#innovacion
#financiacion
#asesoramiento
#internacionalizacion

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI Centro para el Desarrollo Tecnológico Industrial

@CDTIoficial

Programas Europeos sobre Ciberseguridad
Oportunidades de financiación 2019

ESHORIZONTE2020

Portal español del Programa Marco de Investigación e Innovación de la Unión Europea

@EsHorizonte2020

Maite Boyero Egido

Representante y Punto de Contacto Nacional
Sociedades Seguras – Horizonte2020
Centro para el Desarrollo Tecnológico Industrial

Contexto actual...

Objetivos de la Comisión Europea

President Juncker signs Joint Declaration on legislative priorities for 2018-2019 with European Parliament and Council

The Joint Declaration sets out **seven priority areas**:

1. Better protecting the **security of our citizens**;
2. Reforming and developing our **migration policy** in a spirit of responsibility and solidarity;
3. Giving a new boost to **jobs, growth and investment**;
4. Addressing the **social dimension** of the European Union;
5. Delivering on our commitment to implement a **connected Digital Single Market**;
6. Delivering on our objective of **an ambitious Energy Union and a forward looking climate change policy**; and
7. Further developing the **democratic legitimacy** at EU level.

In addition, the three Presidents agreed to pursue the commitment to common European **values**, democracy and the rule of law; pursue a robust, open and fair **trade policy**; tackle **tax** fraud, tax evasion and tax avoidance; ensure **social** protection and social rights as set out in the Pillar of Social Rights; contribute to stability, **security and peace**; and ensure a high level of **data protection**, **digital rights** and **ethical standards in artificial intelligence** and **robotics**.

cPPP en Ciberseguridad

450 M€
entre 2016 y 2020

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

COM (2013) 1

Promoting a single market for cybersecurity products

https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

ECSO (www.ecs-org.eu) y **lanzamiento de la cPPP en Ciberseguridad (5 de Julio de 2016)**

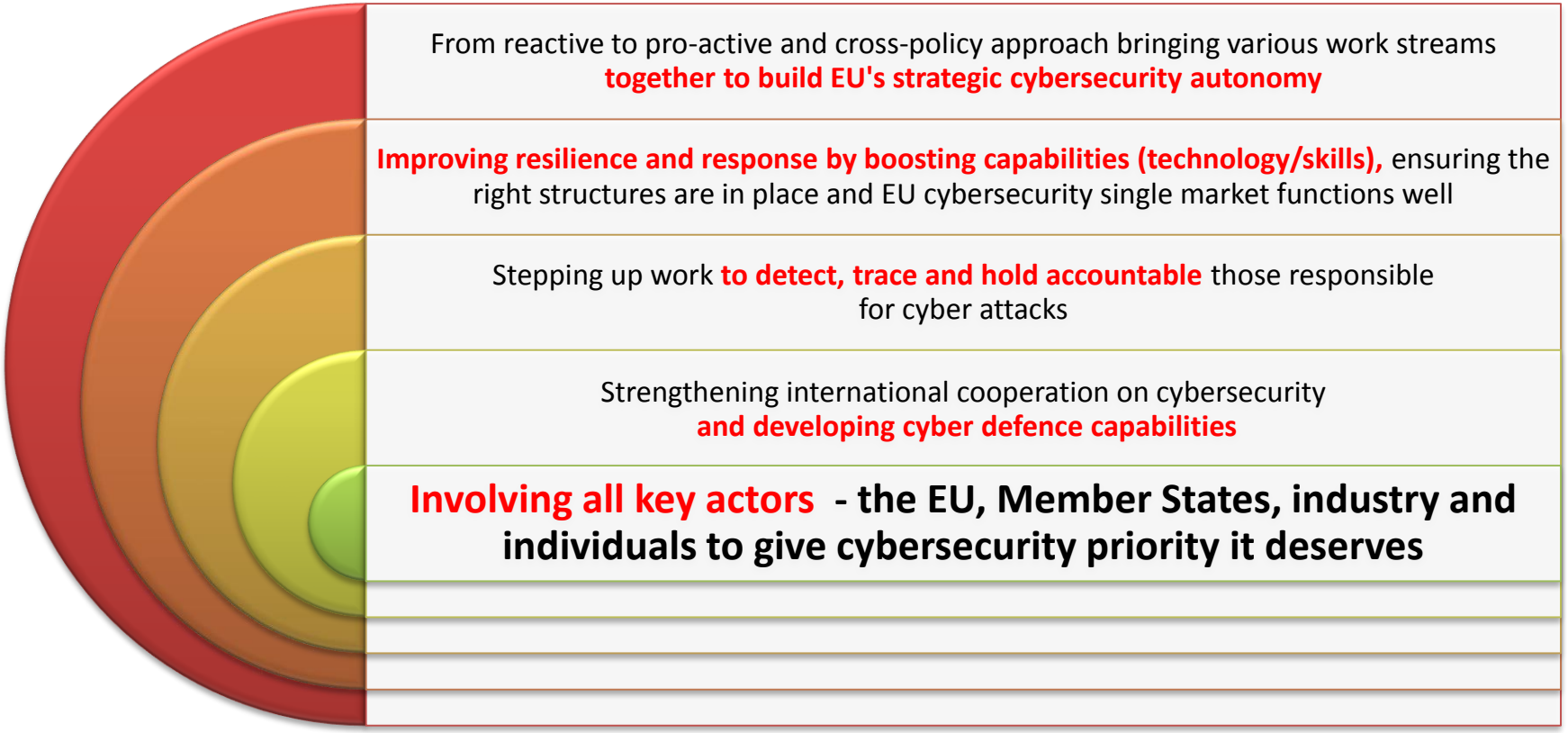
https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

Centro para el Desarrollo Tecnológico Industrial

Cybersecurity — Tallinn Digital Summit

- *Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'*
- *Proposal for a Regulation on ENISA, the 'EU Cybersecurity Agency', and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act')*
- *Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*
- *Communication 'Making the most of the Directive on security of network and information'*
- *Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment*
- *Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems*
- *Communication 'A Fair and Efficient Tax System in the European Union for the Digital Single Market'*

Comunicación: *"Resilience, Deterrence and Defence: Building strong cybersecurity in Europe"*



http://ec.europa.eu/newsroom/document.cfm?doc_id=46998

Discurso del Presidente Juncker sobre el Estado de la Unión (12 sept 2018)

https://ec.europa.eu/commission/priorities/state-union-speeches/state-union-2018_en

New Initiatives, related to R&I:

*Adoption by the co-legislators of the proposal establishing the **European Cybersecurity Industrial, Technology and Research Competence Network Centre**. The Regulation to establish a European Cybersecurity Industrial, Technology and Research Competence Network Centre has been published yesterday by the EC (see here). The proposal is to establish a Joint Undertaking (Art. 187), which would "scale-up" the current contractual Public-Private Partnership (cPPP) on cybersecurity. The Competence Center should implement relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements. On the side of Horizon Europe, the budget would come from the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness'. **On the side of Digital Europe Programme, €1.9 billion would be allocated to the activities of the Competence Center (i.e. the totality of the budget that was planned for cybersecurity under Digital Europe Programme).***

Policy context – Research & Innovation (Work Programme)

Policy Context

- ✓ Digital Single Market Strategy
- ✓ NIS Directive
- ✓ eIDAS, GDPR regulations
- ✓ Proposal for an e-Privacy regulation
- ✓ Communication on Strengthening Europe's Cyber resilience system and fostering a competitive and innovative cybersecurity industry
- ✓ cPPP on Cybersecurity
- ✓ Cybersecurity Package – September 2017
- ✓ Cybersecurity EU Competence Centre (2018) - proposal

R&I – SC7 WP2019-2020

- ➢ Management of cyber-attacks and other risks;
- ➢ Digital security and privacy for citizens and Small and Medium-sized Enterprises and micro-enterprises;
- ➢ Cybersecurity in the energy sector;
- ➢ Digital security, privacy, data protection and accountability in critical sectors/domains;
- ➢ Quantum Key distribution testbed
- ➢ Building blocks for resilience in evolving ICT systems

Oportunidades de financiación en Ciberseguridad
WP 2019 – Secure Societies

Focus Area: Boosting the effectiveness of the Security Union

Budget: ca. €1,000m

Mission	Component	Source
✓ New technologies and processes to meet needs of security practitioners, including for fighting and preventing crime ✓ Reduced loss of life and damage from natural and man-made disasters ✓ Key infrastructure better protected ✓ EU borders better secured ✓ **Secure and trusted digital environment**	✓ Better match R&D objectives with Security Union policy needs. ✓ Strengthen impact of security-related research: involving practitioners and stimulating new markets. ✓ **Identify security-related research in other H2020 societal challenges, and contribute to other policies (Digital, Space, Health, etc.)**	✓ LEIT-ICT ✓ LEIT-Space ✓ SC - Health ✓ SC - Energy ✓ SC – Reflective Societies ✓ SC – Secure Societies

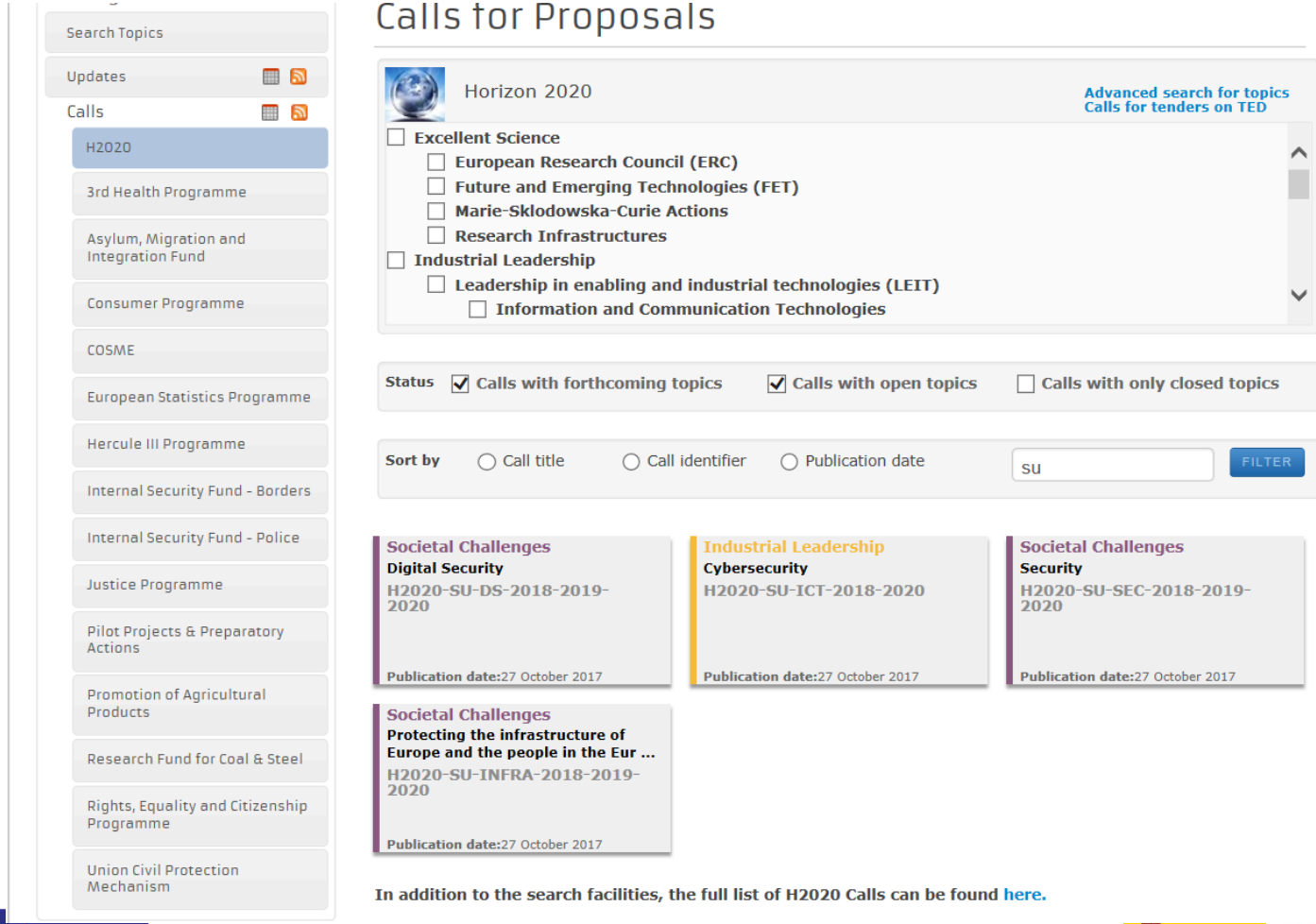
División de Programas de la UE

@EsHorizonte2020

CDTI Centro para el Desarrollo Tecnológico

¿Dónde encontrar los topics de Ciberseguridad?

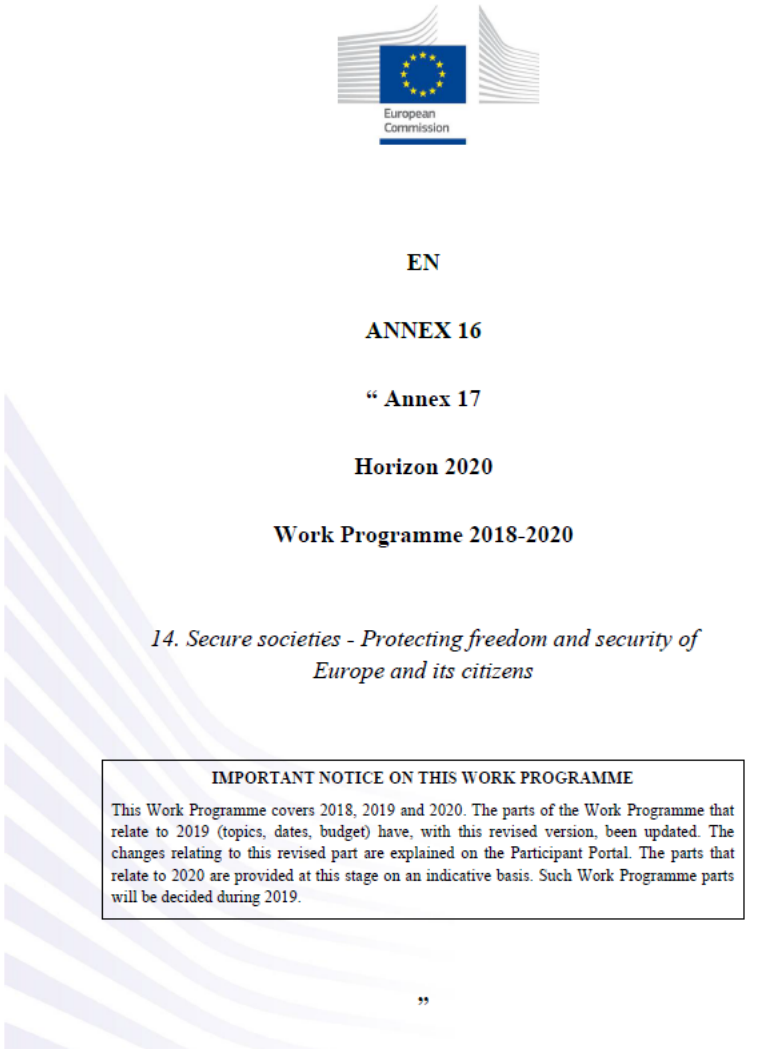
ec.europa.eu/research/participants/portal/desktop/en/home.html



Call 2019 – RS 7

Abre: 14/03/2019

Cierre: 22/08/2019, 17.00h



EN

ANNEX 16

" Annex 17

Horizon 2020

Work Programme 2018-2020

14. Secure societies - Protecting freedom and security of Europe and its citizens

IMPORTANT NOTICE ON THIS WORK PROGRAMME

This Work Programme covers 2018, 2019 and 2020. The parts of the Work Programme that relate to 2019 (topics, dates, budget) have, with this revised version, been updated. The changes relating to this revised part are explained on the Participant Portal. The parts that relate to 2020 are provided at this stage on an indicative basis. Such Work Programme parts will be decided during 2019.

"

Digital Security - Cybersecurity

Cybersecurity, Digital Privacy and data protection .....

SU-DS01-2018: Cybersecurity preparedness - cyber range, simulation and economics.....

SU-DS02-2020: Management of cyber-attacks and other risks.....

SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises .....

SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches.....

SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors.....

Digital Security - Cybersecurity

SU-DS03-2019: Digital security and privacy for citizens and Small and Medium Entreprises and Micro Entreprises → IAs of 4-5 M€ of TRL 7

Sub-topic (a) Protecting citizens' security, privacy and personal data

- Proposals should bring innovative solutions to personal data protection (…) in order to help citizens better monitor and audit their security, privacy and personal data protection
- They should include innovative approaches, techniques and user-friendly tools, covering different aspects of data protection on the web/applications
- TRL – 7
- Expected Impact: to reduce economic damage caused by harmful cyberattacks and privacy incidents, including personal data protection breaches; more trustworthy digital environment

SU-DS03-2019: Digital security and privacy for citizens and Small and Medium Entreprises and Micro Entreprises → IAs of 3-4 M€ of TRL 7

Sub-topic (b) SMEs and MEs: defenders of security, privacy and personal data protection

- Proposals should deliver innovative solutions to increase knowledge sharing in digital security across SMEs&MEs and between SMEs&Mes and larger providers
- They should include innovative approaches, techniques and user-friendly tools, covering monitoring, vulnerabilities, management and forecasting and building on-line collaboration on security, privacy and data protection
- TRL-7
- Expected Impact: SMEs&Mes better protected and becoming active players in the DSM, including implementation of NIS Directive and GDPR

SU-DS05-2018-2019-2020: Digital security, privacy and accountability in critical sectors (2018)

Sub-topic (a): In multimodal transport

IAs of 5 M€ and TRL 7

Proposals should cover, at least, 2 of the following items:

- Secure access management for citizens to all type of vehicles
- Assurance and protection against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities
- Standardization to allow quick adoption of cybersecurity best practices in the domain

SU-DS05-2018-2019-2020: Digital security, privacy and accountability in critical sectors (2018)

Sub-topic (b): In the healthcare ecosystem

RIAs of 5 M€ and TRL 7

Practical implementation of relevant EU legislation (NIS,eIDAS, GDPR) in the healthcare complex ecosystem involving all stakeholders

Proposals should cover, at least, 2 of the following items:

- Develop dynamic vulnerability data basis for collecting, uploading, maintaining and disseminating vulnerabilities of ICT-based medical systems, applications and services
- Deliver dynamic, evidence-based, sophisticated security, privacy and personal data protection risk assessment frameworks and tools that can deal with cascading effects of threats and propagated vulnerabilities
- Provide collaborative privacy-aware tools enabling healthcare stakeholders to access and share information

Protecting the infrastructure of Europe and the people in the European smart cities

Proyectos de 2 años

Participación de la industria es un requisito!!!!

Protecting the Infrastructure in Europe

SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

IAs of bout 8 M€ and TRL 7 for deploying solutions that allow forecast, prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs) over the life span of the infrastructure and also the neighbouring populations and the environment.

- Interdependent physical (e.g. bombing, plane or drone overflights & crashes, spreading of fires, floods, seismic activity, space radiations, etc.) **and cyber threats and incidents (e.g. malfunction of SCADA system, non-authorised access of server)** and consider the cascading risks.
- Scenarios of real life in real-time and tackling physical **and cyber threats**.
- **SECTORS: Water systems, energy infrastructure (power plants and distribution), transport infrastructure, communication infrastructures, health services, e-commerce and the postal infrastructure, and financial services.**
- **At least 2 operators** (not necessary to be coordinators) of the chosen type of critical infrastructure operating in 3 Member States or Associated Countries.

Condiciones de elegibilidad

- Al menos 2 operadores de infraestructuras críticas de al menos 2 EEMM o Asociados (INFRA01) o al menos 2 ciudades / aglomeraciones de 2 EEMM o Asociados (INFRA02) como SOCIOS
- Implicación de **la industria OBLIGATORIA**
- Implicación de otro tipo de usuarios, OPCIONAL
- Duración máxima de los proyectos: 2 años
- Se financiarán proyectos que demuestren que NO SE SOLAPAN con los ya financiados (en cuanto a sector de actividad)

Fight Against Crime & Terrorism

SOME TOPICS HAVE DIFFERENT SUB-TOPICS depending on the year!!!!!!!

Fight Against Crime & Terrorism

SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism

At least 3 LEAs

IAs de 8 M€ & TRL 5-7 (SÓLO 1 Proyecto) → Developing solutions (in compliance with EU societal values, including privacy and fundamental rights) that allows the LEAs **to manage voluminous and heterogeneous data** (images, videos, geospatial intelligence, communication data, traffic data, financial transactions related date, etc.) and turn it into **actionable intelligence**.

- **Trend analysis of emerging cybercrime activities based on past of (cyber)criminal activities, on technological developments, and on trends in the society.**
- **Behavioural/anomaly detection** systems (using dif. sensors) and methodologies .
- **Balance** of IT specialists, psychologists, sociologists, linguists, etc. exploiting big data and predictive analytics: a) to caracterize trends in cybercrime and in cybercriminal organizations and b) to enhance citizens' security against terrorist attacks in places considered as soft targets, including crowded areas (shopping malls, entertainment venues, etc.).
- **Societal aspects** (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed.

LEIT-ICT – WP 2019

FECHA DE CIERRE: 14 DE NOVIEMBRE DE 2018

SU-ICT-04-2019: Quantum Key Distribution Testbed

- Current security of the digital infrastructures and services will soon be under threat of no longer providing long-term security. Confidentiality of data and communications, authentication, as well as the long-term integrity of stored data have to be guaranteed, even in the advent of quantum computers. **Introducing Quantum Key Distribution (QKD) in the underlying infrastructure has the potential to maintain end-to-end security in the long-term.**
- Building an **experimental platform to test and validate the concept of end-to-end security, providing quantum key distribution as a service**. Proposals should develop an open, robust, reliable and fully monitored metropolitan area testbed network (ring or mesh configuration).
- **IAs – 15 M€**

Save-the-date

- **Security Research Event 2018 (SRE) in Brussels.** Theme: "Making Europe a safer place: demonstrating the impact of EU-funded security research"

  Date: 5th and 6th December 2018

  https://ec.europa.eu/home-affairs/sites/homeaffairs/files/201807_save-the-date-web.pdf

- **ICT 2018: Imagine Digital – Connect Europe**

  Date: 4-6th December 2018, Vienna

  https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe

- **5th International HLS and Cyber Conference,** Tel Aviv, 12-15 de Noviembre de 2018

  https://israelhlscyber.com/

Ciberseguridad H2020 (2014-2017)*: ICT-LEIT + RS7 ¡Buenos resultados!

Retorno económico	**M€** **% UE (% del total)**	**27,3 M€ (249,2 M€)** **11,8 % (11%)**
Tasas de éxito	**España** Total	**12,7%** 12%

UK
11,6%

DE
11,62%

ES
11%

* Datos provisionales

División de Programas de la UE
@EsHorizonte2020

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI Centro para el Desarrollo Tecnológico Industrial
@CDTIoficial

El equipo de Sociedades Seguras en España

La **Delegación** española en el **Comité de Gestión** Secure Societies

Dirección Programas Internacionales	Maite Boyero Egido maite.boyero@cdti.es
DG GUCI - Servicio de Innovación tecnológica	Ramón Darder rdarder@guardiacivil.es
CNP - Servicio de Innovación tecnológica	José Francisco López josef.lopez@policia.es

Puntos Nacionales de Contacto de la temática

Dirección Programas Internacionales	Maite Boyero Egido maite.boyero@cdti.es

El equipo CDTI en Bruselas

Dirección Programas Internacionales	Marina Martínez marina.cdti@sost.be

Cómo mantenerse informado

Listas de distribución CDTI:
http://www.cdti.es/index.asp?MP=8&MS=69&MN=2&r=1024*819

Síguenos:
@h2020_seguridad

Grupo: Horizonte2020 Sociedades Seguras

ESHORIZONTE2020

Portal español del Programa Marco de Investigación e Innovación de la Unión Europea

+ info sobre programas y ayudas para la internacionalización de la I+D+I española

www.eshorizonte2020.es - www.cdti.es

@EsHorizonte2020 - @CDTIoficial

División de Programas de la UE

@EsHorizonte2020

CDTI Centro para el Desarrollo Tecnológico Industrial | E.P.E.

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI Centro para el Desarrollo Tecnológico Industrial

@CDTIoficial