

Impulso al sector nacional de la ciberseguridad a través de retos sectorizados

Ignacio Caño Luna
S-MOVING

www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD

SPANISH NATIONAL
CYBERSECURITY INSTITUTE

 **incibe_**

INSTITUTO NACIONAL DE CIBERSEGURIDAD



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y EMPRESA

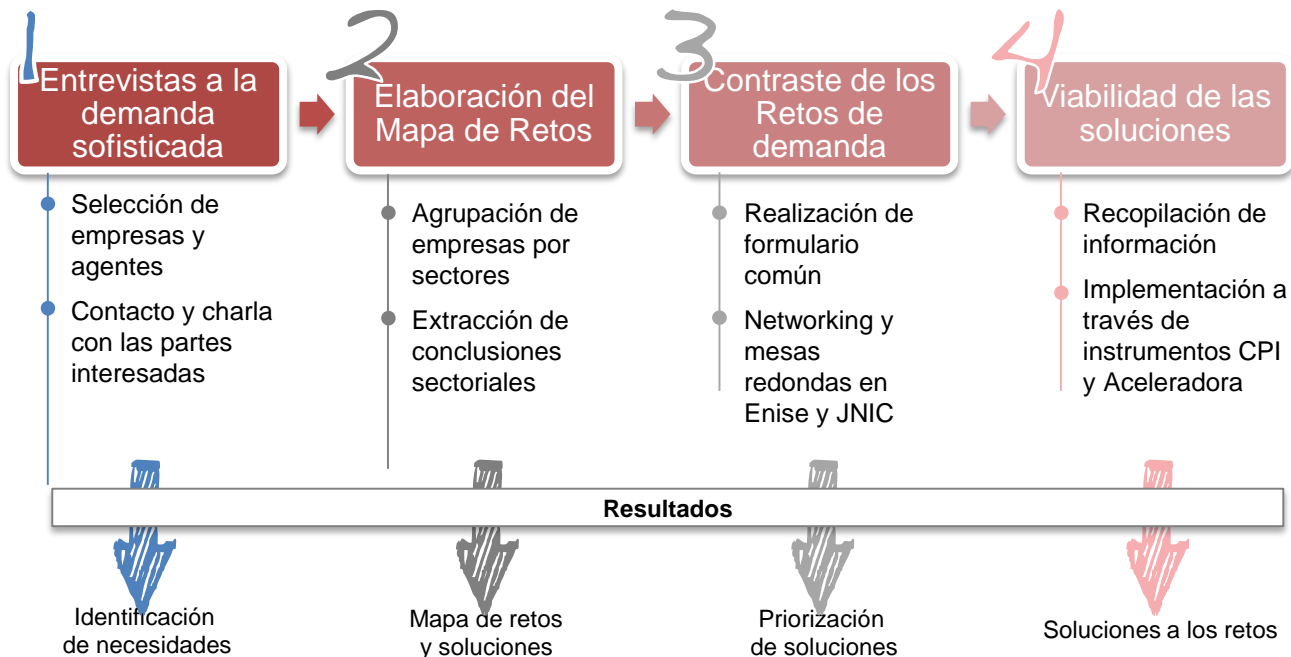
Protección de vehículos inteligentes y autónomos



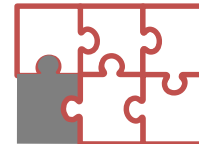
- La ciberseguridad como **motor esencial** de transformación digital
- Análisis de **oportunidades y tendencias** de Ciberseguridad
- **Retos sectorizados**: protección de coches inteligentes, vehículos aéreos no tripulados, SaaS, hacking ético, dispositivos médicos conectados, laboratorios de educación en Ciberseguridad, sistemas ICS y SCADA, simulación incidente y ciberejercicios, etc.
- **Ejemplos de casos de éxito**, y datos detallados sobre ámbito de aplicación, ubicación en la cadena de valor, previsiones de demanda, segmentos de clientes, potencial mercado, etc.
- **Guía de internacionalización** en Ciberseguridad, caracterización del **mercados y países objetivo**.
- **Información de interés**: indicadores económicos, marco fiscal, caracterización en el país destino, hoja ruta de internacionalización, principales entidades apoyo, eventos relevantes, socios en destino, entorno competitivo, etc.
- Impulsar el **modelo exitoso de colaboración** entre empresas del sector transporte, reguladores, integradores y empresas proveedoras de Ciberseguridad.
- Primer **encuentro de coche conectado Ciberseguro**: CTAG, Rodhe-Schwarz, Indra, GMV, Tinámica, Tecnalía, BQ, etc.

Proceso de identificación de retos tecnológicos

El proceso se basa en la **colaboración y participación** de los agentes de la demanda y oferta en Ciberseguridad para la identificación de ámbitos de trabajo conjunto y la valoración de las soluciones seleccionadas.



Mapa de retos y soluciones en sector transporte



El análisis de demanda del **sector del transporte** da como resultado la identificación de algunos retos y oportunidades:

- **Infraestructuras**, enfoque hacia protección de los sistemas de **suministro y control**
- **Negocio**, enfoque hacia la prevención de ataques al **servicio de transporte** de una empresa

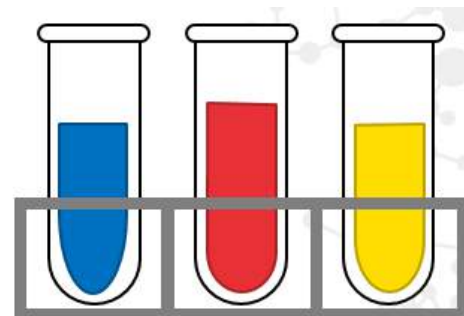
Mapa de retos del sector del transporte

| | Retos | Medidas |
|------------------|--|---|
| Infraestructuras | <ul style="list-style-type: none">• Medidas para la protección de elementos físicos | <ul style="list-style-type: none">• Herramientas para análisis de riesgos en infraestructuras de transporte |
| | <ul style="list-style-type: none">• Medidas para la securización del back-office | <ul style="list-style-type: none">• Sistemas adaptativos para hacer frente a los ataques• Gestión remota de endpoints |
| | <ul style="list-style-type: none">• Medidas para protección de la cadena de suministro | <ul style="list-style-type: none">• Evaluación de productos y servicios, reputación TIC en la cadena (revisión de si se encuentran en lista de spammers, bots, etc.) |
| | <ul style="list-style-type: none">• Medidas para la protección de sistemas de control industrial | <ul style="list-style-type: none">• Servicios de seguridad gestionada: Seguridad perimetral /Seguridad en redes / Herramientas Anti-APT |
| | <ul style="list-style-type: none">• Medidas para protección de elementos IOT | <ul style="list-style-type: none">• Security by design en sensores, máquinas y otros dispositivos |
| Negocio | <ul style="list-style-type: none">• Medidas para la prevención y mitigación de ataques | <ul style="list-style-type: none">• Investigación de incidentes, grabación masiva del tráfico (Big Data) y detección de patrones• Herramientas de inteligencia avanzada: para sistemas, redes sociales y otros canales potenciales de entrada |

¿Cómo encontrar soluciones a los retos en el sector?

Piloting projects to solve end users' challenges and create future market leaders

- 1. Dynamize demand** of cybersecurity solutions
 - Public instruments to **encourage** participation, such as **pre-commercial public procurement** to adopt innovation.
 - Focus** around main challenges and **specific use cases** to develop the supply of innovation capabilities and environment for **experimentation and testing**
- 2. Facilitate supply capabilities**
 - Competence centers** and training
 - Facilities for experimentation** and **rapid prototyping**.
- 3. Reduce market transfer gap**
 - PoCs into MVP** that solve client needs
 - IPR protection**
 - Talent and tech skills into SMEs** and start-ups





INCIBE supports the national cybersecurity sector

In a nutshell, INCIBE implements a **complete programe** including activities to increase **local demand, new tech suppliers, and stronger international positioning.**

Strategic actions:

1 - Cluster Development and support existing companies

Supporting market development, higher visibility abroad, latest trends and opportunities

2 - R&D transfer to solve industry tech challenges

Better alignment and communication between academia and industry

3 - New start-ups and entrepreneurship

Incubation and acceleartion programs

Industry: Identified issues for cybersecurity growth

Industry associations

- Variety of initiatives on **regulatory, standards** and awareness aspects.

Innovation

- Broad range of research and technological groups but **lack of leadership**

Talent

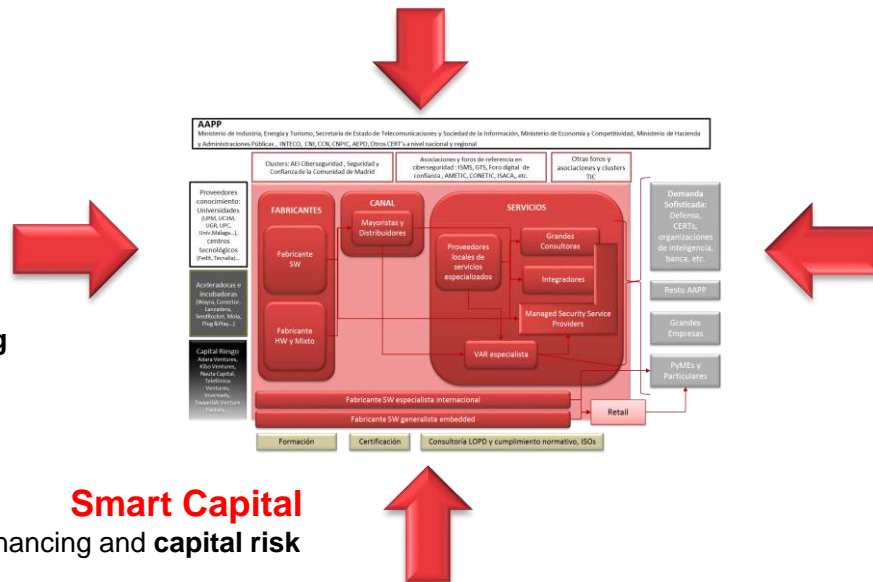
- Limited offer of **specialized training**
- Limited collaboration **University-Industry**

Smart Capital

- Lack of financing and **capital risk**

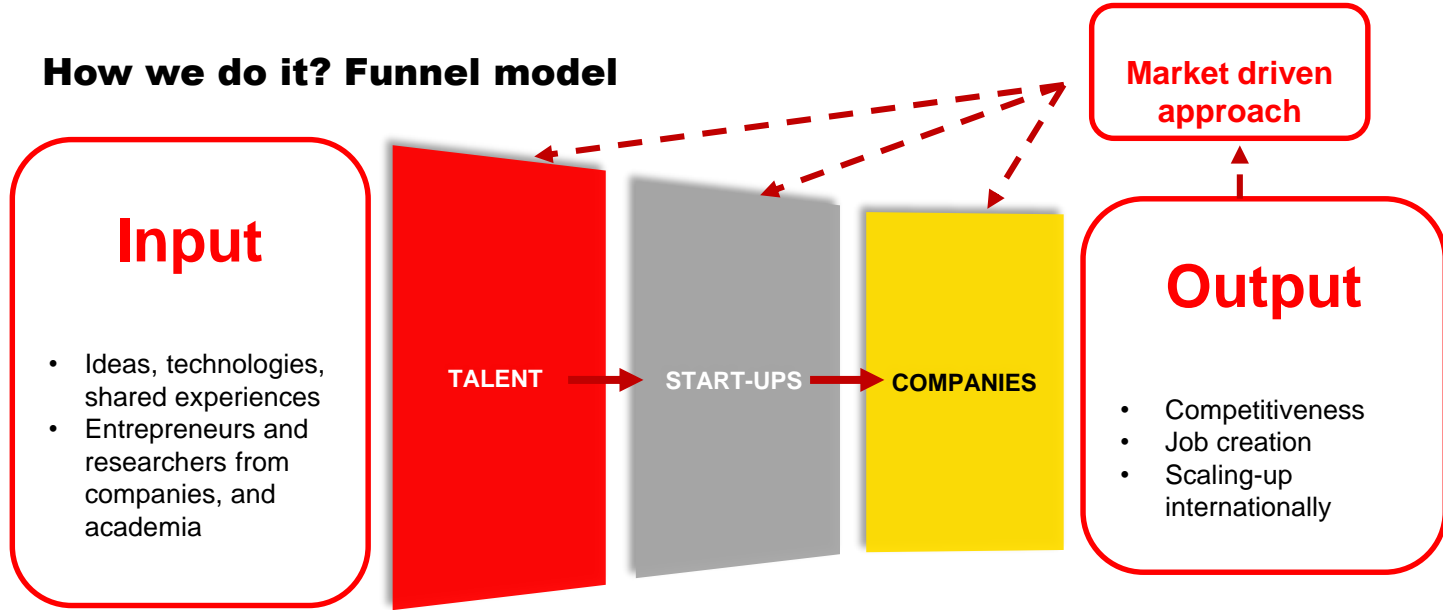
Local demand

- Key role of the Public Administration to develop **innovation ecosystem**
- Product **certification criteria**
- **Public Demand:** Defense, Home Affairs, CERTs, CIPs Authorities, etc



INCIBE drives cybersecurity innovation

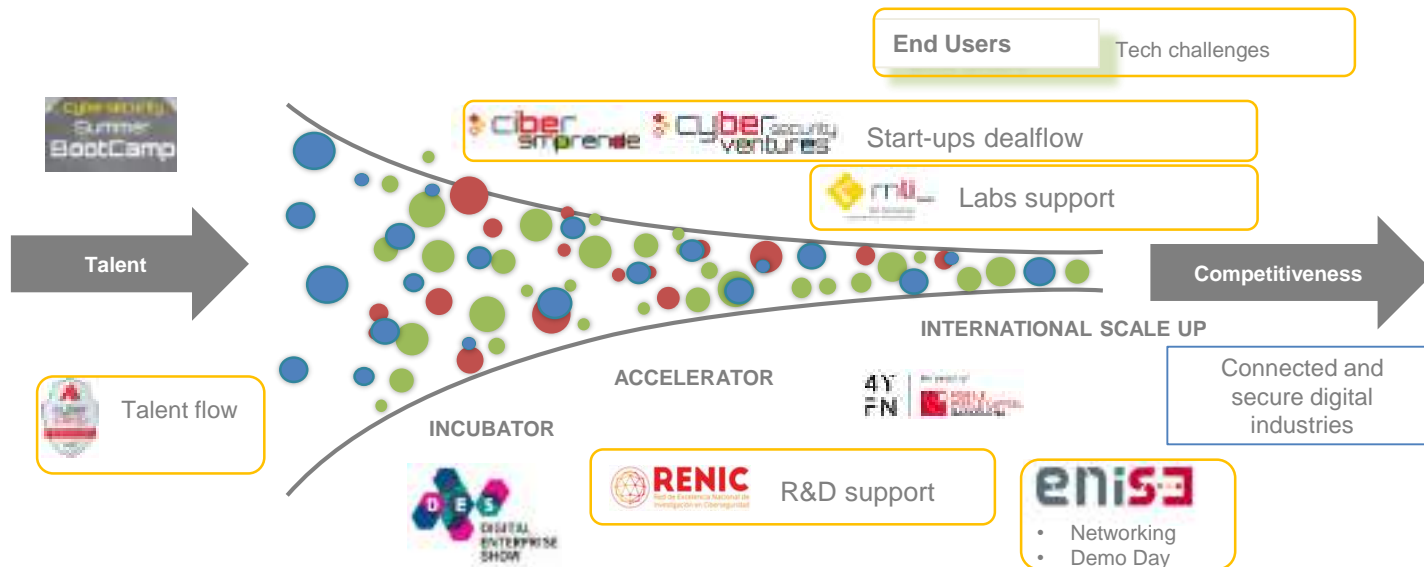
How we do it? Funnel model



| TECH TRANSFER | ACCELERATOR | To INDUSTRY CLUSTER |
|-----------------------|------------------------|-----------------------|
| COMMUNITY DEVELOPMENT | MENTORING AND TRAINING | NEW PRODUCTS |
| BUSINESS MODELING | SCALABILITY | INTERNATIONAL OPPORT. |
| PRIZE AWARDS | INVESTORS - DEMO DAY | COLLABORATION |

Our Building blocks to develop local champions

Integrated wide Program



1. Cluster development (International Meeting on Information Security)



1,300 participants and 136 speakers in 11ENISE



Objectives

- Promote and foster international **sector development**
- Increase in the **turnover** of the Spanish cybersecurity companies in the national and international markets.
- A broad range of parallel activities i.e. Smart and connected Car



Target Audience

- Cybersecurity experts
- ICT professionals
- Entrepreneurs in Cybersecurity
- Cybersecurity demand



Parallel activities

- ENISE Award
- Entrepreneurial Track
- International Business Forum

Next edition: October 2018, León

2. R&D transfer (talent development)

Orchestrating the National R&D Excellence Network in Cybersecurity

To avoid fragmentation and reach critical mass

- +100 Research teams
- +1.000 Researchers
- Infrastructure

Coordination & prioritization

- National Cybersecurity Research Agenda
- European Commission NIS-Strategic Research Agenda

Objectives

- Knowledge transfer to Industry
- Spin-offs / Start-ups
- Attract Seed Capital / Venture Capital (VC).



2. R&D transfer (talent development)

INCIBE as a Centre of Excellence
Promotes talent and advanced professional training



Cybersecurity R&D&I
Network of Centres of
Excellence



Grants for excellence
of advanced research teams



National Conferences
on Cybersecurity
Research



Workshops
"Cybersecurity Spaces"



CyberCamp



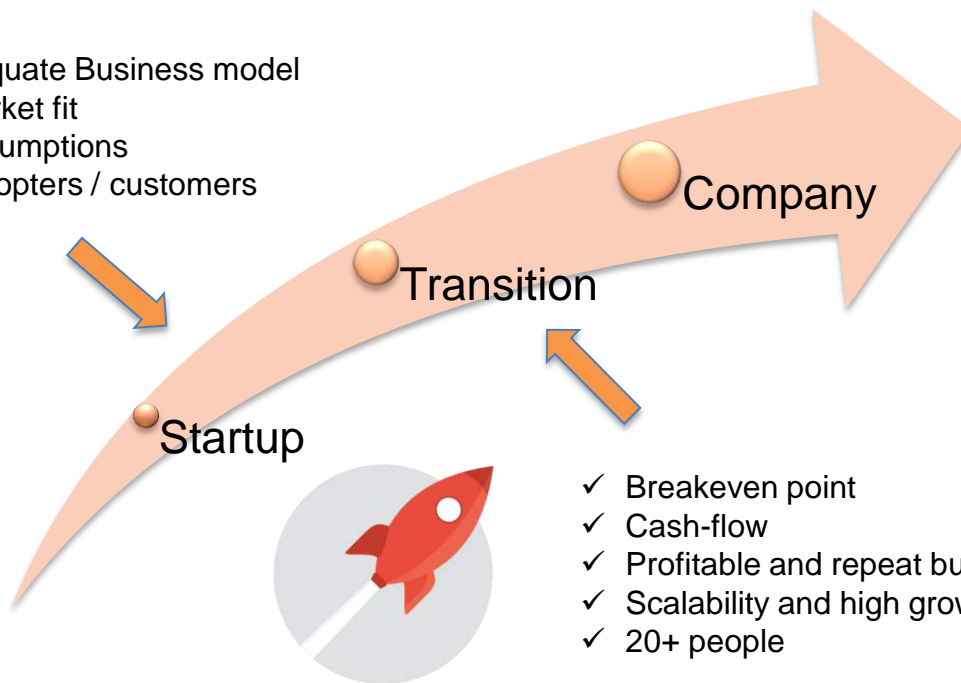
European CyberSecurity
Challenge

3. Start-ups support

- ✓ Seeking adequate Business model
- ✓ Product / market fit
- ✓ Validated assumptions
- ✓ First early adopters / customers

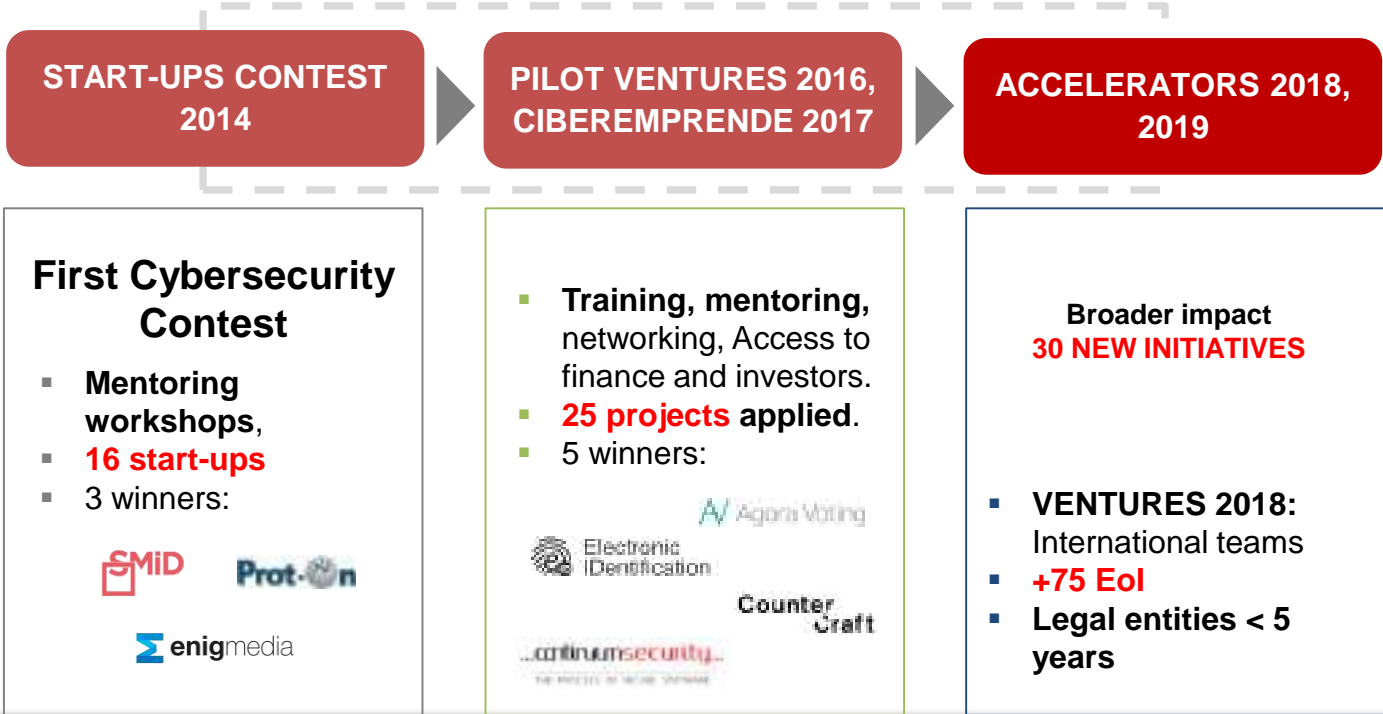
INCIBE

Catalyst for cybersecurity innovation and technology in the field of cybersecurity



- ✓ Breakeven point
- ✓ Cash-flow
- ✓ Profitable and repeat business
- ✓ Scalability and high growth
- ✓ 20+ people

3. Start-ups (track record)



3. Start-ups (acceleration results)

>30 Collaborating organizations

>70 Meetings facilitated with investors, customers and business partners

11 Cybersecurity challenges proposed by Large Corporations

Potenciales Clientes – Socios comerciales



Financiación pública



3. Start-ups (success stories)

Estos españoles cazan a los traficantes que pagan drogas, armas o 'malware' con Bitcoin



ElReferente

Continuum Security recibe 1,5M€ de los fondos de inversión Swanlaab, JME y Sunae



Electronic Identification nombrada en España Cool Vendor 2017



El contraespionaje de la 'startup' CounterCraft capta un millón



Los archivos del Pentágono

3. Start-ups (success stories)



Threat Intelligence Platform for early malware detection



Encrypted content to transfer and secure information



Insider Threat detection and employee incident prevention



Parental control on mobile devices



Online Training platform and employee awareness



Insurance fraud detection through AI



Anomaly detections in electrical substation networks



Multi-factor authentication with *Dome* secret sites



Dualogy Security

Security analysis of every asset exposed to the Internet



keynetic

Digital identity and access control based on SDN

More information

CONTACT

We care about **our digital image** so that it reflects what we are, what we are capable of doing and what we do info@incibe.es

VISIT US

Instituto Nacional de Ciberseguridad (INCIBE)
info@incibe.es

LEARN MORE

Computer Emergency Response Team for Security and Industry (CERTSI)
<https://www.certs.es>
Internet Security Office (OSI) <https://www.osi.es>
CyberCamp <https://www.cybercamp.es>
Internet Segura for Kids <https://www.is4k.es>

FOLLOW US!

Twitter, Youtube, Facebook, LinkedIn, G+. @Incibe
@Certs_ @Osiseguridad @is4k @CyberCampEs @CiberEmprende
@protegeempresa

REPORT

Incidents, vulnerabilities, online fraud, phishing, malware, etc.
incidencias@certsi.es, consultas@osi.es y empresas@incibe.es