MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD

CIBERDEFENSA:
Retos y oportunidades para el sector de la Defensa y Seguridad

Marina Villegas Gracias
Subdirección General de
Proyectos de Investigación (DGICT)

24 de septiembre de 2013

CIBERDEFENSA

- Seguridad y control de la información en la Red
- Todo circula por la red, se lleva a cabo y se controla desde la Red
- Ventajas: rapidez, eficacia y control
- El mercado debe sentirse seguro
- Con las mismas aplicaciones se gestiona cualquier tipo de información, sea ésta privada, pública, económica, social o militar.
- Los desarrollos informáticos tienen un uso completamente dual, tanto en el ámbito civil como en el militar. Aprovechamiento de los desarrollos realizados en el mundo civil para incorporarlos a la Ciberdefensa militar.

CIBERDEFENSA EN LA SEIDI

Antes de 2010: Seguridad , especialmente, seguridad Industrial.

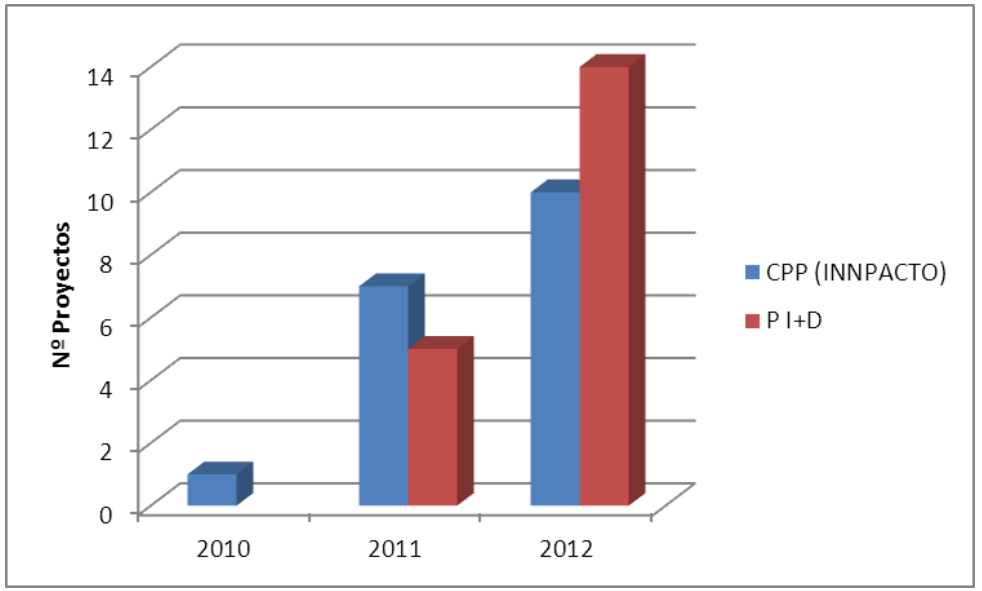
INNPACTO: llegada de las TIC

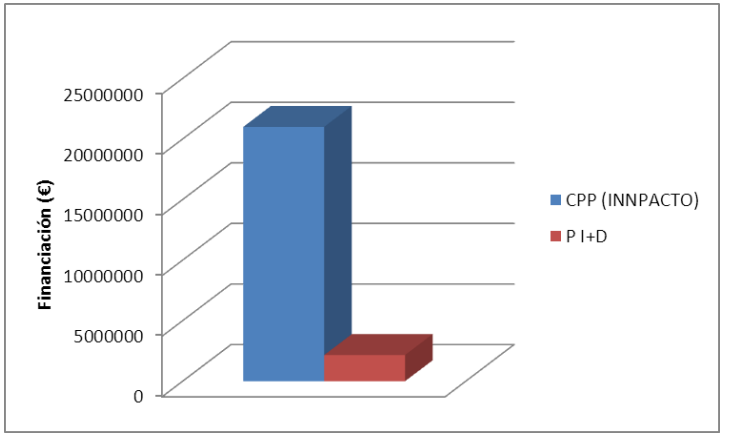
la mayoría de los proyectos financiados están relacionados con la **Ciberseguridad** de uno u otro modo.

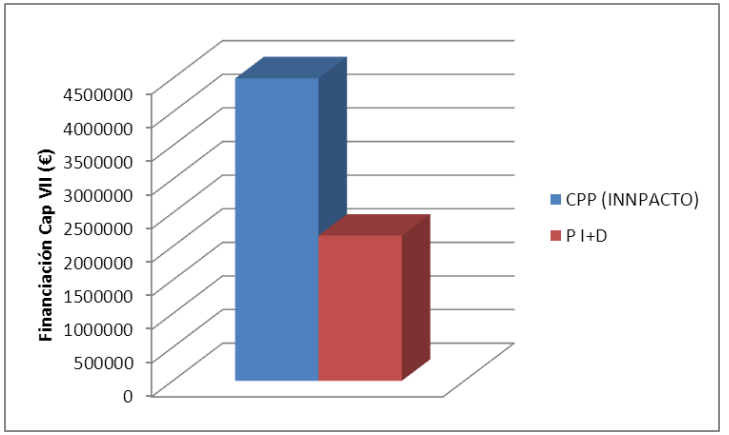
Los proyectos que financia la SEIDI suelen tener un perfil más civil/comercial dada la baja cofidencialidad en las convocatorias públicas o público-privadas.

- ✓ Mejoras en el reconocimiento de voz
- ✓ Mejoras en la adquisición de imágenes
- ✓ Incremento de la seguridad de la información

CIBERDEFENSA EN LA SEIDI



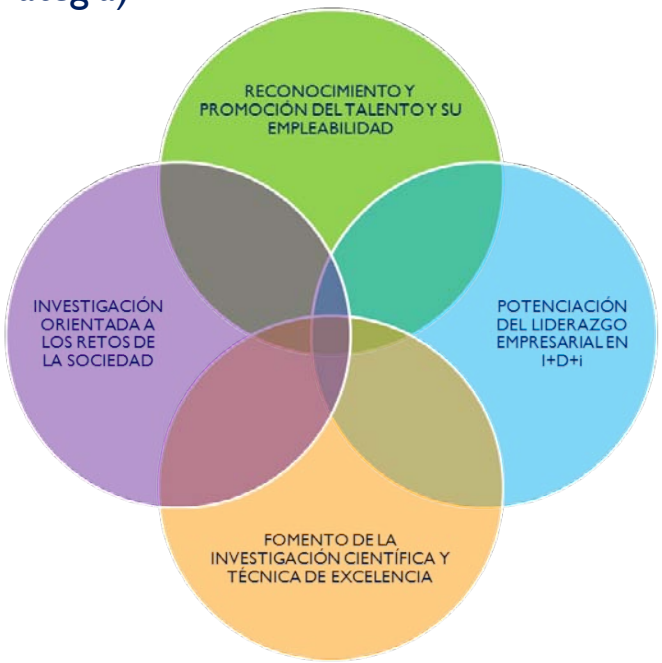




ESTRATEGIA ESPAÑOLA DE CIENCIA Y TECNOLOGÍA Y DE INNOVACIÓN

Objetivo:

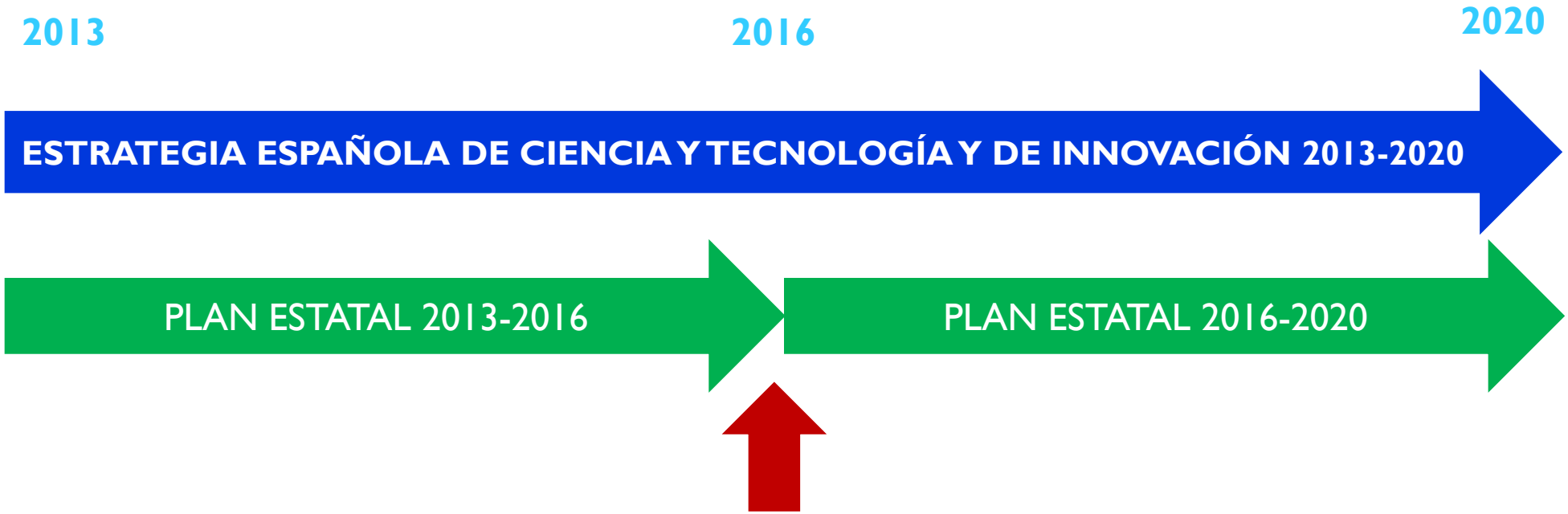
Convertir el SECTI en un sistema más competitivo, donde la capacidad de innovar se convierta en realidad, donde la investigación y la innovación no sean "cajas" estancas, sino que sean un mismo recorrido (una única estrategia)



EECTI

H2020

ESTRATEGIA ESPAÑOLA DE CIENCIA Y TECNOLOGÍA Y DE INNOVACIÓN

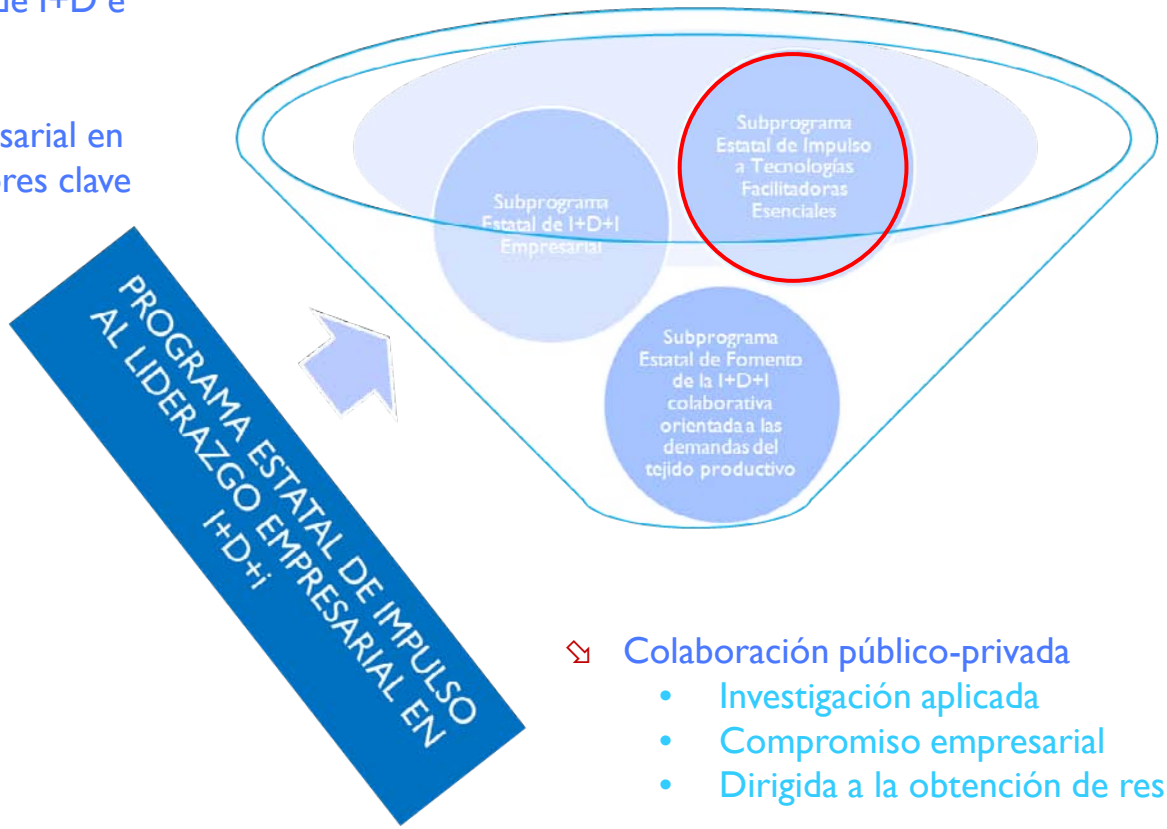


El Plan Estatal instrumentaliza los objetivos y ejes principales de la EEICTI

Estrategia Española de Ciencia y Tecnología y de Innovación 2013-2020	Programas del Plan Estatal de Investigación Científica, Técnica y de Innovación 2013-2016
Promoción del TALENTO y la EMPLEABILIDAD	Programa Estatal de Promoción del Talento y Empleabilidad
Fomento de la EXCELENCIA	Programa Estatal de Excelencia para Fomentar el Conocimiento
Impulso del LIDERAZGO EMPRESARIAL	Programa Estatal de Liderazgo Empresarial
Fomento de I+D+i orientadas RETOS DE LA SOCIEDAD	Programa Estatal de I+D+I Orientada a los Retos Globales de la Sociedad

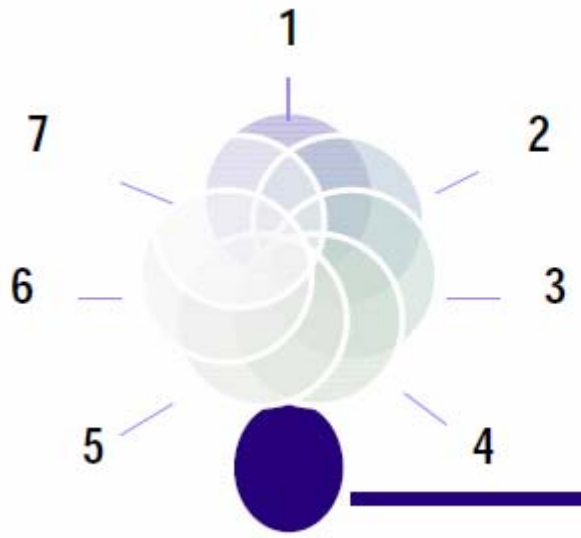
PLAN ESTATAL DE INVESTIGACIÓN CIENTÍFICA Y TÉCNICA Y DE INNOVACIÓN

- Ejecución de actividades de I+D+i
- Incorporación de PYMES a actividades de I+D e innovación
- Internacionalización de empresas
- Incremento de la competitividad empresarial en todos los sectores y en especial a sectores clave de la economía española



- Colaboración público-privada
  - Investigación aplicada
  - Compromiso empresarial
  - Dirigida a la obtención de resultados

PLAN ESTATAL DE INVESTIGACIÓN CIENTÍFICA Y TÉCNICA Y DE INNOVACIÓN



1. Salud, cambio demográfico, bienestar
2. Seguridad alimentaria, agricultura, recursos forestales, marinos e investigación en aguas continentales
3. Energía segura, limpia y eficiente
4. Transporte inteligente, integrado y no contaminante
5. Acción de Cambio Climático, recursos naturales, agua y materias primas.
6. Cambios sociales e innovación
7. Seguridad y protección de las libertades y derechos ciudadanos

8. Economía y Sociedad Digital

Los RETOS son cuestiones *-science and technology driven-* no son sectores ni disciplinas

La investigación en Ciencias Sociales y Humanidades tiene un carácter transversal a todos los RETOS

RETO EN SEGURIDAD, PROTECCIÓN Y DEFENSA

Estrategia de Tecnología e Innovación para la Defensa (ETID)

Desarrollo de tecnologías e innovaciones (desde una perspectiva global) que refuercen la seguridad y las capacidades de defensa a nivel nacional y permitan el desarrollo de un tejido tecnológico de seguridad y defensa competitivo a nivel internacional

PRIORIDADES TEMÁTICAS

- ✓ Tecnologías de sistemas de información y comunicaciones
- ✓ Tecnologías de aplicación a la protección de personas
- ✓ Tecnologías de aplicación a plataformas

RETO EN ECONOMÍA Y SOCIEDAD DIGITAL

Acción Estratégica en Economía y Sociedad Digital. Agenda Digital para España

TICs como factores clave en la mejora de la competitividad de las empresas

Quedan incluidas en el **Subprograma Estatal de Tecnologías Facilitadoras Esenciales**

TICs y servicios asociados constituyen un sector intensivo en I+D+i, cuyos avances tienen un efecto multiplicador sobre un número importante de actividades claves en la economía española

PRIORIDADES TEMÁTICAS

- ✓ **Ciberseguridad y confianza digital**
- ✓ Internet del futuro
- ✓ Redes y sistemas móviles
- ✓ Cloud computing y Open/linked/big data
- ✓ Ciudades inteligentes
- ✓ Redes sociales

RETO: proceso de transformación en el que están implicadas las empresas, las instituciones y la sociedad civil.

HORIZONTE 2020

H2020. Orientación Política y Objetivos. Clara de la Torre DG Research and Innovation European Commission

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE

Se identifican **5** prioridades estratégicas:

I. Alcanzar «ciber-resistencia»
II. Reducir drásticamente el «ciber-crimen»
III. Desarrollar la política de ciberdefense y las capacidades relacionadas con la Política de Seguridad y Defensa común (CSDP)
IV. Desarrollo de recursos industriales y tecnológicos para ciberseguridad
V. Establecimiento de una política internacional del ciberespacio coherente en la UE que promueva los valores europeos fundamentales

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE

«Fostering R&D investments and innovation»

La I+D puede apoyar una fuerte política industrial, promover una industria europea en **tecnologías de la información y la comunicación** (**ICT**) fiable, impulsar el mercado interior y reducir la dependencia europea de las tecnologías extranjeras

Tiene que complementarse con esfuerzos para trasladar la I+D en soluciones comerciales mediante incentivos

Horizonte 2020 financiará investigación en seguridad relacionada con **ICTs** emergentes, proveerá de incentivos para la implementación y adopción de soluciones ya existentes y abordará la interoperatividad entre las redes y los sistemas de información

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE

La Comisión:

- Usará H2020 para abordar, desde la I+D y la innovación, las **ICTs** en los campos de la privacidad y la seguridad
- Establecerá mecanismos para coordinar mejor las agendas estratégicas de los EEMM y para incentivar a los EEMM para que inviertan más en I+D

Los EEMM:

- Promover el desarrollo de buenas prácticas para el uso del la **compra pública innovadora** para estimular el desarrollo y despliegue de características para la seguridad en los productos y servicios de las **ICTs**
- Promover la implicación de la industria y la academia en el desarrollo y coordinación de las soluciones propuestas. Esto debe hacerse además con la coordinación entre las agendas de I+D de las organizaciones civiles y militares

HORIZONTE 2020

European Commission: «look for the challenges, technological gaps and necessary research directions related to cybersecurity and the best suited instruments to implement the tasks»

Siempre teniendo en cuenta de que en H2020 y, especialmente, en el pilar dedicado a los Retos de la Sociedad tendrá especial importancia el apoyo a actividades cercanas al mercado

Se identifican **5** retos que deben abordarse para aumentar el nivel global de **ciberseguridad**:

1. Afrontar las necesidades desde la perspectiva del usuario
2. Construcción (del entorno de la ciberseguridad)
3. Hacer de la ciberseguridad un caso de negocio positivo
4. El papel de la tecnología
5. Definición de las medidas en ciberseguridad

HORIZONTE 2020

Para abordar estos **5** retos se proponen la búsqueda/propuesta de los mejores **instrumentos**:

a) Actividades de I+D
b) Demostradores
c) Infraestructuras
d) Apoyo a los usuarios
e) Incentivos

Programa de Trabajo Reto 6: Inclusive, innovative and secure societies

Muchas gracias!!!!

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE

1. Abordar las necesidades desde la perspectiva del usuario
   - ***Usabilidad y efectividad*** *de la seguridad de los productos y aplicaciones de las ICTs, o características de seguridad en función de una aproximación basada en el riesgo*
   - ***Percepción*** *pública de la ciberseguridad*
   - ***Educación*** *y entendimiento de los aspectos de seguridad de las ICTs*
   - *Conciencia de que el uso de las ICTs tiene algunos riesgos y de que el usuario debe protegerse a sí mismo y a otros*
   - *Más* ***políticas*** *de seguridad que no se centren en el usuario*

2. Construcción
   - ***Disuasión****. Teniendo en cuenta que la ciberseguridad es asimétrica, el esfuerzo para la protección es mucho mayor que el esfuerzo para perpetrar un ataque*
   - ***Inteligencia****. Actualmente no hay una fuente central de información de confianza*
   - ***Colaboración****. Actualmente no se comparten suficientemente los incidentes, riesgos y vulnerabilidad de los sistemas*
   - *Hay insuficiente* ***cooperación*** *público-privada para asegurar la ciberseguridad*

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE

3. Ciberseguridad: Un caso de éxito…
   - ***Economía***. *No hay datos fiables del coste de la ciberseguridad*
   - ***Acceso***. *La soluciones propuestas y su coste no parecen asequibles*
   - ***Feedback***. *No existe un feedback referente al nivel de seguridad de un producto o de la calidad de la seguridad*

4. Papel de la tecnología
   - ***Seguridad a través del diseño***. *No existen especificaciones en el diseño de las ICT para ciberseguridad*
   - ***Cultura***. *No hay cultura de manejo de riesgos*
   - ***Escala***. *Las soluciones son «todo o nada», no son escalables en función del nivel o complejidad del riesgo*
   - ***Especificidad***. *Actualmente las soluciones de seguridad son específicas del dispositivo o aplicación en la que se implementan*

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION: AN OPEN, SAFE AND SECURE CYBERSPACE

5. Definición de la métrica en ciberseguridad
   - ***Rapidez***. *Actualmente el tiempo para encontrar medidas de apoyo en la Comisión no permite un rápida respuesta en una emergencia*
   - ***Acuerdo***. *No hay reglas, normas ni buenas prácticas comunes a nivel de la UE respecto a la seguridad*
   - ***Benchmarking***. *Dificultad para comparar los productos*
   - ***Dependencia***. *La mayoría de las aplicaciones más populares (p. ej. Redes sociales) no se han desarrollado en Europa*
   - ***Certificación***. *Consume tiempo y no es obligatoria para la mayoría de aplicaciones y dispositivos*

HORIZONTE 2020

a) Actividades de I+D
   - *Investigación experimental, uso de proyectos de I+D maduros*

b) Demostradores
   - *Prototipos a gran escala (incluidos los de viabilidad), proyectos de prueba de concepto, proyectos de lanzamiento*

c) Infraestructuras
   - *Laboratorios públicos de innovación, líneas de fabricación de prototipos, observatorios de tecnología, laboratorios de simulación, infraestructuras «en la nube», ciber-ejercicios, certificación europea, «líneas calientes» de seguridad, ...*

d) Apoyo a los usuarios
   - *Formación y educación de usuarios individuales y corporativos, «universidad» europea en seguridad, programas de concienciación, construcción de «comunidad»*

e) Incentivos
   - *Búsqueda de ofertas, apoyo rápido a soluciones, compra pública innovadora, apoyo a negocios de desarrollo de soluciones de seguridad, competitividad de planes de negocio, programas industriales, co-inversión, premios en seguridad*