
CONTRA PROPIEDAD INDUST./INTELEC.	172	183	167	121
DELITOS SEXUALES	768	974	1.233	1.188
FALSIFICACIÓN INFORMÁTICA	1.608	1.874	2.361	2.697
FRAUDE INFORMÁTICO	26.664	32.842	40.864	45.894
INTERFERENCIA DATOS Y EN SISTEMA	359	440	900	1.110
Total HECHOS CONOCIDOS	42.403	49.935	60.154	66.586



INSTITUTO NACIONAL DE CIBERSEGURIDAD





CIBER DELINCUENCIA ORGANIZADA

AMENAZA CON ENTIDAD PROPIA

CARÁCTER PRIORITARIO DE ACTUACIÓN

Agenda Europea de Seguridad (2017-2020)

Dentro de las líneas estratégicas de AES, el **cibercrimen** es identificado por la Comisión Europea como una de las tres principales amenazas, **junto al terrorismo y el crimen organizado**, otorgándole un **carácter prioritario de actuación**, para afrontar dichas amenazas se hace necesario una **actuación de forma inmediata** [...]



Internal Security Fund - Police

Call for proposals document

Cybercrime and child sexual exploitation

ISFP-2017-AG-CYBER

Version 1.0
23 November 2017

4.1. COUNTER TERRORISM

4.2. ORGANISED CRIME

4.3. CYBERCRIME

In line with the objective of **ensuring a high level of security in the Union in accordance with the priorities identified in relevant Union strategies, policy cycles, programmes, threat and risk assessments** covered by this budget line, this work programme contains the actions to be financed and the budget breakdown for year 2017 as follows:

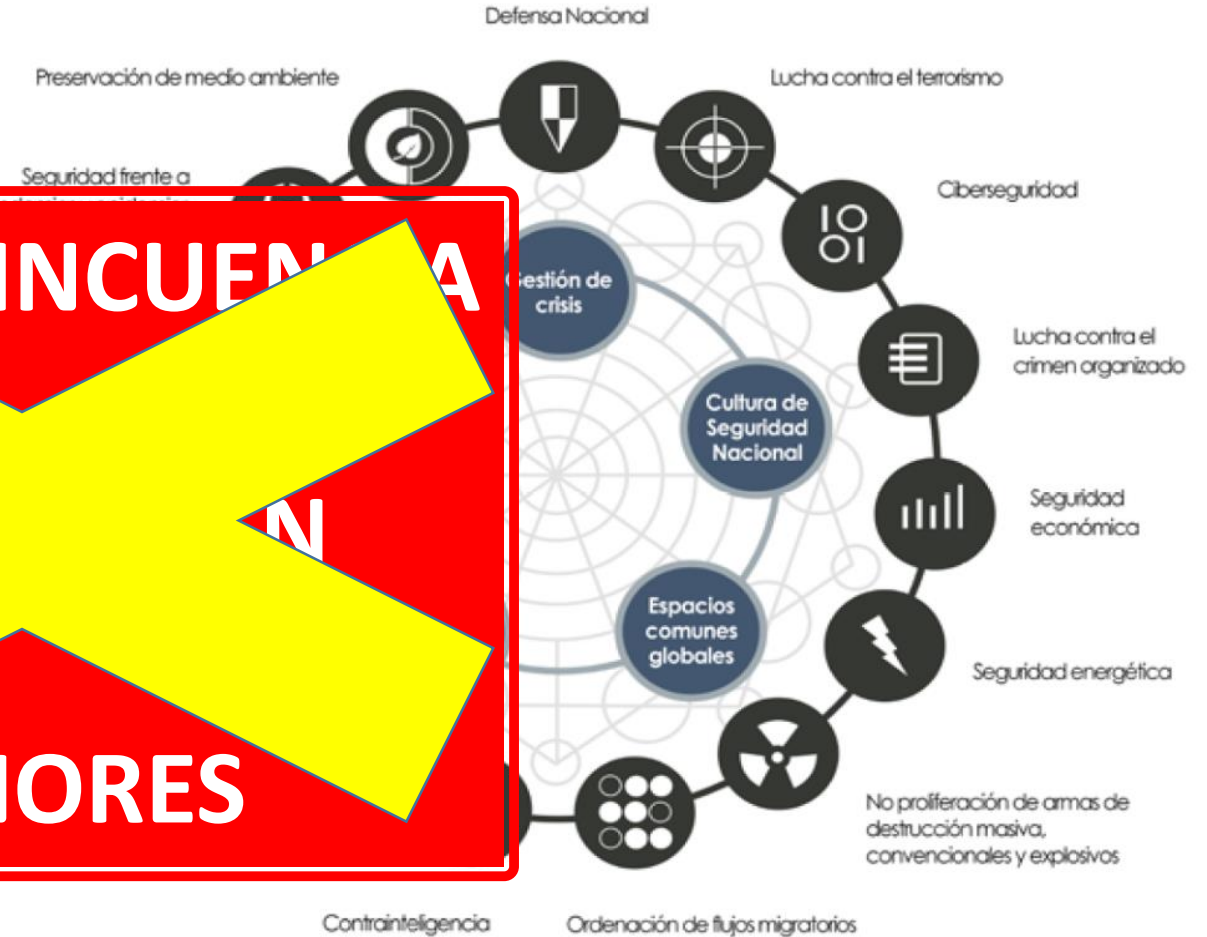
Procedures	Amount	Co-financing rate	Planning
Open Calls for Proposals:	8 000 000 €	90%	Q4
Restricted Calls for Proposals:	0 €	N/A	N/A
Direct Awards:	0 €	N/A	N/A
Other:	0 €	N/A	N/A
TOTAL:	8 000 000 €		

ESTRATEGIA DE SEGURIDAD NACIONAL

2017



UN PROYECTO
DE TODOS Y





CIBER DELINCUENCIA ORGANIZADA

AMENAZA CON ENTIDAD PROPIA

CASO PRÁCTICO

Comienzo ...

El 76% del PIB español se genera fuera de nuestras fronteras.

Las empresas españolas cada día tienen más presencia internacional.

Sectores:

- Ingeniería.
- Banca.
- Telecomunicaciones.

Esto es una historia real...que le puede suceder a cualquiera

Empresa española X del ramo de la ingeniería se presenta para oferta en país del Medio Oriente (XXX).

Proyecto de XXX millones de euros.

Ofertan una pluralidad de compañías de varios países.

- ☐ Francia.
- ☐ Estados Unidos.
- ☐ Inglaterra.
- ☐ España



El mundo real funciona así..

Una vez se resuelve el concurso, la licitación la gana una empresa de un país europeo (Fr...)

Tras levantar las sospechas de la empresa española, ésta solicita una investigación interna al objeto de conocer si pudo haber fugas de información.

Lo que viene a continuación es fruto de las pesquisas realizadas.
(XXXX)

Comenzamos..

La empresa española posee una oficina comercial en dicho país.

Se compone por personal mixto.

Su misión:

Networking.

Operativa comercial.

Entrega de ofertas.

Selección de partners.

Etc.

El competidor

Objetivo: Obtención del pliego de la compañía española.

Medios: Los necesarios para culminar el objetivo.

Fuentes:

- Obtención técnica.
- Obtención humana.

Tiempo estimado: Tres meses.

Primeros pasos

- Recolección de información a través de redes sociales.

Perfiles de LINKEDIN de ex trabajadores.
Se contacta con ellos bajo la cobertura de
querer cambiar de proyecto y preguntar sobre
la empresa española.
Se trabaja perfiles de ingenieros.

Perfiles de LINKEDIN de trabajadores actuales.
“Abierto a nuevas oportunidades”.
Se contacta por dos vías:

1. Empresas de selección de trabajadores, haciendo una primera entrevista por Skype.
2. Trabajadores de empresas que piden referencias para concursar en alguna plaza abierta por la empresa española.

P.D: La cobertura usada es una empresa de selección de personal.



Hasta aquí

Se ha obtenido:

- La gente que trabaja en el proyecto (dicho por trabajadores).
- Los problemas de la empresa a nivel trabajador.
- Las personas clave dentro de la empresa (RRHH).
- Personal que está relacionado directamente con la oficina en ese país.

Operativamente:

- Dos trabajadores de la citada empresa que están dispuestos a cambiar de empresa (tras la entrevista de trabajo).

El “ataque”

A esos dos trabajadores se les envía un email, que dirige a una web donde deben complementar cierta información.

El formulario descargar un documento de Word con la copia de dicho formulario.

Se les envía a dos direcciones: la suya personal y la corporativa.

Los trabajadores lo rellenan y obviamente interactúan con el documento de Word.

El documento word

Ejecuta una macro, que descargará un binario

Ese binario se ejecuta, obteniendo acceso a su equipo.

Payload muy sencillo.

Funciones de keylogger.

Pivotando por la empresa

Una vez infectados, lo que se hace es pivotar por la empresa.

Al conocer los nombres internos y demás de la empresa, pueden conectarse a la oficina de ese país.

Se infecta al responsable de la oficina.

Se obtiene la oferta.

El cierre

Los dos trabajadores hacen una tercera entrevista, donde NO son seleccionados.

Los headhunters cierran los perfiles.

Se elimina cualquier rastro del binario.

La empresa lo descubre y..

Se detectan fallos en:

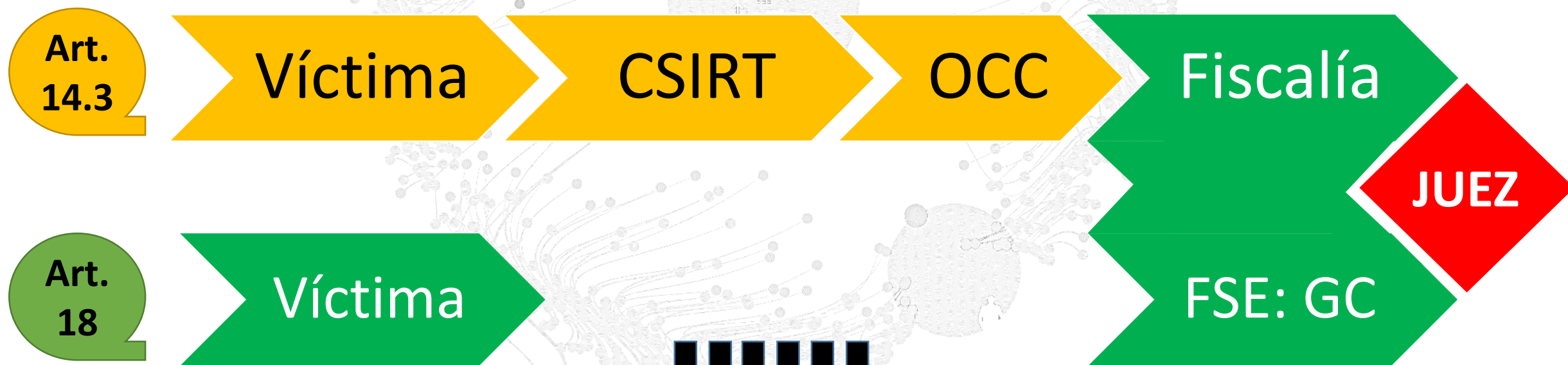
- Nadie había previsto esta situación.
- Fallan controles internos de seguridad.
- Fallan controles de monitorización en redes sociales.
 - ❑ No se dispone de ningún perfil tipo “honeypot”.
- No existen sistemas DLP.

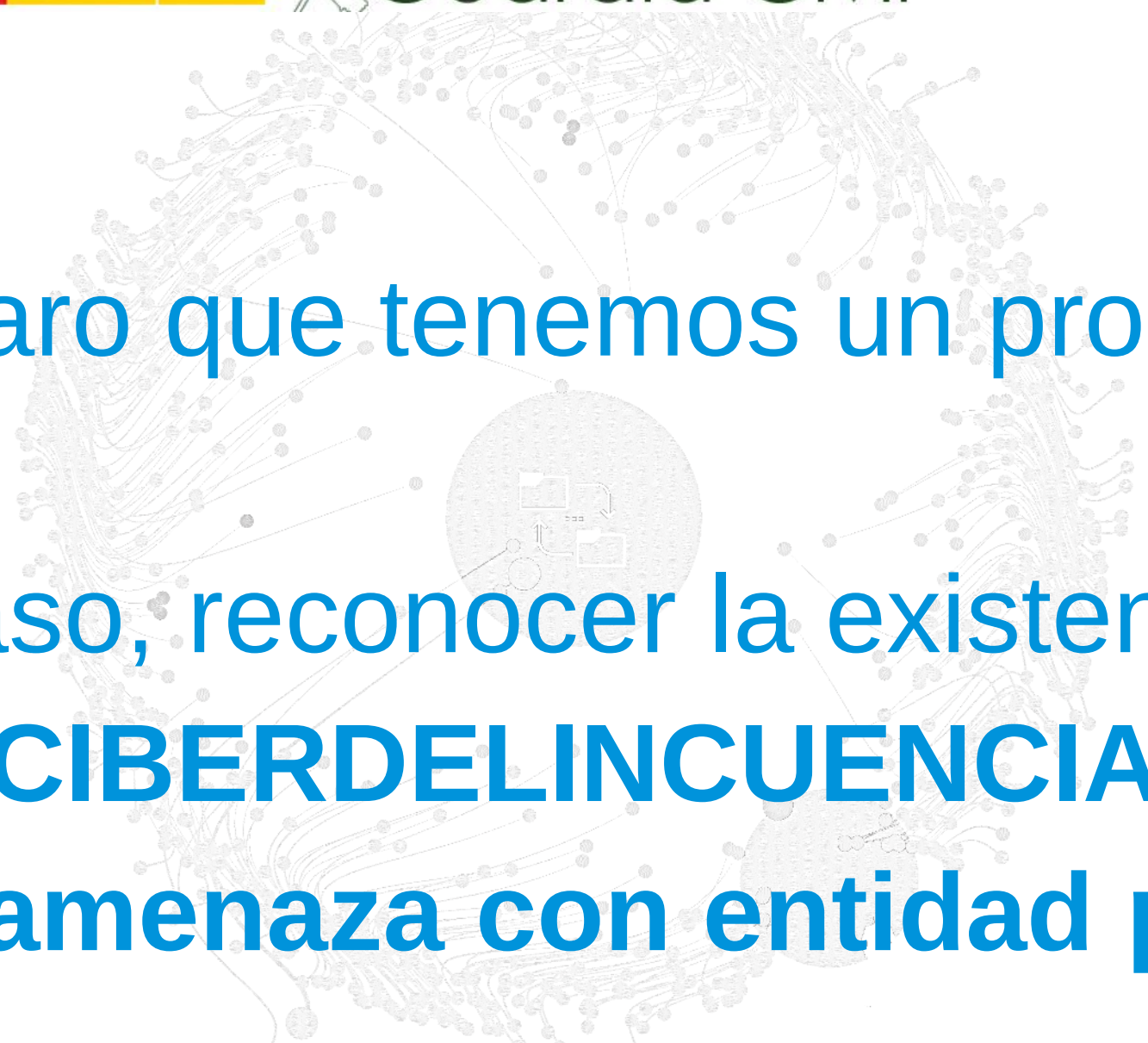
Y ahora ¿qué?.

- ¿Se denuncia?, de denunciarlo ¿Dónde se denuncia?.
- ¿las autoridades españolas?

Denuncia ..

Anteproyecto de ley sobre la seguridad en las redes y sistemas de información:





Esta claro que tenemos un problema

Primer paso, reconocer la existencia de la

CIBERDELINCUENCIA

como amenaza con entidad propia



Para poder luchar eficazmente contra la CIBERDELINCUENCIA:

Denunciar → **Lo que no se conoce no existe.**

No se le otorga la importancia que tiene.

No se proveen de los recursos necesarios.

No permite participar en proyectos financiados por UE.

Importante la confianza en las unidades policiales.



**¡Muchas gracias
por su atención!**

delitostelematicos@guardiacivil.es
www.gdt.guardiacivil.es

➤ 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

