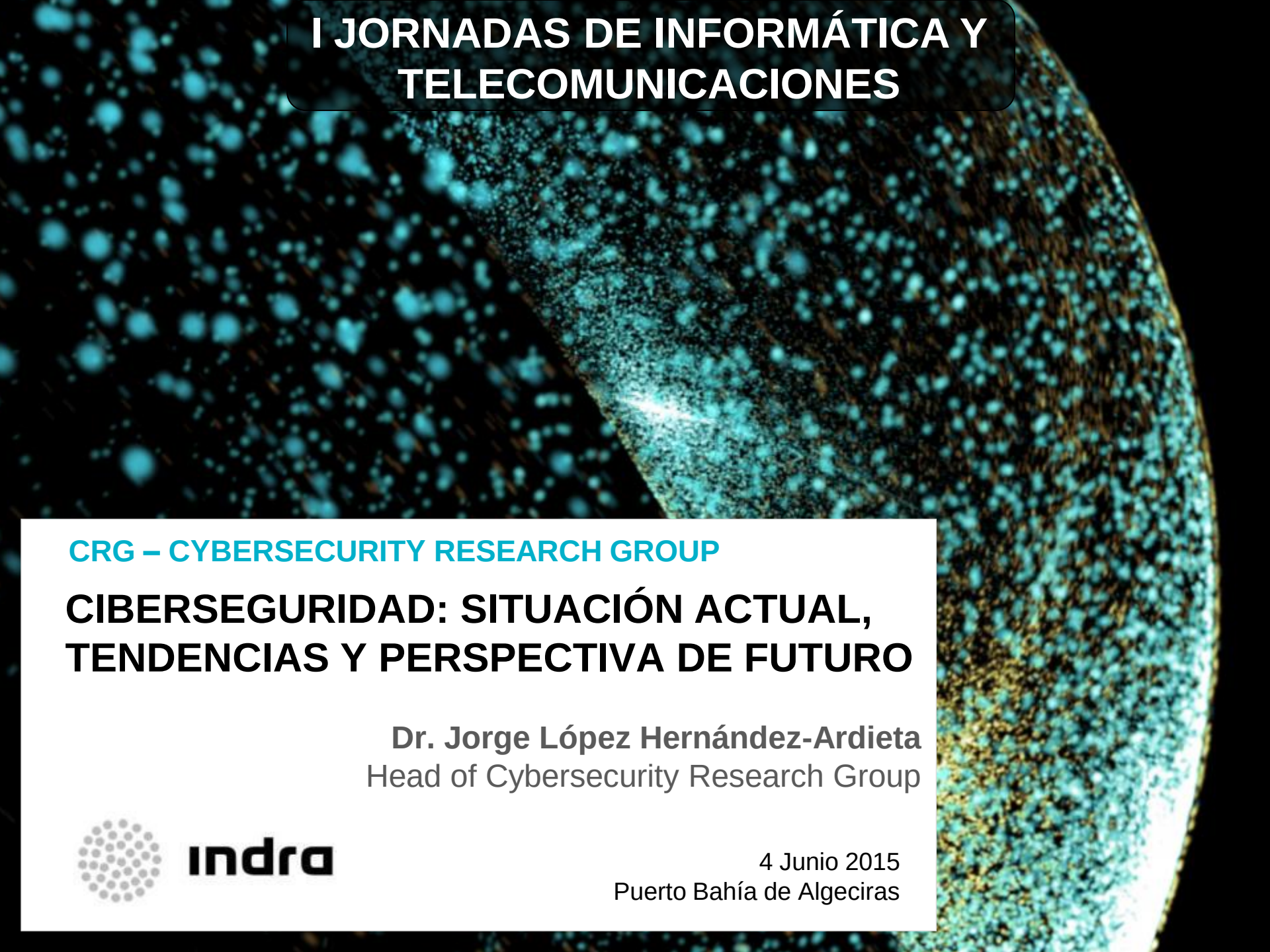


# I JORNADAS DE INFORMÁTICA Y TELECOMUNICACIONES

CRG – CYBERSECURITY RESEARCH GROUP

# CIBERSEGURIDAD: SITUACIÓN ACTUAL, TENDENCIAS Y PERSPECTIVA DE FUTURO

**Dr. Jorge López Hernández-Ardieta**
Head of Cybersecurity Research Group

indra

4 Junio 2015
Puerto Bahía de Algeciras

# ÍNDICE



indra

# QUIENES SOMOS

**MULTINACIONAL LÍDER EN CONSULTORÍA Y TECNOLOGÍA**


## Soluciones y tecnología propia

**I+D: 6-8%ventas**

## Modelp de negocio diferencial basado en la INNOVACIÓN

**VENTAS: 3.000 M€**

**PROFESIONALES: 43.000**

**PAÍSES: 149**

# INNOVACIÓN Y+


**+190**
universidades y centros de investigación
(68 ámbito internacional)

## Innovación y sostenibilidad

**9 años**
Presente en el Dow Jones Sustainability Indices 9 años consecutivos

MEMBER OF
Dow Jones Sustainability Indices
In Collaboration with RobecoSAM

**I+D+i**
Una de las primeras compañías Europeas en Inversión en I+D+i

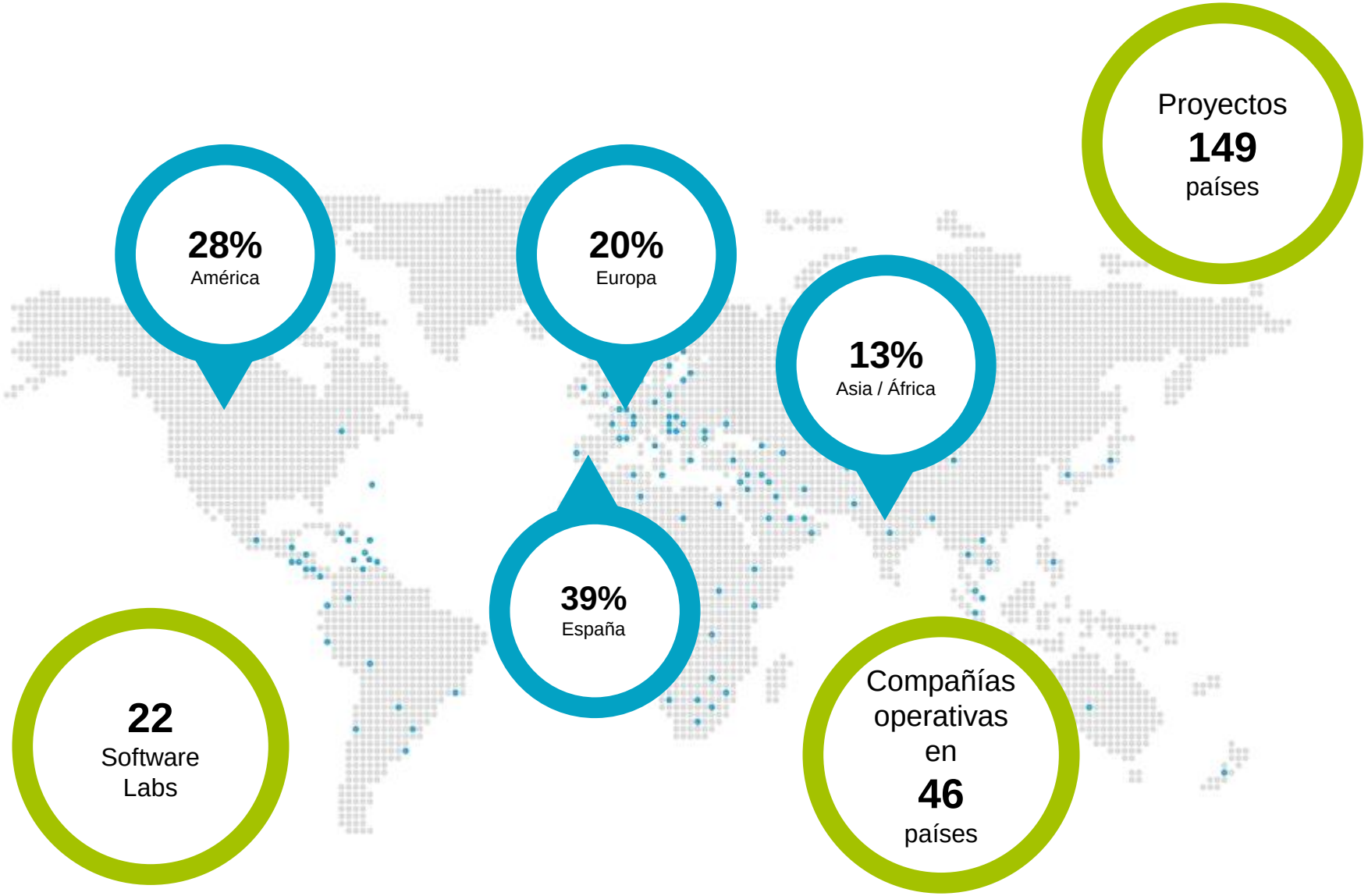
# TALENTO GLOBAL

**43.000** profesionales

**77% Personal** titulado y de **Alta** cualificación

**97** nacionalidades

# PRESENCIA GLOBAL



# NUESTRA ACTIVIDAD

## Oferta

**64%**

**SOLUCIONES**

**Pensar & Construir**

- Consultoría
- Soluciones Tecnológicas

**36%**

**SERVICIOS**

**Operar**

- IT Outsourcing
- BPO

## Sectores

Energía e Industria **16%**

Servicios Financieros **17%**

AA.PP. y Sanidad **18%**

Telecom y Media **11%**

Transporte y Tráfico **21%**

Seguridad y Defensa **17%**

# ÍNDICE



indra

# EL CIBERESPACIO

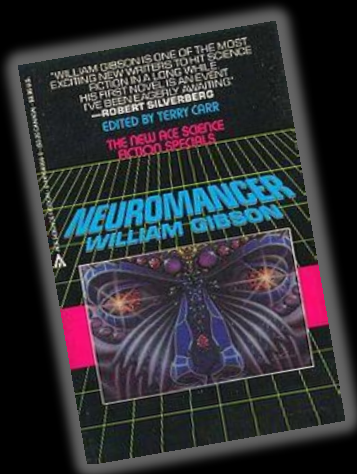
El uso común se refiere a los **sistemas de información y proceso de datos interconectados por redes de comunicaciones**

¿qué es?

La palabra proviene del griego cibernético (κυβερνήτης) - “piloto” o “timón” usado por el matemático Norbert Wiener para describir la tecnología de sistemas de control

RAE
“Ámbito artificial creado por medios informáticos”

La primera vez que se utilizó el término CIBERESPACIO fue en el libro Neuromancer (1984) de William Gibbson para denominar a Matrix, el entorno virtual de sus novelas.



# ASPECTOS CLAVE

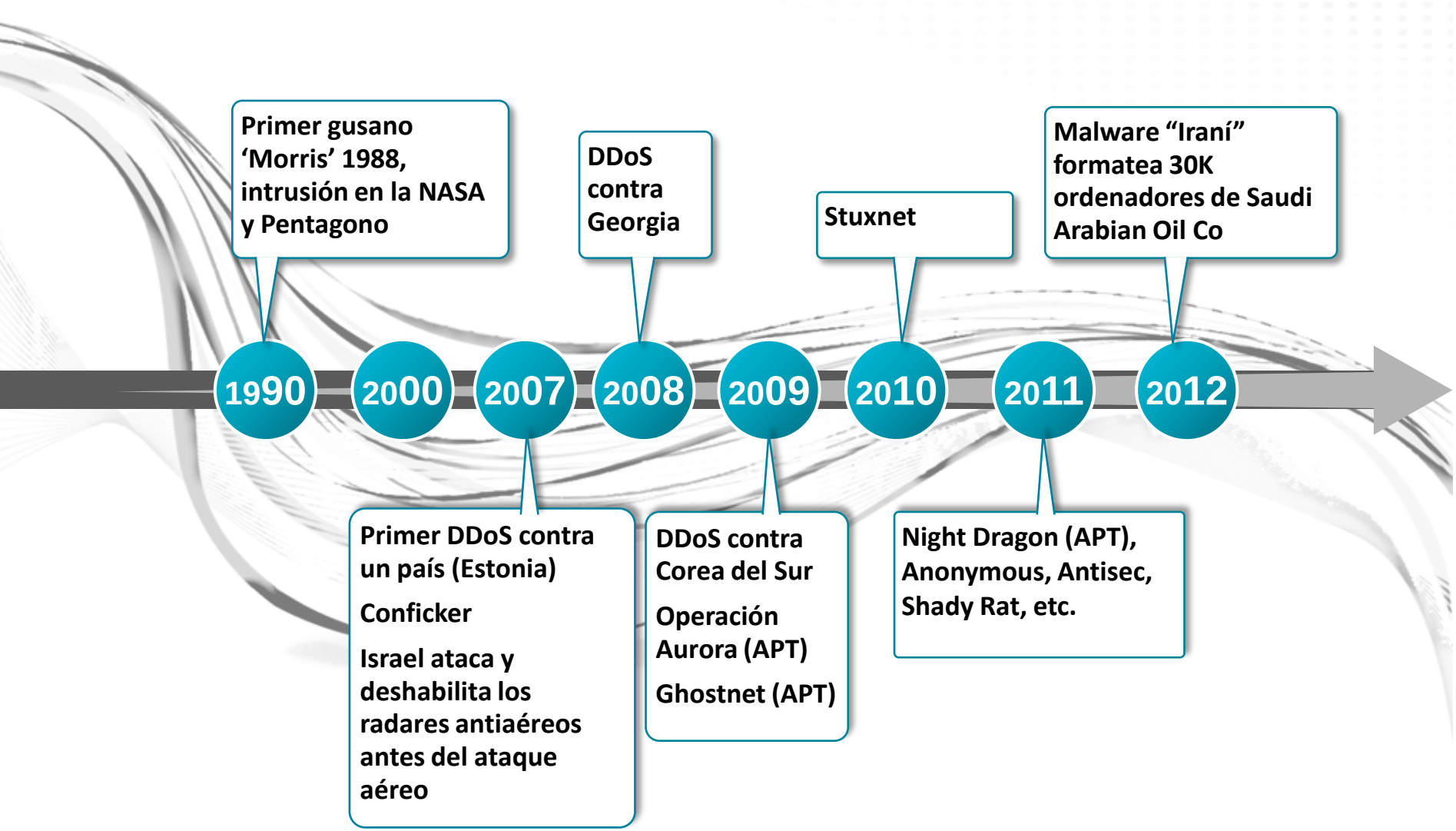
**La evolución tecnológica y los nuevos paradigmas (Ciudades Inteligentes, modernización y apertura de IICC, IoT, Sistemas no tripulados, BYOX, Big Data, etc.) han propiciado la aparición de nuevas amenazas y retos en la defensa del ciberespacio**

## INTERDEPENDENCIA E INTERCONEXIÓN ENTRE SISTEMAS, OBJETOS, PERSONAS

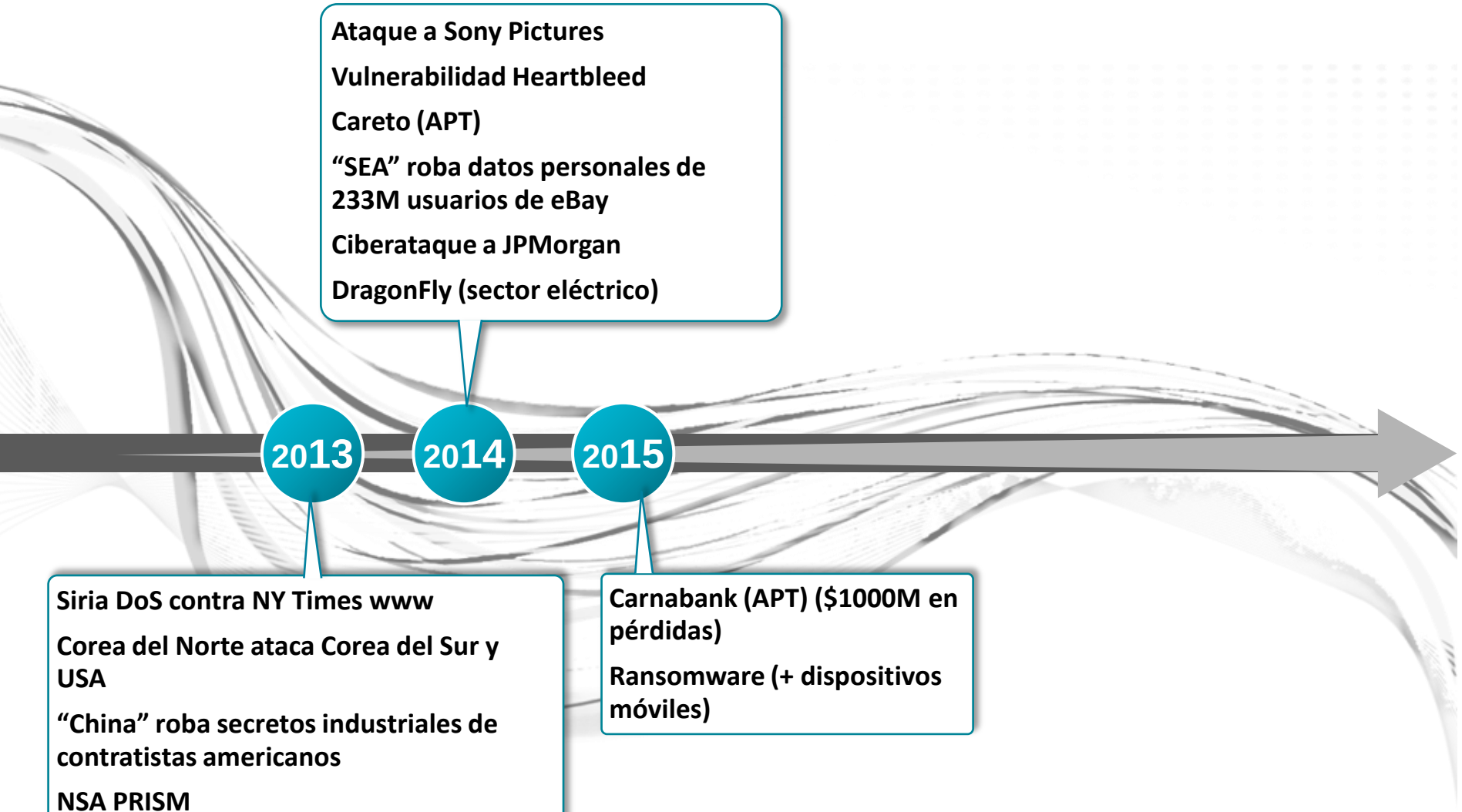

## COMPLEJIDAD CRECIENTE DE LA TECNOLOGÍA

## EVOLUCIÓN DE LAS AMENAZAS

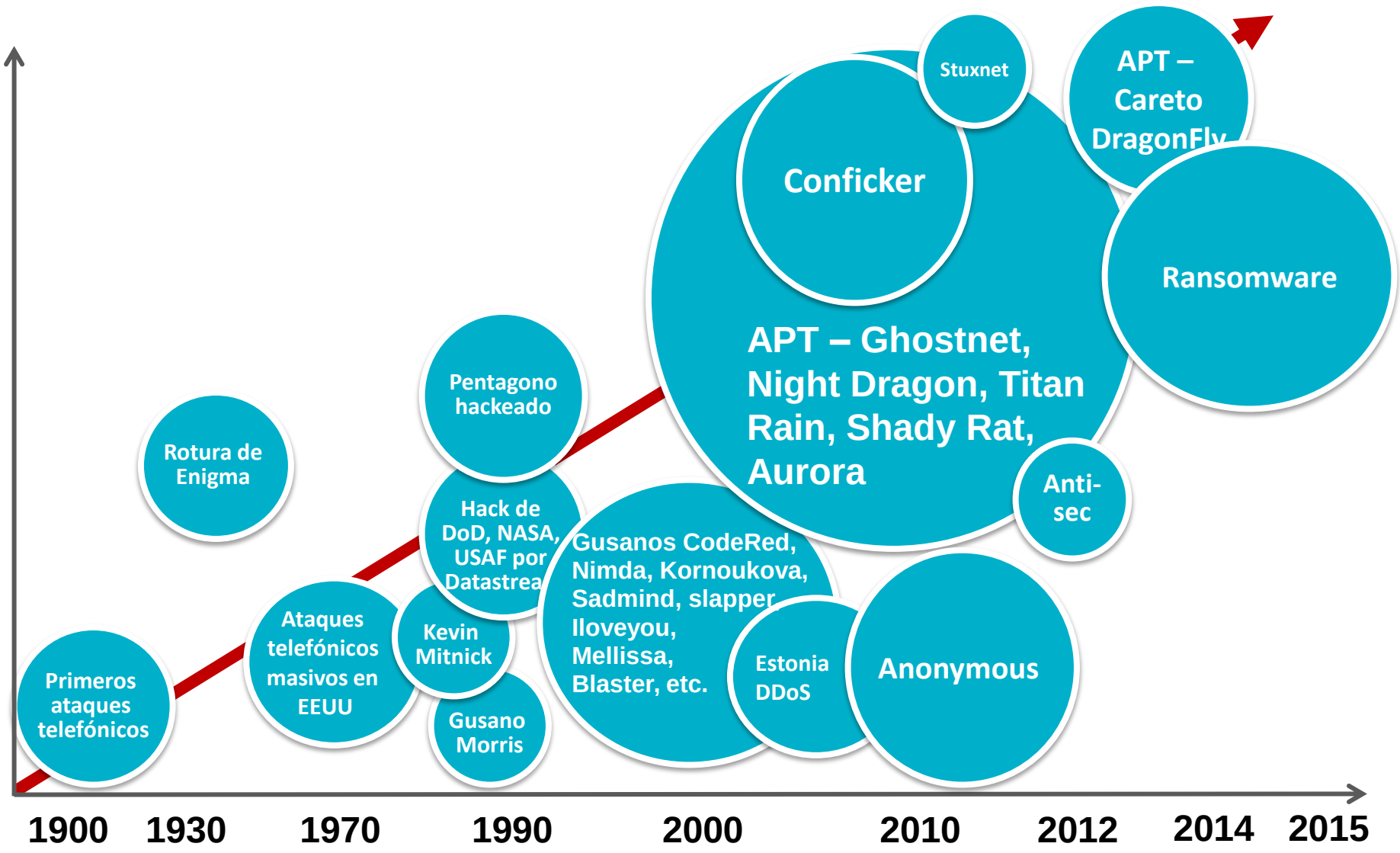
# CRONOLOGÍA DE CIBERATAQUES (RELEVANTES)



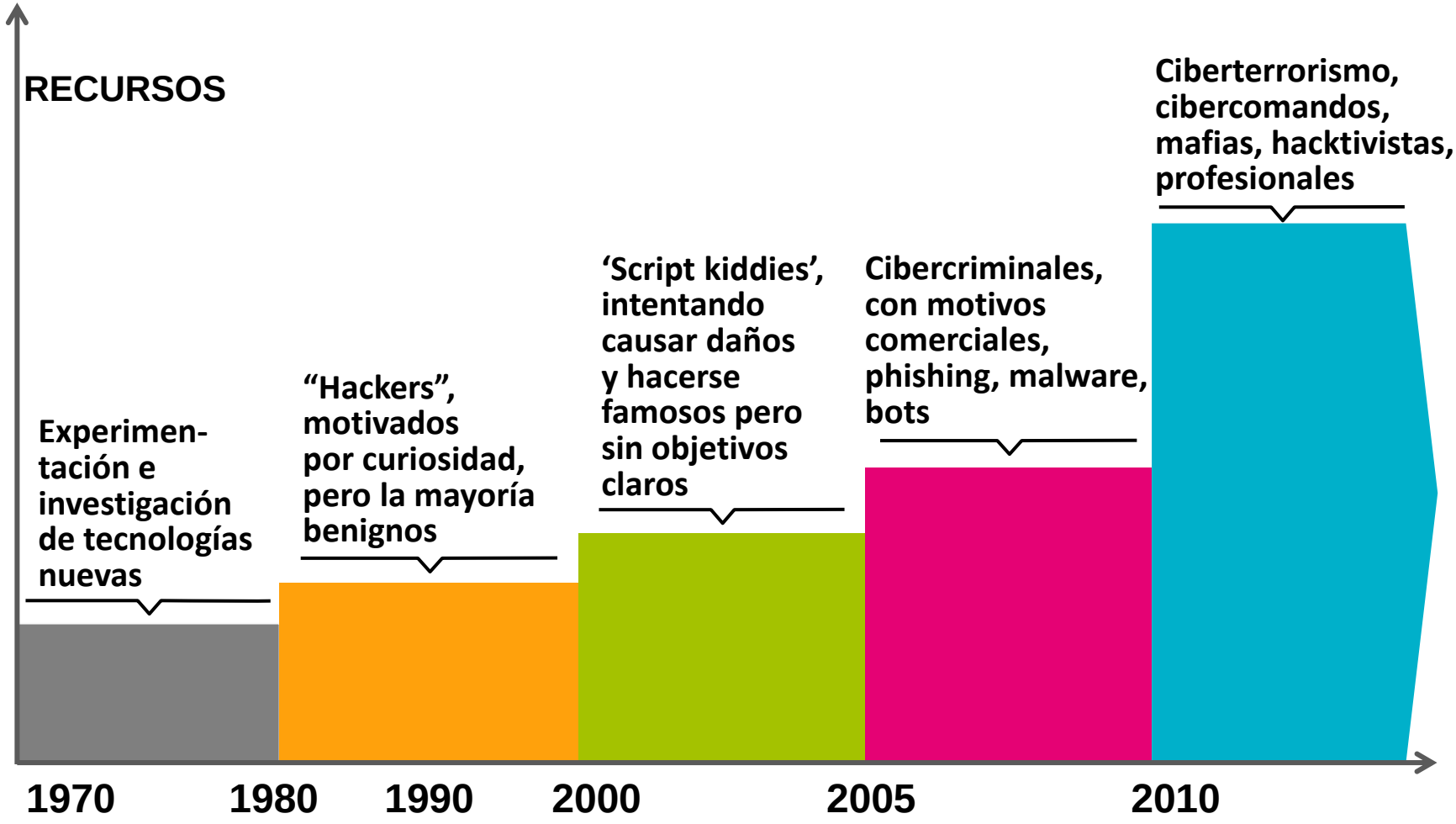
# CRONOLOGÍA DE CIBERATAQUES (RELEVANTES)



# INCREMENTO EN LA SOFISTICACIÓN E IMPACTO DE LOS CIBERATAQUES



# EVOLUCIÓN DE LA AMENAZA



# CIBERATAQUES NOTORIOS

## World nuclear facilities vulnerable to cyber-attack

Author: ATAdmin | June 1, 2015

Asia Times News & Features | cyber attack, nuclear

## FBI director fears ISIS could launch cyber attack against U.S.

POSTED 2:34 PM, MAY 21, 2015, BY SHELLIE NELSON

FACEBOOK 37 TWITTER 25 GOOGLE PINTEREST LINKEDIN 43 EMAIL

(CNN) — ISIS is "waking up" to the idea of using sophisticated malware to cyber-attack critical infrastructure in the U.S., FBI Director James Comey said Wednesday, May 20, 2015.

"Logic tells me it's coming," and that the terror group is "looking into" whether it is capable of pulling off such attacks, Comey said at the Cybersecurity Law Institute at Georgetown University.

An ISIS fighter, who speaks perfect English with a North American accent, is shown orchestrating the mass execution of a group of men in an ISIS recruitment video called "Flames of War". (photo from video posted online by the FBI)

# CAMBIO EN LA DOCTRINA MILITAR

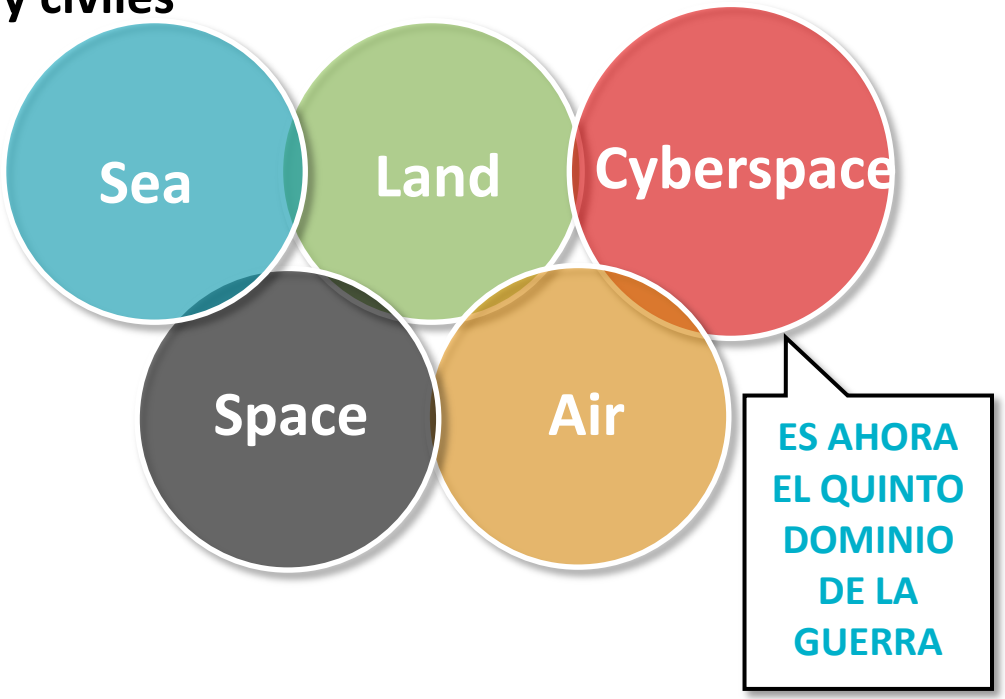
**Muchas naciones han declarado el ciberespacio como 5º dominio de la guerra, a la luz del incremento de ataques con gran impacto a redes militares y civiles**

SEGURIDAD | España

## Defensa crea el Mando Conjunto de Ciberdefensa frente a las 'ciberamenazas'

Efe | Madrid
Actualizado martes 26/02/2013 **13:19 horas**

El Ministerio de Defensa ha creado el **Mando Conjunto de Ciberdefensa**, que dirigirá y coordinará las acciones de las Fuerzas Armadas frente a los 'ciberataques', **"una amenaza actual, real y en crecimiento para los intereses nacionales"**.




**Gobiernos y organizaciones internacionales, incluyendo la OTAN, han creado unidades especializadas de ciberdefensa para proteger los activos críticos del país y responder activamente a la amenaza**

# PROPIEDADES DE LOS CIBERCONFLICTOS

- El ciberespacio presenta situaciones impredecibles y en constante evolución
- Los ciberconflictos exigen respuestas inmediatas (tiempo real)
- Una mala decisión puede tener consecuencias severas para los intereses del país y sus ciudadanos
- Las cantidades ingentes de datos requieren constante procesamiento y refinamiento
- La cooperación con aliados es clave para el éxito, pero complica las operaciones
- El adversario juega un papel activo, pero la atribución del ataque es complejo

# ÍNDICE



indra

# RIESGOS EN EL SECTOR MARÍTIMO

**El sector Marítimo es un sector crítico para la sociedad, con influencia significativa en la economía y la seguridad nacional**

**Estudios realizados sobre el sector Marítimo (ENISA, Cyberkeel) apuntan a que el sector está altamente expuesto a ciberataques**

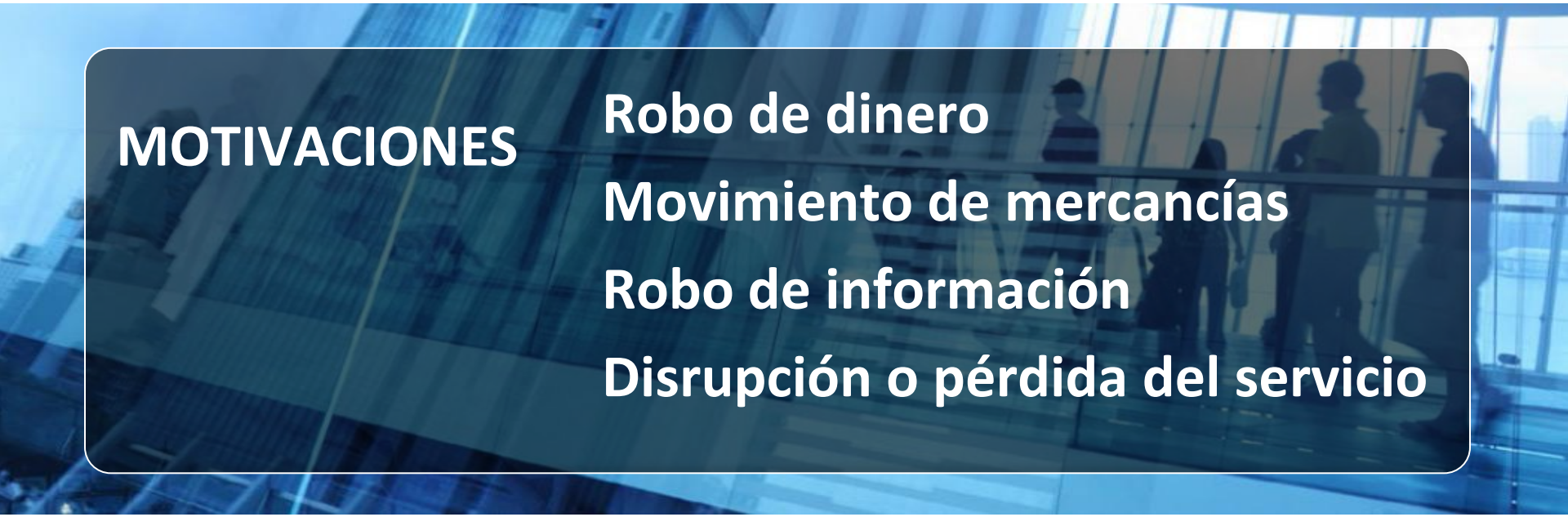
## Combinación de vulnerabilidades

**Específicas al sector: tecnologías específicas, procesos de negocio**

**Generalistas: tecnologías de amplio espectro, factor humano**

# RIESGOS EN EL SECTOR MARÍTIMO

- Alta dependencia en las TIC en entornos abiertos a Internet
- Nula concienciación de los riesgos
- Escasa implantación de tecnologías y soluciones de ciberseguridad
- SW/HW sin garantías de seguridad
- Escaso o nulo personal capacitado en ciberseguridad



# RIESGOS EN EL SECTOR MARÍTIMO

## Ejemplos de ataques satisfactorios al sector:

### Malware en HW (2014)

Malware incrustado en el HW de escáneres que, cuando conectados a la red de la compañía, buscaban y comprometían el servidor ERP para modificar información de entregas

Afectó a 8 compañías

### Robo de dinero (2013, 2014)

Ataque MITM en el sistema de correo electrónico de la empresa mercante

Transferencia de grandes cantidades a cuentas bancarias elegidas

# RIESGOS EN EL SECTOR MARÍTIMO

## Ejemplos de ataques satisfactorios al sector:

### IRISL (Iranian Shipping Line) (2011)

Borrado de todos los datos de precios, número de carga, fecha y lugar de entrega , causando entrega en destinos erróneos y pérdida de carga

### ECDIS (Electronic Chart Display and Information System) (2014)

Sistemas presentes en el puente de mando y usado como ayuda a la navegación, e interconectados con otros muchos sistemas e internet

Prueba de concepto que demuestra las vulnerabilidades existentes en los sistemas ECDIS: lectura no autenticada, descarga / sustitución / borrado de cualquier fichero del servidor host

# RIESGOS EN EL SECTOR MARÍTIMO

***Tráfico de drogas / Puerto de Amberes***

**1** **Instalación de keylogger en un ordenador de control de una compañía portuaria**

**2** **Intrusión en los ordenadores del terminal de contenedores para monitorizar aquellos que enviaban con droga**

**3** **Empleando documentación falsa, los conductores recogían la mercancía en el lugar y momento elegido**

**1.044 kilos cocaína y 1.099 kilos heroína durante 2 años, desde 2011**

# ÍNDICE

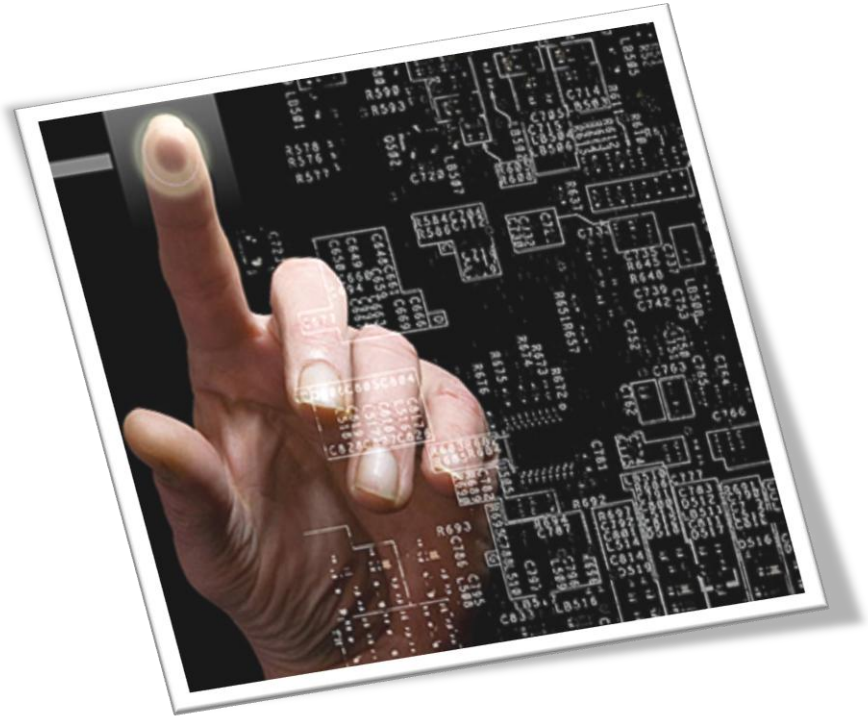


indra

# LA CIBERSEGURIDAD

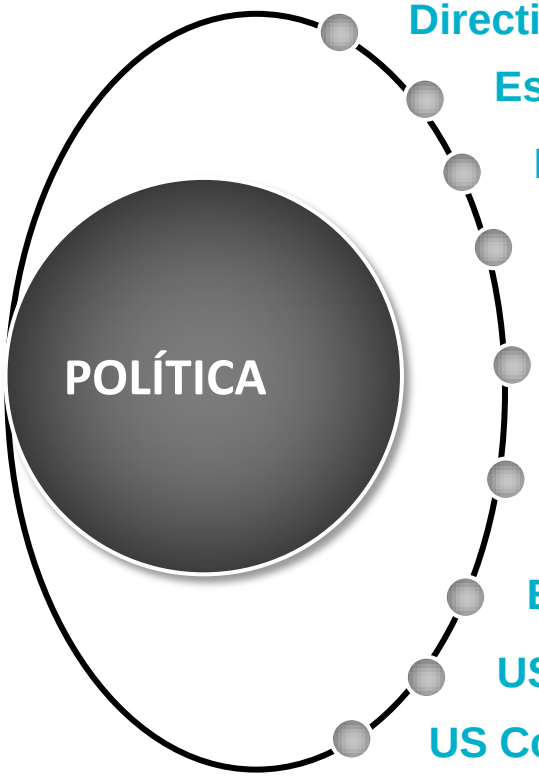
**La CIBERSEGURIDAD es el conjunto de medidas técnicas, políticas y organizativas enfocadas a proteger los sistemas de información y comunicaciones de ciberataques de cualquier índole**

- Debe **prevenir** la ocurrencia, eliminando la oportunidad.
- Debe **detectar** la ejecución en curso, incluso en etapas tempranas.
- Debe **proteger** a los sistemas de información en caso de ocurrencia de un ciberataque, impidiendo que éste sea satisfactorio.
- Debe permitir al sistema de información **recuperar**se a un estado estable previo al ciberataque, en caso que éste haya sido satisfactorio, y de manera que el impacto en el negocio sea mínimo.



# INICIATIVAS POLÍTICAS Y ESTRATÉGICAS

**Impulso a la ciberseguridad desde estamentos políticos europeos e internacionales como eje fundamental de la sociedad democrática**




- **Directiva Europea NIS** (pendiente de aprobación)
- **Estrategia de Ciberseguridad Nacional**, 2013
- **Estrategia de Seguridad Nacional**, 2013
- **Estrategia Europea de Ciberseguridad** «Un ciberespacio abierto, protegido y seguro», 2013
- **Propuesta de Directiva NIS de la CE** para garantizar unos niveles altos comunes de seguridad NIS, 2013
- **Orden Ejecutiva de Obama** «Improving Critical Infrastructure Cybersecurity», 2013
- **Esquema Nacional de Seguridad (ENS)**, 2010
- **US Cyberspace Policy Review**, 2009
- **US Comprehensive National Cybersecurity Initiative**, 2008

# INICIATIVAS POLÍTICAS Y ESTRATÉGICAS

# FORMACIÓN Y ENTRENAMIENTO

Escasez de capital humano especializado.

La constante evolución tecnológica y la diversidad e incremento en número de las ciberamenazas exige a empresas e instituciones disponer urgentemente de un elevado número de profesionales altamente cualificados y en constante formación.

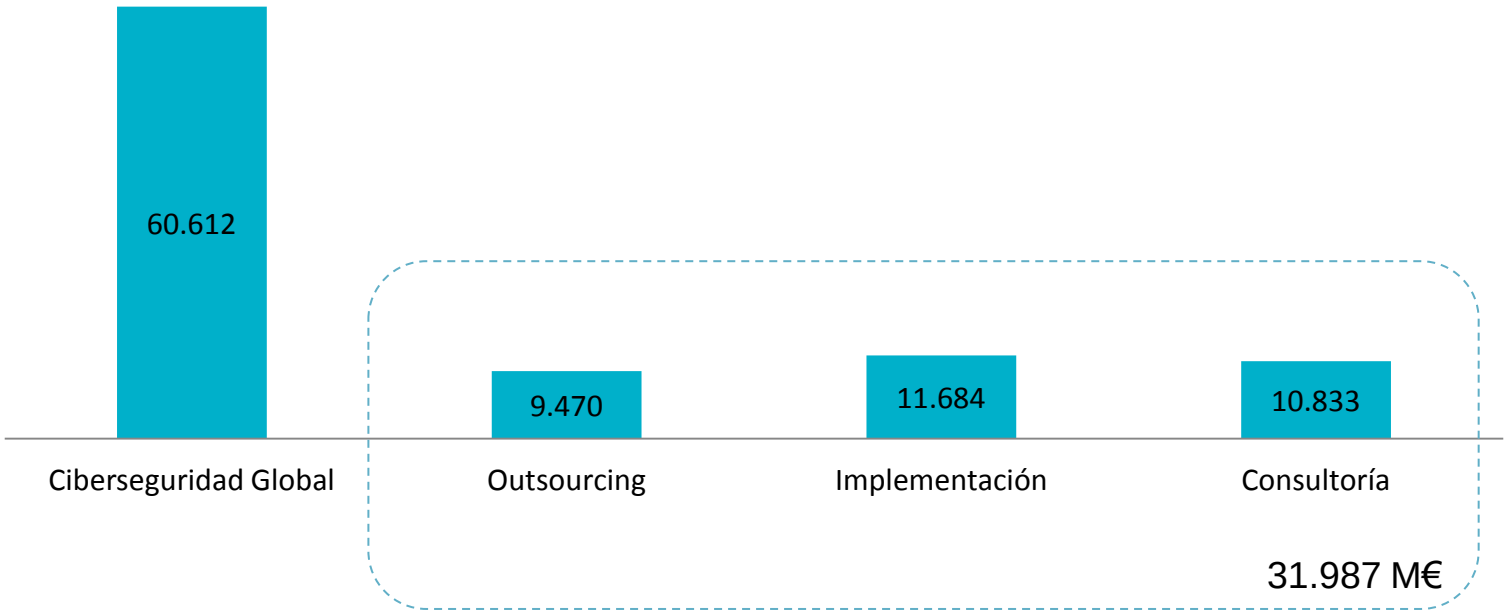
## Sin embargo…

El número de profesionales cualificados que se genera anualmente no cubre la demanda.

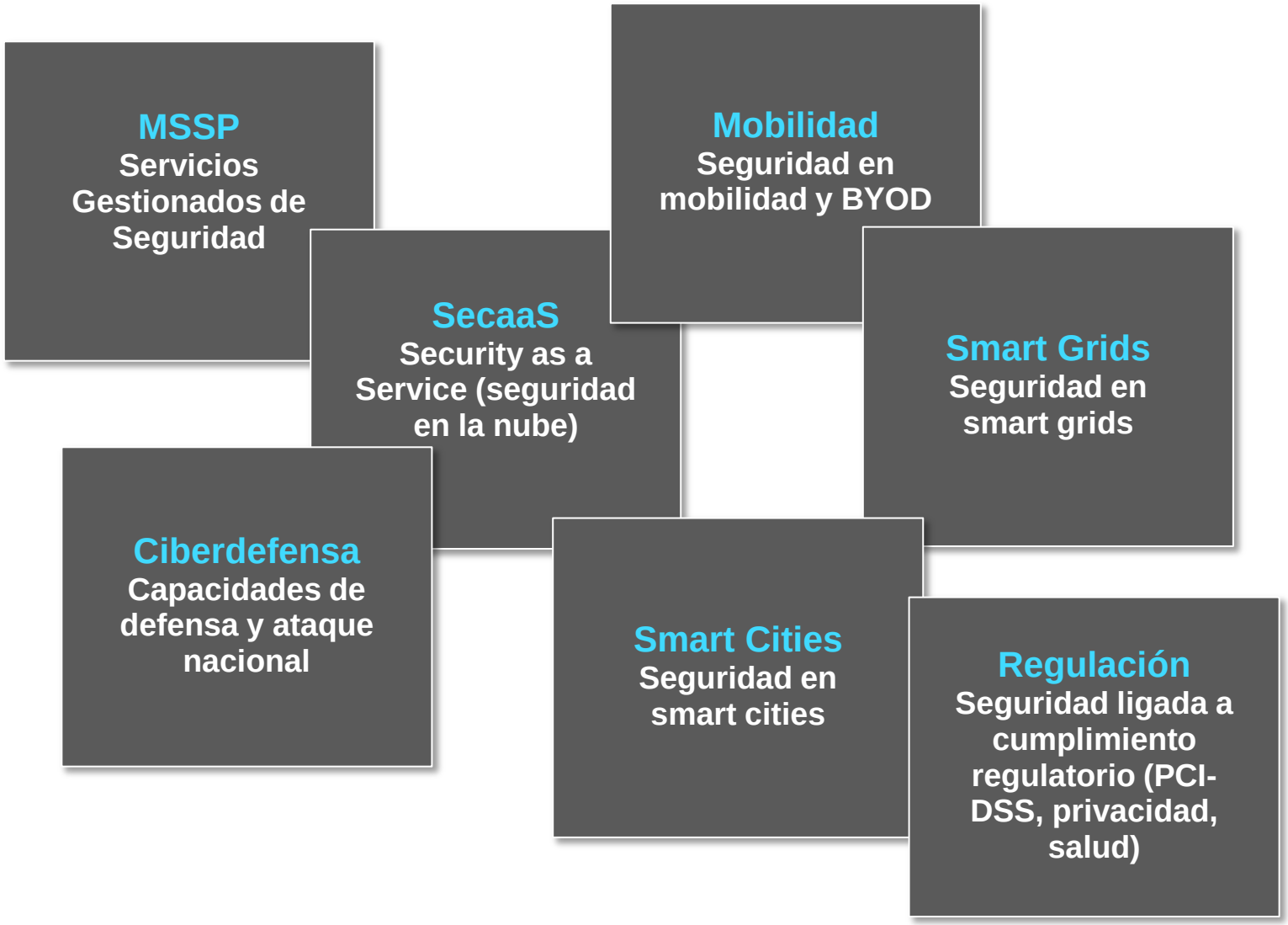
Existen importantes barreras de entrada (conocimiento) que ralentiza y encarece el proceso.

La ciberseguridad exige una formación práctica, que demanda muchos recursos del formador, por lo que es generalmente costosa.

# MERCADO MUNDIAL POR LÍNEAS DE ACTUACIÓN



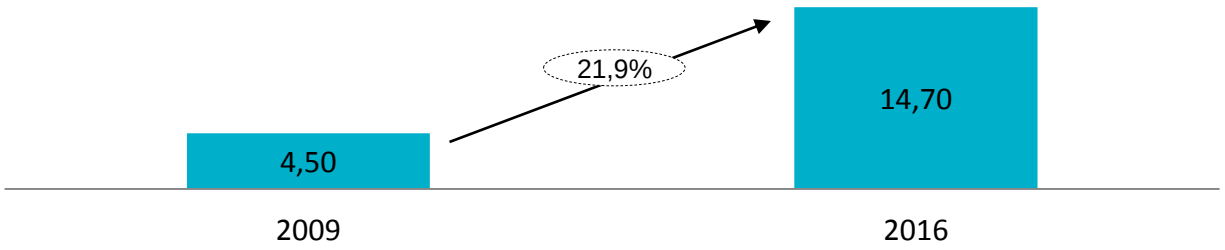
# TENDENCIAS DE FUTURO



# PERSPECTIVAS DE NEGOCIO

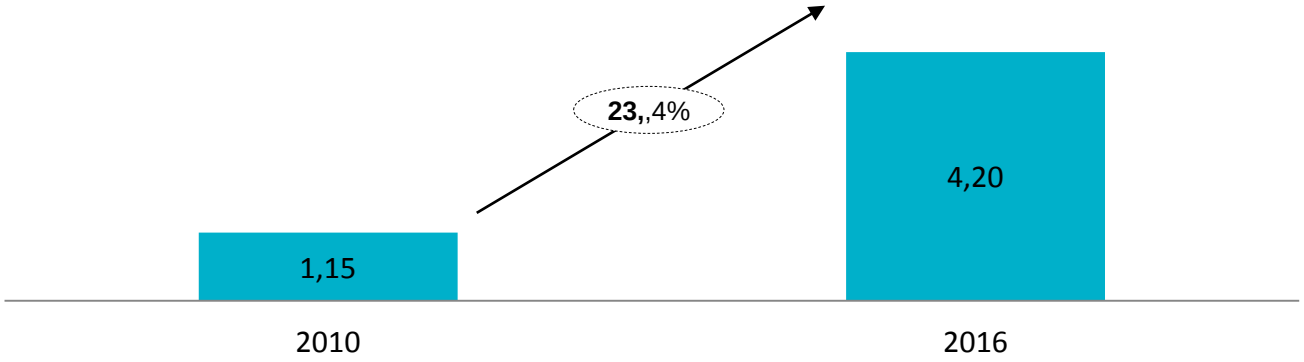
## MSSP

**Fuente: Frost & Sullivan**



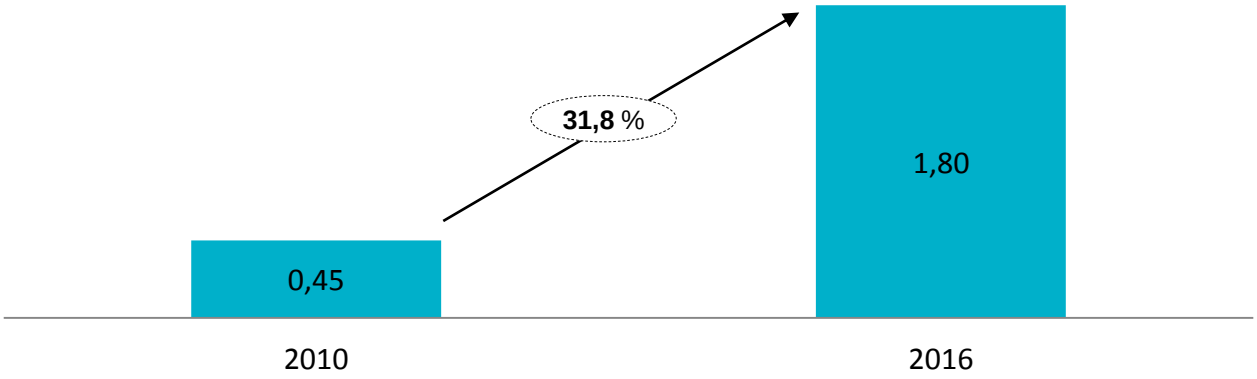

## SecaaS

**Fuente: Gartner**




## Mobile

**Fuente: IDC**

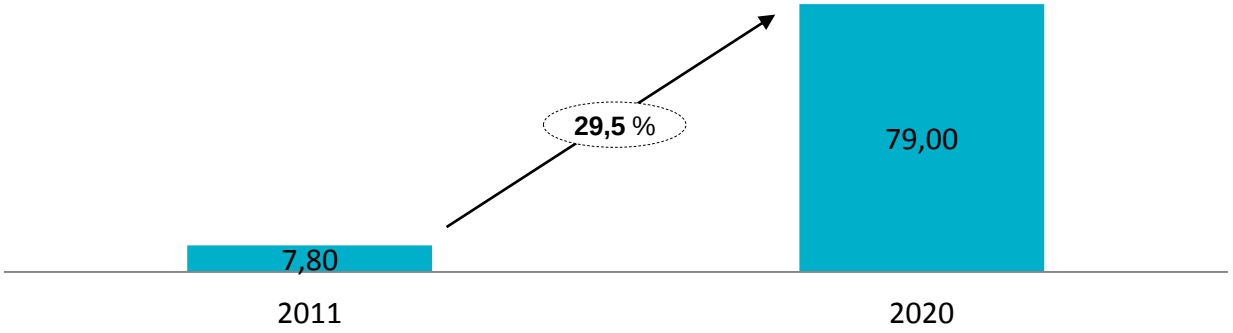



**mM $**

# PERSPECTIVAS DE NEGOCIO

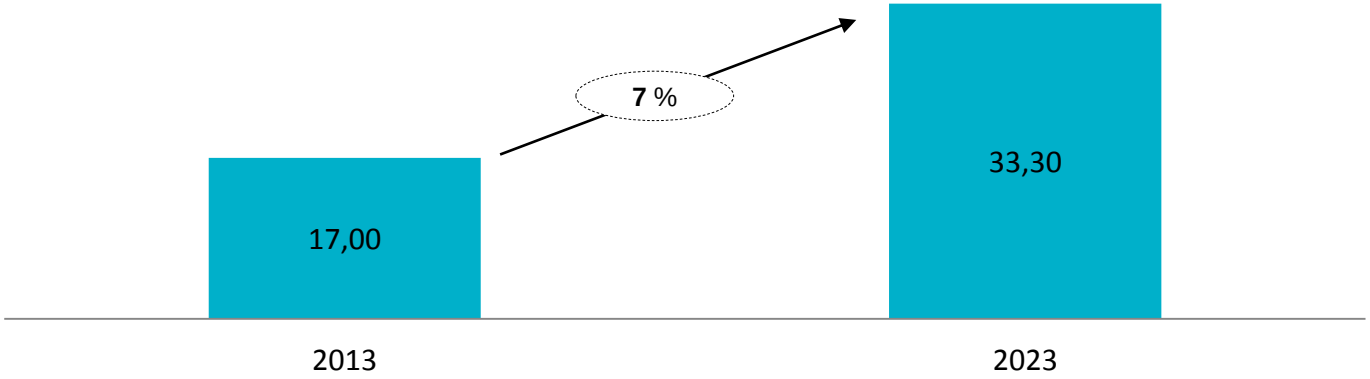
## Smart Grid

**Fuente: ReportsnReports**




## Ciberdefensa

**Fuente: Visiongain**



# ÍNDICE



indra

# ALGUNAS CONCLUSIONES

El ciberespacio es un entorno abierto, pero hostil

**Las ciberoperaciones ofensivas y los ciberataques crecen en número, sofisticación e impacto**

Actualmente adolecemos de la tecnología y las personas adecuados para hacer frente a los retos

Existen numerosas iniciativas estratégicas para dotar a los países y los sectores críticos de capacidades de detección y respuesta


El análisis histórico sugiere que, siguiendo la misma estrategia de siempre, continuaremos un paso por detrás de la amenaza

# Gracias

jlhardieta@indra.es

**www.indracompany.com**