



Estudio de viabilidad, oportunidad
y diseño de una red de centros
de excelencia en I+D+I en ciberseguridad

INSTITUTO NACIONAL DE

CIBERSEGURIDAD

SPANISH NATIONAL

CYBERSECURITY INSTITUTE

 **incibe**_

Autor

INCIBE

Este estudio ha sido elaborado con la colaboración de diversos agentes representativos del ecosistema nacional de I+D+i en ciberseguridad. El **Anexo I PARTICIPANTES EN EL ESTUDIO** contiene un listado completo de las entidades y sus representantes que han colaborado en el estudio.

Mayo 2015

La presente publicación pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y está bajo una licencia Reconocimiento-No comercial 3.0 España de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento. El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE o CERTSI como a su sitio web: <http://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de CERTSI como titular de los derechos de autor. Texto completo de la licencia: <http://creativecommons.org/licenses/by-nc-sa/3.0/es/>

ÍNDICE

1 PUNTO DE PARTIDA Y MOTIVACIÓN DEL ESTUDIO	5
1.1 Contexto y objetivo del estudio	5
1.2 Estructura.....	6
1.3 Principales conclusiones	6
2 MARCO DE ANÁLISIS.....	13
2.1 Modelo de análisis	13
2.2 Metodología.....	13
2.3 Consideraciones iniciales	15
3 POSICIONAMIENTO COMPETITIVO DEL ECOSISTEMA DE I+D+I EN CIBERSEGURIDAD 17	17
3.1 Mapa de Agentes	17
3.2 Análisis del contexto institucional, jurídico y económico.....	19
3.3 Caracterización del ecosistema de I+D+i en ciberseguridad	22
3.3.1 Recursos	22
3.3.2 Modelo de generación de valor de la I+D+i	25
3.3.3 Resultados	28
3.4 Modelo de relación del ecosistema de I+D+i en ciberseguridad.....	29
3.4.1 Principales redes o modelos colaborativos nacionales	29
3.4.2 Principales redes o modelos colaborativos internacionales.....	32
3.5 Factores limitantes a la competitividad de la I+D+i en ciberseguridad.....	33
3.5.1 Carencias y obstáculos generales y estructurales.....	34
3.5.2 Carencias y obstáculos específicos de la ciberseguridad.....	34
3.5.3 Conclusiones	35
3.6 Análisis DAFO del ecosistema de I+D+I en ciberseguridad.....	36
3.7 Plan de actuaciones para el incremento de la competitividad del ecosistema de I+D+i en ciberseguridad	38
4 ANÁLISIS DE OPORTUNIDAD Y DAFO DE LA CREACIÓN DE UNA RED DE CENTROS DE EXCELENCIA EN I+D+I EN CIBERSEGURIDAD.....	43
4.1 Análisis de Oportunidad.....	43
4.2 Análisis DAFO	43
5 ALTERNATIVAS DE MODELOS DE RED DE EXCELENCIA	45
5.1 Valoración multicriterio de alternativas del modelo de red de Excelencia.....	47
5.2 Presentación y validación de alternativas con los interesados	48
6 MODELIZACIÓN DE LA RED.....	50
6.1 Formulación estratégica de la red	52
6.1.1 Misión, visión y valores	52
6.1.2 Objetivos estratégicos, líneas de actuación y medidas	54
6.2 Alineamiento estratégico con el proyecto del polo tecnológico en ciberseguridad .	55
7 PLAN DE ACCIÓN: HOJA DE RUTA DE ACTUACIONES A CORTO, MEDIO Y LARGO PLAZO	57
7.1 Fase 0: Definición colaborativa.....	57

7.2 Fase 1: Arranque del piloto.....	58
7.3 Fase 2: Despliegue	58
7.4 Fase 3: Estabilización	59
7.5 Fase transversal: Gestión de la implantación	59
7.6 Calendario Plan de Acción	59
Anexo I PARTICIPANTES EN EL ESTUDIO	61
AI.1 Entrevistas.....	61
AI.2 Cuestionarios	62
AI.3 Participantes en los Focus Group	64
AI.3.1 Primer Focus Group.....	64
AI.3.2 Segundo Focus Group.....	64
Anexo II LÍNEAS ESTRATÉGICAS Y MEDIDAS	66
Anexo III FUENTES DOCUMENTALES CONSULTADAS	70
Anexo IV AGENTES DEL ECOSISTEMA DE I+D+I EN CIBERSEGURIDAD EN ESPAÑA.....	74
Anexo V REDES COLABORATIVAS ANALIZADAS	79

1

PUNTO DE PARTIDA Y MOTIVACIÓN DEL ESTUDIO

1.1 Contexto y objetivo del estudio

El Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Industria, Energía y Turismo (MINETUR), a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación española y empresas, especialmente para sectores estratégicos.

En el marco del Plan de Confianza en el Ámbito Digital derivado de la Agenda Digital para España, INCIBE ha impulsado la realización del **“Estudio de la viabilidad, oportunidad y diseño de una Red de Centros de Excelencia en I+D+i en ciberseguridad”**.

Este estudio ha tenido como objetivo conocer el contexto y las dinámicas bajo las cuales se desarrolla la I+D+i en ciberseguridad en España, con el fin de determinar la idoneidad y pertinencia en la creación de una red de centros de excelencia en I+D+i en ciberseguridad.

La futura red se orientaría a superar la fragmentación de la investigación, aglutinando la masa crítica de las mejores capacidades, activos y talentos científicos y tecnológicos, propiciando de este modo la mejora de la competitividad del ecosistema español de I+D+i en ciberseguridad.

El presente documento presenta una síntesis de los principales resultados obtenidos tras la ejecución del estudio.

Un trabajo ejecutado bajo un enfoque participativo, colaborativo y consensuado.

La caracterización de un ecosistema como el de la ciberseguridad, de gran complejidad y amplitud, no tendría sentido sin considerar la visión, experiencia y opinión de los agentes que lo componen, verdaderos conocedores de las dinámicas, capacidades tanto del propio ecosistema, así como de las carencias, debilidades y problemáticas que presenta. Por ello, el estudio se ha realizado con la participación y la inteligencia del ecosistema como eje motor.

El estudio ha contado con la colaboración de un grupo de agentes representativos pertenecientes a las cuatro grandes tipologías de entidades que conforman cualquier ecosistema de este tipo: Administración Pública, Sector Académico, Organismos de Soporte a la I+D+i e Industria. Dichos agentes han aportado su visión sobre el estado actual del ecosistema así como de las problemáticas y retos a las que se enfrenta la ciberseguridad.

El estudio refleja la “inteligencia global”, materializada en las visiones y opiniones que han contado con un consenso y respaldo mayoritario por parte de los participantes en el estudio. De este modo, se garantiza la representatividad de los resultados obtenidos.

La inteligencia ha participado a lo largo de todo el estudio, no sólo en la identificación del estado del arte de la I+D+i en ciberseguridad y los retos que debe abordar nuestro país para mejorar su posicionamiento. Igualmente, ha participado activamente en la identificación, validación y definición consensuada de las premisas básicas y misión que debería guiar la creación de la futura Red de Excelencia, así como los objetivos que se incluirían dentro de su agenda.

1.2 Estructura

Los contenidos de este documento se han estructurado de acuerdo a la lógica seguida durante la ejecución del estudio:

En primer lugar se presenta, a modo de resumen ejecutivo, las principales conclusiones, en términos del posicionamiento del ecosistema de I+D+i en ciberseguridad y los retos que debe abordar, la viabilidad en la creación de una Red de Excelencia y los elementos estratégicos que deberían guiar su creación y actividad.

El apartado [MARCO DE ANÁLISIS] ilustra la metodología que ha guiado la elaboración del estudio. A continuación se muestran los principales resultados de la radiografía y diagnóstico del ecosistema, a nivel de recursos disponibles, dinámicas de producción de valor y resultados obtenidos. Esta radiografía se complementa con el estado del arte en lo relativo a los modelos y dinámicas de colaboración presentes en el ecosistema.

Como resultado de esta radiografía y diagnóstico, se exponen los principales limitantes y los retos que deberá afrontar el ecosistema para mejorar su competitividad, así como una propuesta de plan de actuaciones para abordar dicha mejora.

Este encuadramiento de la I+D+i en ciberseguridad permite avanzar hacia el siguiente paso, determinar la idoneidad y viabilidad de crear una Red de Excelencia, propiciando un salto en la producción de valor y en los resultados del ecosistema.

Se presentan las principales alternativas de modelos de red para dar respuesta a los retos planteados, que, consensuada y colaborativamente, se ha considerado como más factible e idóneo para la futura red.

El estudio se cierra con la caracterización estratégica de la red (misión, valores y objetivos estratégicos) y un plan de acción para la puesta en marcha de sus actividades en los próximos años.

A modo de información complementaria, los anexos al documento detallan los participantes en el estudio, las fuentes documentales consultadas, una aproximación al mapa de agentes de la I+D+i en ciberseguridad en España y el detalle de modelos colaborativos analizados.

1.3 Principales conclusiones

La oportunidad: posicionar la I+D+i española en la arena global

Con carácter general y teniendo en cuenta las limitaciones en la cuantificación de la ciberseguridad, cabe destacar que España no dispone de un claro posicionamiento de la I+D+i a nivel internacional, no figurando dentro de los *best in class* en ninguna de las áreas científico-tecnológicas en las que podría encuadrarse la ciberseguridad¹.

Nuestro país se encuentra por detrás de otros países europeos, presentando una importante brecha tecnológica tanto en investigación y en transferencia. Los países líderes (Estados Unidos, Israel, Reino Unido) presentan como factores diferenciales políticas y focos de investigación claros y una inversión en I+D+i a medio y largo plazo, que permita la maduración necesaria para obtener retornos. Esta brecha también se replica a nivel europeo, donde nos encontramos por detrás de países como Francia, Alemania y Holanda.

Existen en nuestro ecosistema una serie de limitaciones que explican este débil posicionamiento y que configuran un entorno que no favorece un posicionamiento entre los referentes mundiales de la ciberseguridad.

Muchos retos por delante

Nuestro ecosistema deberá resolver estas limitaciones (retos) para abordar la mejora de su competitividad y resultados. Estos retos, de profundo calado e impacto, junto a la escasez de redes y modelos de colaboración en la I+D+i en ciberseguridad, constituyen una oportunidad y justifican la **necesidad de crear una Red de Excelencia** que, a través de la conexión, puesta en común y explotación de los activos, de respuesta a dichos retos.

La red jugaría sin duda alguna un papel clave en el futuro del ecosistema, al dar los primeros pasos hacia un ecosistema más cohesionado, unido y con mayores sinergias, que redunden en mayores niveles de I+D+i.

Buena parte de estos retos están relacionados con debilidades estructurales y coyunturales del Sistema de Ciencia y Tecnología, que no han acompañado en los últimos años al impulso de un sector tan estratégico y crítico; de un lado, la crisis económica ha supuesto una restricción del crédito presupuestario de la I+D+i, que obviamente ha afectado a la ciberseguridad; de otro, las debilidades estructurales del Sistema de Ciencia y Tecnología y los factores culturales (aversión al riesgo, baja cultura colaborativa) constituyen un freno para la generación de I+D+i en nuestro país.

Asimismo, también existen retos específicos de la I+D+i en ciberseguridad, pues son muchos los elementos que aún están pendientes de desarrollo en nuestro país. Destacan la necesidad de establecer un foco o estrategia clara por parte del Estado sobre las prioridades a partir de las cuales articular la I+D+i, revertir la tendencia hacia la escasez de presupuestos y fomentar un mercado interno más amplio, a través de una mayor tracción en la demanda de soluciones de ciberseguridad, principalmente por parte de la Administraciones Públicas y el Estado.

¹ En el marco del estudio, se han identificado como grandes grupos de áreas científico-tecnológicas las siguientes: investigación, movilidad, hardware, ciberdefensa/ciberataque, secure coding y procedimientos/operaciones.

Aprovechar el momentum generado, poniendo en valor las capacidades del ecosistema para pasar una nueva etapa de la ciberseguridad en España

Sin embargo, las importantes capacidades de nuestro país en I+D+i, la sensibilización que los agentes del ecosistema tienen sobre la necesidad de resolver los retos, junto a la gran predisposición de éstos para embarcarse en una nueva etapa para la I+D+i en ciberseguridad, juegan a favor, al ser el combustible que permitirá dar el salto hacia una nueva etapa.

Esta predisposición del ecosistema para construir la nueva generación de la ciberseguridad debe estar acompañada de los cambios y actuaciones que la Administración Pública, desde su rol de facilitador e impulsor, ha de emprender inexcusablemente para que este salto pueda ser una realidad. Elementos como el desarrollo de estrategias con focos concretos, el establecimiento de una Agenda en I+D+i específica, el posicionamiento en la Unión Europea o los desarrollos necesarios en el campo normativo o de certificaciones, son parte de las condiciones contextuales que este cambio exige.

Igualmente, para conformar una “solución ganadora”, esta apuesta debe ser seria, con compromisos y presupuestos claros, lejos de planteamientos teóricos y declaraciones de intenciones que no se traducen en resultados tangibles y reales.

Un breve repaso por el estado del arte de la I+D+i en ciberseguridad

La situación actual de la I+D+i en ciberseguridad permitirá esbozar los retos a los que se enfrenta el ecosistema y sobre los que la red jugará un papel clave.

Un sector dinámico con muchas oportunidades

Son muchas las oportunidades que presenta el sector de la ciberseguridad, destacando algunos factores tales como:

- El incremento en número, tipología y sofisticación de las amenazas.
- El mayor número de vulnerabilidades, debido al uso cada vez más generalizado de la tecnología (en especial tecnología móvil y soluciones en la nube).
- Una conciencia creciente de las organizaciones y de los consumidores sobre las amenazas de seguridad.
- La regulación, que impone obligaciones sobre protección de datos personales, la información y las infraestructuras que la soportan.

Un contexto institucional que ha dado los primeros pasos, pero que debe concretar los focos y prioridades

La ciberseguridad figura como asunto clave en la agenda gubernamental española; el Gobierno de España hace suya la problemática planteada por la Unión Europea (Estrategia

Europea de Ciberseguridad), estableciendo una serie de estrategias con compromisos en materia de ciberdelito, seguridad de las administraciones públicas y ciberdefensa².

A pesar de que estas estrategias son un importante paso, son planteamientos de alto nivel que se traducen en declaraciones de intenciones que delimitan el problema y ofrecen soluciones generales, pero que han de ser concretadas y aterrizzadas.

Es especialmente llamativa la ausencia de focos temáticos o prioridades en estas estrategias. Los agentes participantes en el estudio consideran que es necesario un desarrollo claro para la I+D+i en ciberseguridad, con foco y financiación, que muestre las prioridades y el “camino” para que el ecosistema pueda orientarse en la dirección marcada. Buena parte de los agentes participantes en el estudio reclaman la creación de un programa o agenda específica de I+D+i en ciberseguridad.

La legislación vigente a la fecha de realización de este estudio, viene marcada por el desarrollo de aspectos normativos concretos, si bien, al igual que el caso de las estrategias, aún queda mucho camino por recorrer. Es de esperar que en el futuro, conforme se vayan creando las políticas de ciberseguridad, el marco normativo se vaya convirtiendo en un elemento mucho más amplio.

Un ecosistema con amplia capacidad para generar más valor

Nuestro ecosistema es amplio y diverso, ya que se compone de más de 300 agentes (pertenecientes a la ciencia, la industria, la administración y los organismos de soporte a la I+D+i). Sin embargo, está fuertemente fragmentado y desconectado, al presentar unas dinámicas de relación entre sus agentes más puntuales que generales y sin un foco concreto en su actividad. Se trata, en definitiva, de un ecosistema de que no aprovecha todas las sinergias que la colaboración puede aportar, lo que se le sitúa probablemente muy por debajo de sus capacidades.

Los resultados de la actividad de I+D+i son escasos en términos de transferencia y aplicabilidad al mercado. Esto supone que muchas publicaciones y patentes no se convierten en productos o servicios con aplicación en el mercado. Los escasos incentivos del Sistema de Ciencia y Tecnología para la transferencia de los resultados de la investigación hacia el mercado es uno de los principales limitantes para revertir esta tendencia.

Son los agentes especializados en transferencia (Organismos de Soporte a la I+D+i) los que deben tomar el liderazgo en el proceso de transferencia y comercialización de los resultados de la investigación hacia la industria, requiriendo para ello una profunda revisión de sus mecanismos de transferencia e incentivos.

² La Estrategia de Ciberseguridad Nacional (ECSN), encuadrada dentro de la Estrategia de Seguridad Nacional (ESN), la Estrategia de Seguridad Marítima, también encuadrada en la ESN, con una acción específica relativa a la ciberseguridad en el ámbito marítimo y la Agenda Digital para España (inspirada en la Agenda Digital para Europa contempla) que desarrollar el Plan de Confianza Digital, materializando las actuaciones en materia de confianza digital.

Sin embargo, y a pesar de todos estos limitantes, es un ecosistema relativamente joven y con múltiples activos, por lo que existe un amplio margen de recorrido y mejora en la explotación y puesta en valor de sus capacidades.

Un marco financiero escaso para la I+D+i

España presenta una clara debilidad en la financiación, con niveles de inversión inferiores a los países líderes³. Esto supone una merma de la capacidad competitiva de la industria y del sistema de investigación, cuyas consecuencias impactarán en el largo plazo, al ser los retornos de la I+D+i relativamente largos en el tiempo.

A pesar de que la estrategia de I+D+i (Plan Estatal de Investigación Científica, Técnica y de Innovación 2013-2016) menciona la ciberseguridad como prioridad temática, no se concreta su alcance a nivel de recursos presupuestarios, considerándose un plan “financieramente escaso”. El sector privado ha acusado también la restricción presupuestaria, como consecuencia de la crisis económica, con fuertes recortes en la inversión en I+D+i.

Finalmente, la falta de tracción de la Administración, no sólo por el bajo nivel de concreción en las políticas de ciberseguridad, sino también por la ausencia de presupuestos en los organismos públicos que han de implantar estas soluciones en sus propias instancias, agrava el problema, añadiendo una dimensión “de demanda” a la ya de por sí compleja situación presupuestaria.

Un reducido mercado en España que limita el crecimiento de las soluciones de I+D+i

Los bajos niveles de demanda de soluciones de ciberseguridad en España configuran un reducido mercado. La baja sensibilización de la necesidad de protección frente a ciberataques por parte de consumidores, empresas y Administración Pública (ámbito civil, defensa e inteligencia) sería un claro factor que explicaría esta baja demanda. Se hace por tanto necesario seguir avanzando en la cultura de la ciberseguridad en nuestro país.

Además, se reclama por parte de los agentes participantes en el estudio acciones orientadas a potenciar las soluciones españolas y un mayor impulso en la Administración Pública de la demanda de soluciones innovadoras.

El talento como una de las grandes preocupaciones

La principal problemática del talento en España, por su recurrencia en las conversaciones mantenidas con los agentes del ecosistema que han participado en este estudio, es la fuga de talento hacia otros países, en busca de mejores oportunidades. Esto plantea una situación extremadamente preocupante, dado que la ciberseguridad es un ámbito que requiere de talento especializado y en el que la formación de profesionales requiere de tiempo y madurez. Todo ello en un contexto en el que se prevén fuertes necesidades de profesionales para los próximos años.

³ Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la Agenda Digital para España, publicado en 2012.

Uno de los principales factores que contribuyen a frenar la capacidad del ecosistema para retener y reconocer el talento son las deficiencias del Sistema de Ciencia y Tecnología, cuya precariedad en la retribución no contribuye a generar una percepción de la investigación como opción profesional. A ello se une la necesidad de organizar y estructurar el talento, a través de enfoques específicos para la formación de profesionales e investigadores en ciberseguridad, que permitan establecer un itinerario y un perfil formativo claro.

El papel de la futura Red de Excelencia

A la vista del diagnóstico del ecosistema, la red podría jugar un papel clave en la búsqueda e implementación de las soluciones que den respuesta a los retos planteados, caminando hacia un ecosistema fuerte, cohesionado, robusto y con capacidad de posicionarse en la “liga de los ganadores”.

Como consecuencia del proceso colaborativo realizado con los agentes del ecosistema, se identificó preliminarmente que la red podría colaborar en la resolución de los siguientes retos:

- Definición de un plan o agenda de la I+D+i en ciberseguridad a nivel nacional así como una estrategia de posicionamiento de España en el programa Horizonte 2020.
- Identificación de los mecanismos de incentivación de la investigación.
- Sensibilización y concienciación sobre la necesidad de proteger la información, los sistemas y las redes ante las ciberamenazas y los ciberataques.
- Identificación de las capacidades, potencial y nivel de excelencia del ecosistema.
- Revisión de los mecanismos de retención y atracción del talento, que contribuyan a frenar la fuga de talento.
- Identificación de puntos de interés común en el ecosistema y la generación de incentivos de colaboración en torno a ellos.
- Identificación de las necesidades del mercado para el desarrollo de soluciones con foco comercial.

Misión y objetivos de la Red de Excelencia

Durante el proceso de formulación estratégica de la red, se destacaron como elementos clave para la actividad de la red:

- Objetivos concretos, tanto a largo como a corto plazo, con foco en la I+D+i y en la transferencia de los resultados de la investigación al mercado.
- Capacidad de respuesta en un contexto en el que la velocidad del cambio tecnológico exige una respuesta flexible, abierta y rápida. No sólo las tecnologías avanzan a ritmo exponencial, sino también las ciberamenazas y ciberataques.
- Coordinación con el Gobierno y las Administraciones Públicas responsables del desarrollo de la ciberseguridad para poder generar las respuestas adecuadas de forma coordinada y colaborativa.
- Excelencia como eje rector de la Red.

Poner en valor los recursos de I+D+i como misión primordial de la Red.

La principal razón de ser de la red será contribuir a la mejora de la competitividad, buscando el desarrollo de soluciones que respondan a necesidades del mercado. Para ello, trabajará activamente en superar la fragmentación actual del ecosistema, a través de las acciones que permitan explotar las capacidades del ecosistema de forma colaborativa, sinérgica y conjunta.

A fecha de elaboración de este documento, las medidas específicas y sus prioridades para el cumplimiento de los objetivos estratégicos, líneas de actuación son objeto de debate y consenso con los agentes colaboradores del estudio. Estas se describen en el **Anexo II LÍNEAS ESTRATÉGICAS Y MEDIDAS** si bien pueden sufrir modificaciones.

2 MARCO DE ANÁLISIS

2.1 Modelo de análisis

El proceso para la realización del estudio se ha realizado a partir del siguiente **modelo general de análisis**, que refleja el conjunto de activos, agentes y dinámicas que permiten la producción de valor en el ecosistema de I+D+i en ciberseguridad.

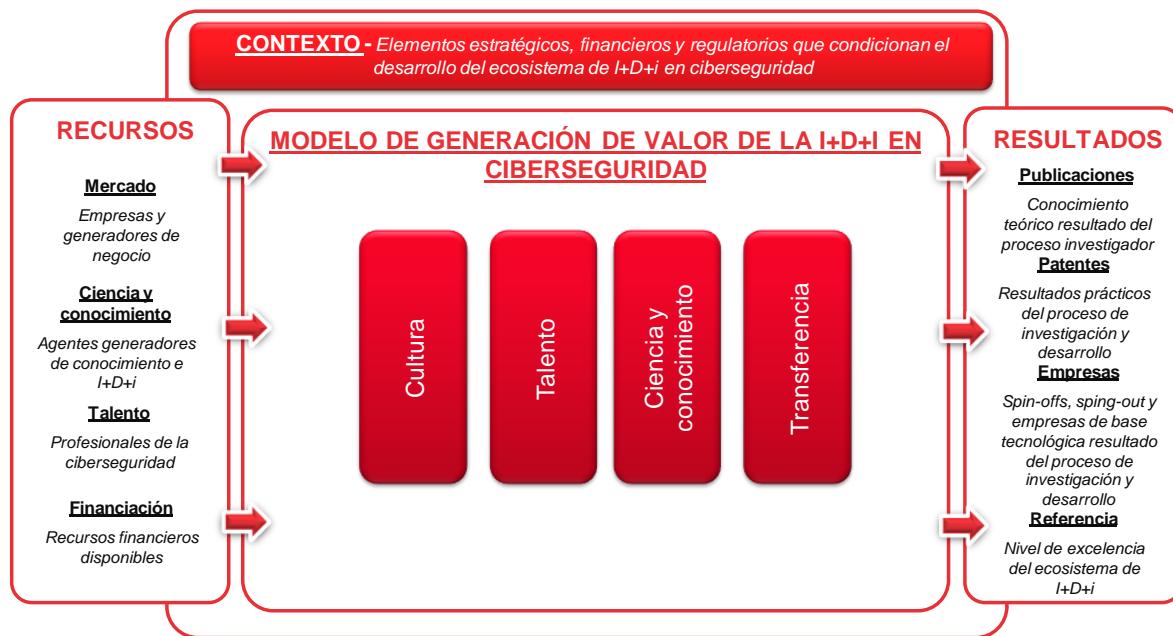


Figura 1: *Modelo general de análisis*.

Desde esta perspectiva, se ha empleado una abstracción simplificada del ecosistema que consiste en verlo como un “sistema” que, a partir de unos **recursos** disponibles, genera valor en sus **resultados** fundamentales.

- **Recursos:** ¿de qué elementos dispone el ecosistema para producir valor?
- **Resultados:** ¿cuál es el resultado real y el valor producido por el ecosistema?
- **Modelo generación de valor de la I+D+i:** ¿de qué “vehículo” de producción de valor dispone el ecosistema?

2.2 Metodología

La metodología para la realización del estudio se basa en un doble enfoque:

- **Ejercicio de reflexión colectiva** con diferentes agentes clave del ecosistema que han aportado su visión y perspectiva. Para aumentar la representatividad de los participantes, éstos pertenecen a diferentes colectivos, incluyendo expertos, empresas, universidades, centros tecnológicos e instituciones públicas. La participación se ha realizado a través de los siguientes mecanismos:

- **Conversaciones individuales, privadas y anónimas**, con el objeto de obtener opiniones libres, a un total de 18 agentes de ecosistema (15 de ámbito nacional y 3 de ámbito internacional).
- **Remisión de cuestionarios** para su cumplimentación a un total de 65 agentes del ecosistema.
- **Contraste con INCIBE** de los resultados obtenidos en los ejercicios de reflexión colectiva, a través de una sesión Think Tank. El objetivo de esta sesión fue alinear los aspectos de la Red perfilados por la Inteligencia Colectiva con los documentos estratégicos que justifican tanto este estudio como la propia iniciativa de la constitución de la Red de Excelencia.
- **Sesiones Focus Group** orientadas a generar una discusión libre y guiada para ultimar aspectos relevantes de la Red con el mayor grado de consenso posible. Se celebraron dos sesiones con la participación de un grupo de agentes relevantes.

El Anexo I PARTICIPANTES EN EL ESTUDIO incluye el listado de las entidades y personas que han colaborado en la elaboración de este estudio.

- Para complementar estas opiniones, se ha realizado un contraste con **información analítica y fuentes documentales disponibles para la ciberseguridad** tanto a nivel nacional como internacional, procedente de diversas fuentes de referencia.

El Anexo III FUENTES DOCUMENTALES CONSULTADAS incluye el detalle de las fuentes analizadas durante la elaboración del estudio.

El objetivo de este análisis combinado fue lanzar, en una primera etapa, un **análisis divergente** que permitió identificar el universo de potenciales escenarios de solución, para, en una segunda fase, **converger** hacia aquellos escenarios más factibles en el desarrollo e implementación de la futura Red de Centros de Excelencia en I+D+i en ciberseguridad.

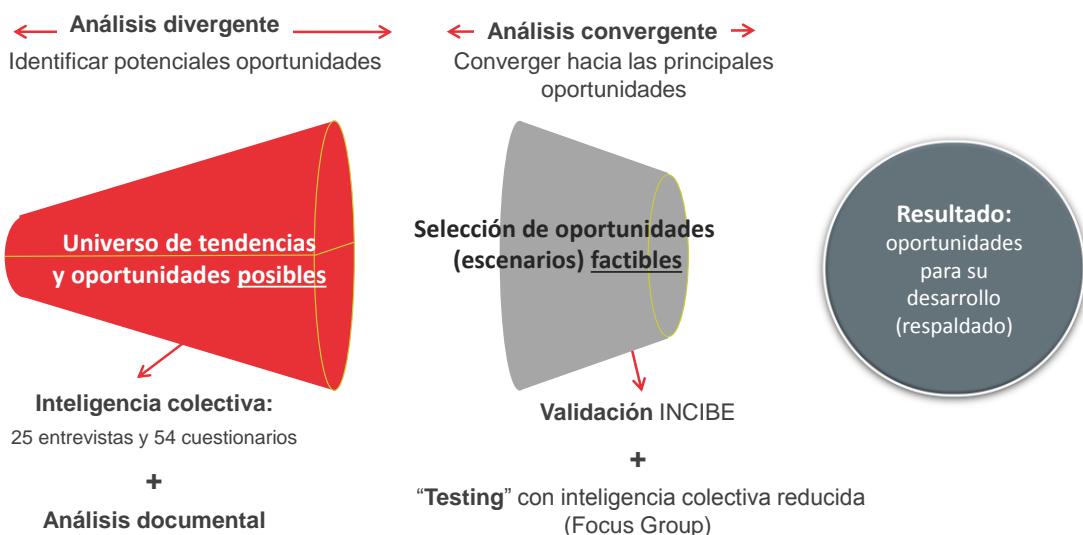


Figura 2: Metodología de análisis.

2.3 Consideraciones iniciales

La interpretación de los resultados del estudio debe hacerse teniendo en cuenta una serie de elementos que condicionan los resultados del mismo.

En primer lugar, la ciberseguridad es un concepto relativamente novedoso y emergente, lo que supone la **práctica inexistencia de estudios y estadísticas específicas** que permitan la realización de un análisis sistemático.

Por otro lado, se trata de un área transversal, con aplicaciones prácticamente en todos los ámbitos de las Tecnologías de la Información y las Comunicaciones (TIC) y en todos los sectores productivos, lo que **hace complejo la obtención de datos económicos que permitan cuantificar tanto la industria como el nivel de I+D+i** de ésta⁴.

Finalmente, se trata de un concepto que tanto por sus múltiples aplicaciones como por sus implicaciones (normativas, civiles, militares, tecnológicas) resulta muy amplio en sus interpretaciones. Más concretamente, en el ámbito de la I+D+i, **la multiplicidad de agentes y áreas científico-tecnológicas y de conocimiento⁵, ha incrementado la complejidad del trabajo**, lo que, unido a la escasez de datos, hace que el análisis de la I+D+i en ciberseguridad no se haya podido realizar global y sistemáticamente.

Como consecuencia, **el análisis realizado no a ha tenido a disposición los datos y estadísticas que serían necesarias** para poder evaluar la I+D+i en ciberseguridad desde un punto de vista cuantitativo de forma exhaustiva. A pesar de ello, se ha tratado de solventar esta dificultad a través de búsquedas e investigaciones dirigidas, basadas en el

⁴ La inexistencia de fuentes públicas y estadísticas que permitan evaluar detalladamente la ciberseguridad, ha tenido como consecuencia la imposibilidad de realizar una evaluación de la capacidad y excelencia investigadora en nuestro país.

conocimiento del ecosistema por parte de INCIBE y de los agentes que han participado en el estudio.

3 POSICIONAMIENTO COMPETITIVO DEL ECOSISTEMA DE I+D+I EN CIBERSEGURIDAD

3.1 Mapa de Agentes

Para encuadrar la situación actual del ecosistema de I+D+i en ciberseguridad, una de las primeras tareas a emprender es el levantamiento del mapa de agentes tanto a nivel nacional como a nivel internacional.

Es necesario destacar la **escasez de fuentes de información formales y estructuradas** que recopilen y caractericen la totalidad de los agentes del ecosistema de forma exhaustiva. Con el fin de que este hecho no afectase al desarrollo del informe, se ha realizado un importante esfuerzo durante el proceso de identificación de agentes, utilizando tanto el conocimiento disponible (expertos colaboradores, agentes entrevistados/encuestados e INCIBE), así como las referencias mostradas en las diversas fuentes documentales analizadas.

El ecosistema de I+D+i de la ciberseguridad es un **ecosistema complejo** compuesto por **múltiples agentes** con roles diferentes que interactúan entre sí: las Administraciones Públicas, el Sector Académico, los Organismos de Soporte a la I+D+i y la Industria.

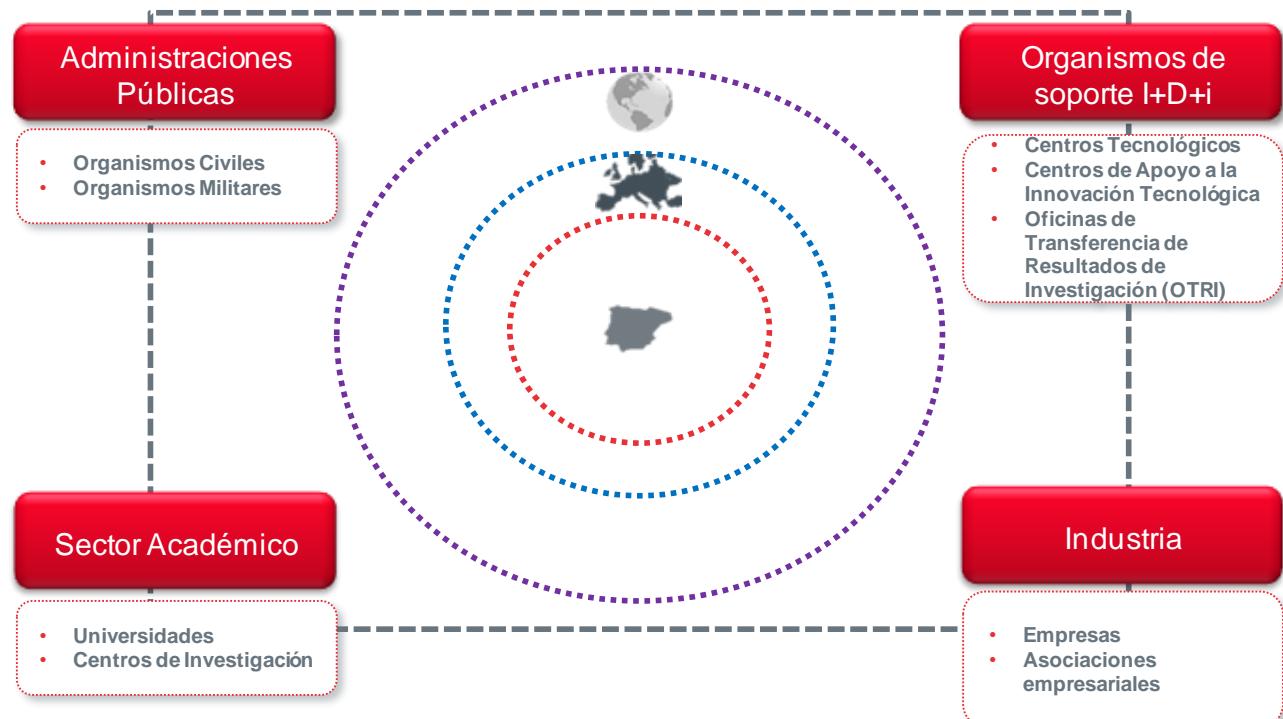


Figura 3: Tipología de agentes del ecosistema de I+D+i en ciberseguridad.

Las **Administraciones Públicas** están integradas por organismos tanto civiles como militares que juegan diversos roles:

- **Rol consultivo.** Se trata de organismos no gubernamentales, de carácter generalmente supranacional, tanto civiles como militares, que realizan procesos de reflexión y marcan las grandes líneas de la ciberseguridad en el ámbito institucional y político. Entre otros elementos, formulan recomendaciones y diseñan estándares globales con el objetivo de crear un marco común que reúna las visiones en el desarrollo de esta materia en las naciones.
- **Rol divulgador.** Orientado a la comunicación, divulgación y puesta en común de diversas temáticas en el ámbito de la ciberseguridad.
- **Rol estratégico.** En esta tipología se encuadran los gobiernos de las naciones, como instituciones cuya misión es el diseño de estrategias y políticas públicas sobre esta materia y hacerlas operativas. Se incluyen también las instituciones de la Unión Europea formuladoras de políticas.
- **Rol financiador.** Agentes gubernamentales encargados de provisionar económica y financieramente a la ciberseguridad. En el ámbito del presente estudio, se han considerado estrictamente los agentes que financian las actividades de I+D+i.
- **Rol legislador.** Agentes que delimitan el marco legal en el que se desenvuelven las actividades de ciberseguridad.

La Administración Pública juega también un **rol inductor de demanda**, en un doble sentido:

- Demandante de seguridad para la protección de la información gestionada por la propia administración.
- Demandante de soluciones de protección y seguridad en el ámbito de la defensa y de la inteligencia nacional.

Los agentes integrantes del **Sector Académico** son el núcleo básico del sistema de investigación científica y desarrollo tecnológico. Dentro de esta tipología se incluyen las **universidades** (con sus grupos de investigación asociados) y los **centros de investigación** (públicos y privados).

Los **Organismos de Soporte a la I+D+i** contribuyen a la dinamización del sistema, propiciando la interacción entre el entorno científico y tecnológico para la difusión y generalización de los procesos de I+D+i. En concreto, se han contemplado tres tipos:

- **Las Oficinas de Transferencia de Resultados de la Investigación (OTRIs)**, cuyo objetivo es contribuir a la comercialización de los resultados de la I+D generada en la universidad y los centros de investigación.
- **Los Centros Tecnológicos (CT)** que, atendiendo los requerimientos de la empresa, desarrollan proyectos de investigación y desarrollo tecnológico, contribuyendo a la transferencia de resultados de investigación, fomentando la investigación cooperativa entre las empresas y elevando su nivel tecnológico y competitividad.

- **Los Centros de Apoyo a la Innovación Tecnológica (CAIT)**, cuyo objetivo es facilitar la aplicación del conocimiento generado en los organismos de investigación y centros tecnológicos, mediante su intermediación entre éstos y las empresas.

La **Industria y las empresas** son analizadas desde una doble perspectiva:

- **Empresas** que desarrollan su negocio en el ámbito de la ciberseguridad.
- **Asociaciones empresariales** que, a través de la unión y colaboración de sus socios e integrantes, buscan la obtención de sinergias, economías de escala y la realización de actividades de I+D+i conjuntas.

A continuación se muestra el mapa del Ecosistema de I+D+i de España identificando el número de agentes que existen dentro de cada una de las tipologías de agentes:

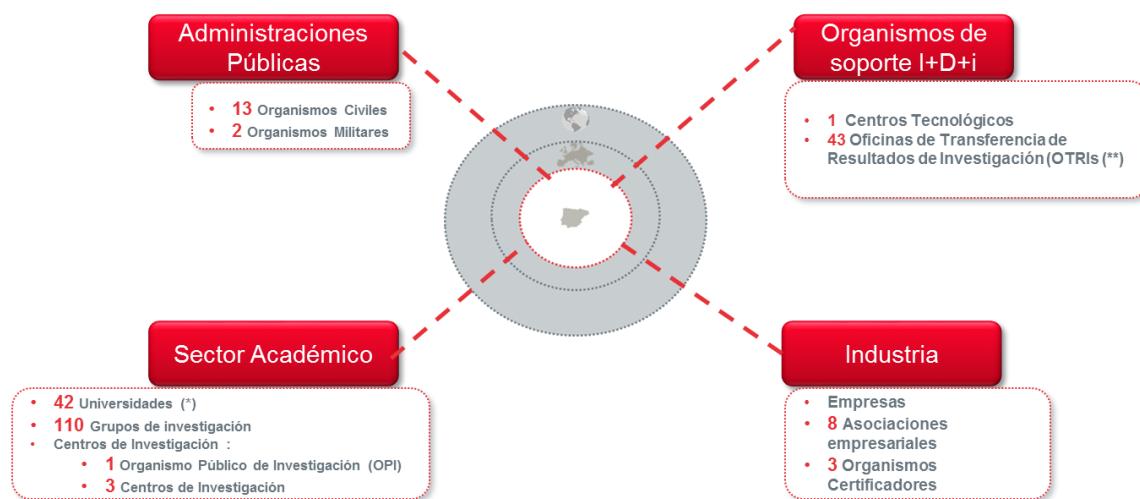


Figura 4: Mapa de agentes del ecosistema de I+D+i en ciberseguridad en España.

NOTA: El Anexo IV AGENTES DEL ECOSISTEMA DE I+D+I EN CIBERSEGURIDAD EN ESPAÑA de este documento ofrece un listado de los agentes identificados por cada tipología.

3.2 Análisis del contexto institucional, jurídico y económico

Dentro del modelo de análisis propuesto para analizar el ecosistema de I+D+i en ciberseguridad, el primero de los elementos a tener en cuenta es el **contexto** en el que se desenvuelve el mismo, que podría asimilarse como las “reglas del juego generales” que delimitan el perímetro de desarrollo de la ciberseguridad.

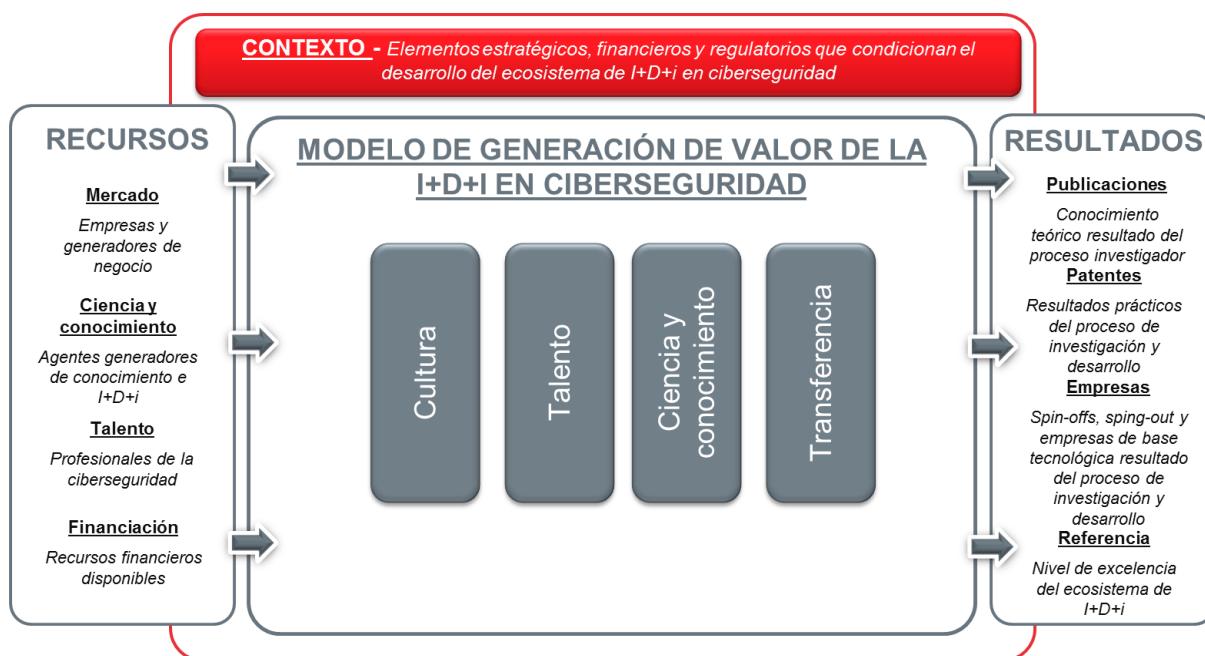


Figura 5: Modelo general de análisis: contexto.

En el **ámbito internacional**, cabe destacar que se han dado los primeros pasos en el reconocimiento de la ciberseguridad como un asunto clave en las agendas gubernamentales, estableciéndose orientaciones estratégicas de alto nivel para su abordaje. Estas orientaciones requieren una revisión constante y continua, ante la velocidad de cambio tanto de las tecnologías de la información como de las ciberamenazas.

La **Unión Europea** reconoce la importancia de la ciberseguridad en su principal eje estratégico, la estrategia Europa 2020, si bien reconoce explícitamente que los Estados miembros deben establecer sus propias estrategias nacionales en este campo.

En el caso de **España** cabe destacar que, a pesar de que se ha reconocido por parte del Estado Español la ciberseguridad como un asunto clave en la agenda gubernamental, la realidad es que las estrategias diseñadas son planteamientos de alto nivel que se traducen en declaraciones de intenciones que delimitan los retos y ofrecen soluciones generales, pero que han de ser concretadas y aterrizzadas.

De hecho, una de las características de las diferentes iniciativas⁶ que, relacionadas con la ciberseguridad, ha emprendido el Gobierno de España, es la **ausencia de focos temáticos o prioridades concretas**.

Esta falta de concreción puede jugar en contra en el desarrollo de la ciberseguridad, planteando un **escenario generalista** a partir del cual es complejo establecer para los agentes del ecosistema una estrategia de actuación.

⁶ Agenda Digital para España, Estrategia de Seguridad Nacional (ESN), Estrategia de Ciberseguridad Nacional (ECSN) y Estrategia de Seguridad Marítima (con una acción específica en ciberseguridad).

La ausencia de focos concretos resta valor a la capacidad del ecosistema de I+D+i para generar valor, puesto que, al no establecer un marco claramente delimitado, no permite focalizar y orientar la actividad del ecosistema, provocando, indirectamente, la dispersión de la actividad de I+D+i en España.

En el **ámbito jurídico**, el escenario es similar al contexto, dado que es un elemento que se desarrolla en paralelo al avance y concreción de las estrategias en ciberseguridad. Queda por tanto un amplio camino por recorrer, cuyo avance y velocidad vendrá marcado por el grado de desarrollo estratégico y político.

En concreto, son varios los elementos que podrían ser destacados como pendientes de desarrollo:

- La armonización del marco legal español y europeo, como elemento crítico para la detección y persecución coordinada de las ciberamenazas y ciberataques.
- Las obligaciones concretas en la protección de infraestructuras críticas.
- Los desarrollos normativos orientados a impulsar el mercado europeo digital.
- La regulación de los aspectos de seguridad en la Administración Electrónica y la interoperabilidad en el intercambio de información electrónica entre administraciones.

El escenario de desarrollo normativo marca una reducción en la capacidad de extraer valor, principalmente por las oportunidades que el desarrollo normativo supone para el sector (en términos de obligaciones y requisitos técnicos).

Finalmente, en lo relativo a la **financiación de la I+D+i**, la ciberseguridad es una de las prioridades temáticas del programa europeo de I+D+i (Horizonte 2020) que cuenta con dotaciones presupuestarias y áreas de desarrollo concretas.

A nivel **estatal**, puede concluirse que la ciberseguridad recibe niveles de inversión inferiores a los países líderes (Estados Unidos, Reino Unido, Israel). A falta de un plan específico para la I+D+i en ciberseguridad, es el Plan Estatal de Investigación Científica, Técnica e Innovación 2013-2016 la principal fuente de financiación para las actividades de I+D+i en este campo. Dicho plan reconoce esta área como clave, si bien tan sólo se dispone de información parcial acerca de la dotación presupuestaria para esta prioridad⁷.

⁷ A través de una petición realizada al Ministerio de Economía y Competitividad sobre el grado de ejecución de proyectos en ciberseguridad, se dispone de los siguientes datos: 1) Dirección General de Investigación Científica y Técnica (DGICT). 27 proyectos financiados durante el periodo 2009-2013, con un importe total de 3,3 millones de euros. 2) Dirección General de Innovación y Competitividad (DGIC): en la convocatoria de Retos de Colaboración de 2014 se han financiado 11 proyectos dentro del Reto 8, Seguridad, Protección y Defensa, con un importe total de 7,8 millones de euros. Adicionalmente, durante el periodo 2010-2012 se han financiado un total de 18 proyectos en el marco del subprograma INNPACTO, por un importe total de 20 millones de euros.

La situación actual de restricción presupuestaria y la no existencia de planes específicos de I+D+i para el sector (con sus correspondientes asignaciones presupuestarias), resta valor a la capacidad del ecosistema de I+D+i para generar valor.

Adicionalmente, el actual escenario de restricción de gasto público es un limitante añadido que frena la capacidad de tracción de la Administración como uno de los grandes demandantes de soluciones de ciberseguridad, tanto en el ámbito civil, militar y de inteligencia.

3.3 Caracterización del ecosistema de I+D+i en ciberseguridad

En este apartado se valoran los diferentes elementos que, además del contexto, conforman el ecosistema de I+D+i en ciberseguridad. En concreto, se analizan los *recursos*, el *modelo de generación de valor* y los *resultados* fruto de este modelo.

3.3.1 Recursos

Los recursos representan los **elementos de base disponibles en el ecosistema de I+D+i para la producción de valor**, representados por el *mercado*, la *ciencia* y el *conocimiento*, el *talento* y la *financiación*.

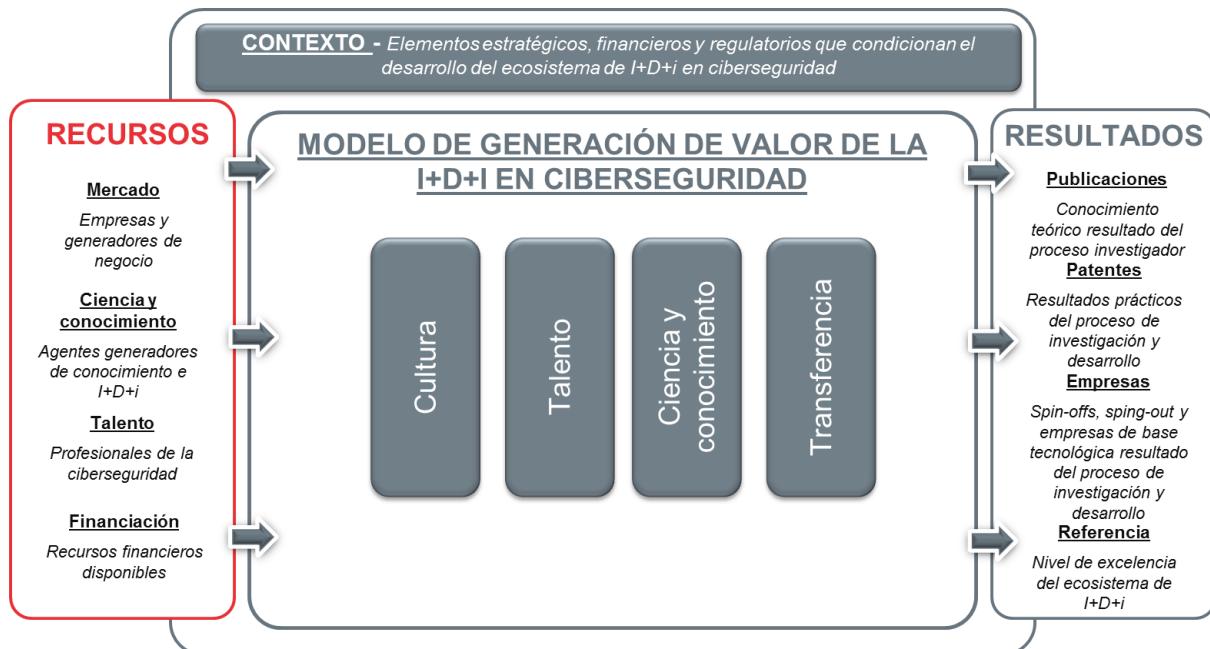


Figura 6: Recursos.

Mercado

En general, la industria española se caracteriza por una alta **fragmentación y diversidad** en la tipología de empresas, desde grandes empresas tractoras (nacionales e internacionales) hasta empresas de nicho.

En cuanto al volumen de empresas, se podría concluir que éste es reducido, en comparación con otros sectores económicos, si bien no se dispone de estadísticas públicas que permitan cuantificar el censo de empresas.

Elementos como la tradicional cultura de aversión al riesgo y las limitaciones del Sistema de Ciencia y Tecnología son claros elementos que lastran la capacidad de nuestro país para generar nuevas empresas de base tecnológica.

Es necesario realizar un esfuerzo en la industria española para superar el gap tecnológico y ganar posiciones en la arena global, ya que nuestra industria, en un nivel agregado, se encuentra a mucha distancia tanto de los grandes líderes industriales (Estados Unidos e Israel) como de la segunda línea de competidores (Reino Unido, Holanda, Francia y Alemania, entre otros).

La actual situación económica ha sido en los últimos años y es en la actualidad un claro elemento reductor de valor para la industria, al limitar la actividad de I+D+i, tanto en su capacidad de financiación propia como en la procedente de las diversas iniciativas públicas de apoyo a la I+D+i.

Esta situación es especialmente crítica en el caso de las pymes, lo que unido a la ya de por si baja cultura de I+D+i, hace que nuestro pequeño y mediano tejido industrial se encuentre lejos de unos niveles razonables de I+D+i.

Finalmente, la **escasa cultura de la ciberseguridad en España y la baja capacidad de tracción sobre la demanda de la Administración Pública** son otros elementos limitantes para la capacidad de la industria de generar y comercializar soluciones en ciberseguridad. Ambos elementos suponen un mercado doméstico reducido que limita las posibilidades de desarrollo de la industria. En el contexto internacional, es Latinoamérica el gran foco de oportunidad para nuestra industria.

Ciencia y conocimiento

Cabe destacar la **existencia de masa crítica investigadora** en España, identificándose 110 grupos de investigación en 42 universidades y 3 centros de investigación dedicados a la ciberseguridad.

La diversidad de áreas científico-tecnológicas (a pesar de que buena parte de los grupos de investigación se dedican a áreas relacionadas con la criptografía), la desconexión y falta de colaboración entre los agentes, hace que la **capacidad investigadora se disperse y no presente fortalezas concretas y delimitadas a nivel agregado**.

De hecho **España no figura dentro de los Best in Class** en investigación y transferencia en ninguna de las áreas científico-tecnológicas de la ciberseguridad.

Talento

El principal elemento que caracteriza el talento de la ciberseguridad en España es el **marcado proceso de fuga hacia otros países**, dadas las mejores oportunidades que ofrecen nuestros competidores.

En términos netos, España presenta un efecto reductor en su volumen de profesionales en ciberseguridad. La falta de liderazgo de España en ciberseguridad juega en contra de la retención y desarrollo del talento y se posiciona como principal elemento reductor de valor en el talento, dificultando en gran medida el proceso de captación y retención, tanto para profesionales de la industria como para personal investigador.

Adicionalmente, el **Sistema de Ciencia y Tecnología** presenta una serie de deficiencias y carencias que suponen un limitante al proceso de captación y retención de personal **investigador** y que contribuyen a acelerar el proceso de fuga de talento:

- “Precariedad” de la política de contratación y becas para el personal investigador, que no contribuye a mejorar la percepción de los profesionales de la investigación como una opción profesional.
- El ratio de reposición del personal investigador en el Sector Académico se encuentra muy por debajo de las bajas, lo que supone una reducción neta del volumen del talento investigador disponible.

El **escaso efecto tractor de la demanda doméstica** en ciberseguridad (consumidores, empresas y Administración) es un elemento que limita el desarrollo de la industria y, por tanto, de la demanda de talento.

Elementos a favor son la **disponibilidad de un buen nivel en el talento disponible**. Sin embargo, se considera por buena parte de los agentes participantes en la iniciativa que es necesario **mejorar los planes de formación y capacitación del talento en ciberseguridad**, generando un enfoque más específico en este campo e incorporando las necesidades del mercado de trabajo (industria) en dichos planes.

Finalmente, es importante destacar la **previsión de una alta demanda de profesionales** en los próximos años, ante las grandes oportunidades que plantea la ciberseguridad.

Financiación

En España, a falta de un plan específico para la I+D+i en el ámbito de la ciberseguridad, cabe destacar que, a pesar de que las políticas estatales (y algunas regionales) establecen la seguridad como una de las prioridades temáticas para la I+D+i, el **nivel de apoyo financiero tan sólo puede ser evaluado parcialmente**.

Prácticamente todos los agentes participantes en el estudio apuntan a una clarísima debilidad de la I+D+i en ciberseguridad en lo relativo a la financiación, que supone una merma de la capacidad competitiva del ecosistema.

El recorte de fondos para la ciencia ha supuesto no sólo la **reducción de financiación para realización de proyectos, sino también la limitación en el personal de investigación con que cuentan las instituciones.**

Ante esta situación, es el programa Horizonte 2020 de la Unión Europea **prácticamente la única vía** para la financiación de la I+D+i. El Plan Estatal de Investigación Científica, Técnica y de Innovación 2013-2016 se considera “financieramente escaso”.

Otra de las vías que utiliza el Sector Académico para obtener fondos es la colaboración con empresas (contratos de I+D); sin embargo, ante la tradicional problemática desconexión ciencia-empresa de nuestro país, esta vía de financiación es aún reducida.

3.3.2 Modelo de generación de valor de la I+D+i

Este modelo se alimenta de los recursos *cultura, talento, ciencia y conocimiento* y *transferencia* y les añade (o resta) valor dependiendo de la configuración de los elementos del modelo de producción de valor para producir un resultado.

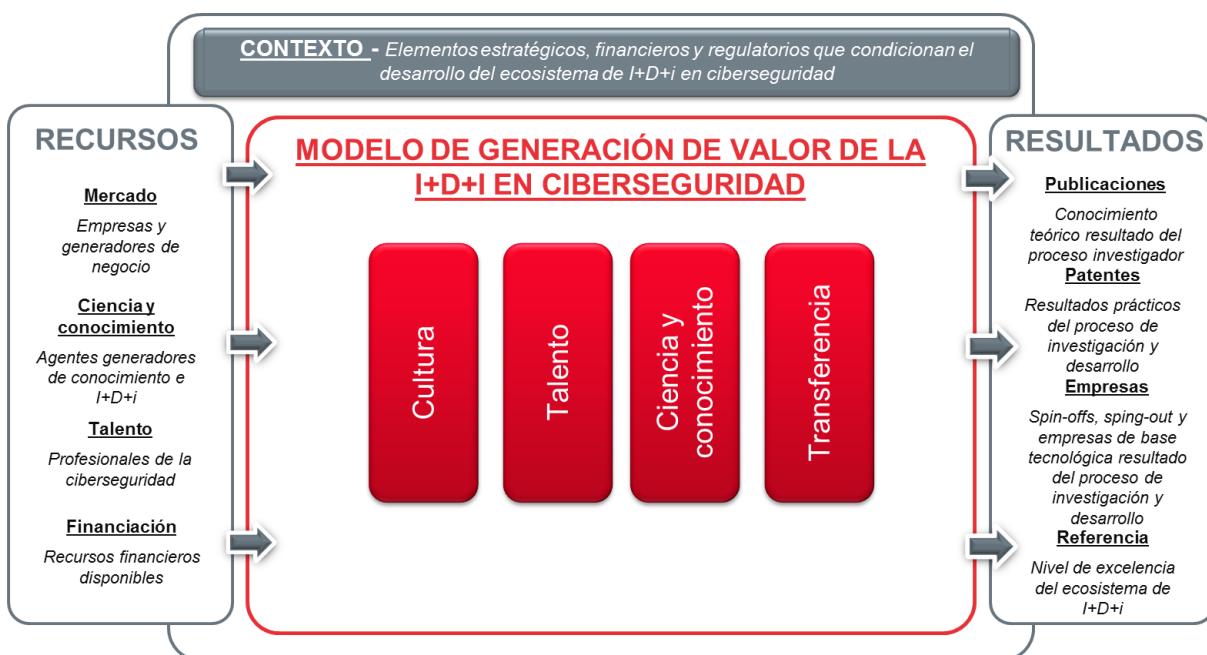


Figura 7: *Modelo de generación de valor de la I+D+i en ciberseguridad.*

Cultura

La cultura colaborativa, de emprendimiento y de ciberseguridad, presenta un efecto reductor de la capacidad del ecosistema de I+D+i para producir valor.

Las recientes estrategias y procesos normativos que establecen obligaciones en cuanto a la protección de la información y los sistemas, caminarán sin duda alguna hacia la creación de una mayor cultura de la ciberseguridad, generando una mayor demanda de soluciones.

- **Cultura de la colaboración.** La cultura colaborativa en nuestro país es baja, lo que supone un elemento reductor en la capacidad del ecosistema de producir valor a través de proyectos conjuntos de I+D+i.
- **Cultura del emprendimiento.** España presenta una cultura de aversión al riesgo, que implica tasas de emprendimiento relativamente bajas. Los agentes participantes en el estudio apuntan a la necesidad de trabajar y reforzar este elemento desde las etapas más tempranas del sistema educativo.
- **Cultura de la ciberseguridad.** Las empresas y el mercado en general no son conscientes de la necesidad de protegerse y prevenir los ataques. Esta situación configura un mercado doméstico reducido, que se traduce en bajos niveles de demanda de soluciones de ciberseguridad en los tres grandes grupos de demandantes de soluciones (consumidores, empresas y Administración Pública). La búsqueda de mercados internacionales, como Latinoamérica, se configura como posible alternativa a esta falta de demanda interna.

Talento

El modelo de generación de talento en ciberseguridad comienza en el sistema universitario, si bien se reclama por parte de algunos de los agentes participantes en el estudio la necesidad de **fomentar la cultura de la ciberseguridad y de las vocaciones profesionales desde las etapas más tempranas del sistema educativo**.

Como punto de partida ha de tenerse en cuenta que este talento **requiere de una formación y capacitación muy especializada**, posterior a la graduación universitaria, por lo que el proceso de preparación y maduración de profesionales en este campo requiere de tiempo. Además, al ser una disciplina transversal, no dispone de un enfoque específico de formación, lo que deriva en **un perfil profesional poco claro**.

Existe mucho volumen potencial de talento, puesto que cualquier informático o ingeniero de telecomunicaciones, con la formación adecuada, puede llegar a convertirse en un profesional de la ciberseguridad. Pero para desarrollar todo este potencial **se reclama un proceso formativo concreto y “dirigido”, alineado con la hoja de ruta nacional en esta materia**, de modo que se garantice disponer de profesionales formados y capacitados para las apuestas de futuro de nuestro país.

Esta alineación de la universidad con la ciberseguridad debiera formularse a través de un contacto más cercano con la industria, armonizando las necesidades del mercado con la formación académica, modelo seguido por algunos países líderes en este campo (Estados Unidos).

Igualmente, los futuros pasos que previsiblemente se den en la **certificación de profesionales en ciberseguridad será un elemento que contribuirá positivamente a diferenciar el talento**.

Ciencia y conocimiento

El ecosistema de I+D+i en ciberseguridad en España se caracteriza por su **amplitud, diversidad, fragmentación, dispersión y por no poseer unas dinámicas claras de relación entre sus agentes**.

En términos generales, se podría afirmar que el ecosistema de I+D+i en ciberseguridad no aprovecha todas las capacidades y sinergias que un ecosistema de este volumen presenta, lo que plantea un modelo reductor de la capacidad para producir valor

Sin embargo, su relativa juventud hace esperar una **evolución positiva en la explotación y puesta en valor de estas capacidades investigadoras**. Es por tanto necesario avanzar en **mayores niveles de colaboración en torno a objetivos comunes**, que permitan situar a nuestro ecosistema en un mejor posicionamiento tanto interno como internacional.

Adicionalmente a la falta de colaboración, existen otros **elementos que lastran su capacidad investigadora para extraer todo su potencial**: la inexistencia de un plan de I+D+i específico para la ciberseguridad y la escasa dotación presupuestaria para la ciencia.

Finalmente se deberá trabajar sobre una serie de elementos que permitan sentar unas bases sólidas para **aumentar la aportación de valor en la I+D+i** en ciberseguridad:

- **Conocimiento** de las capacidades y potenciales de la I+D+i en España como primer paso para potenciar la investigación en España.
- Aumentar la **colaboración entre agentes**.
- Mayor definición de las **políticas (focos)** y **dotaciones presupuestarias públicas**.
- **Relanzar instrumentos que habiliten y potencien el papel de la Administración Pública como tractor de la demanda** de la ciberseguridad. La compra pública innovadora y la demanda temprana de soluciones innovadoras aparecen como elementos útiles para potenciar el desarrollo de soluciones punteras.

Transferencia

El modelo de transferencia de resultados de la investigación en ciberseguridad presenta un claro efecto reductor en su capacidad para transferir las investigaciones hacia el mercado.

Las debilidades de nuestro país en el proceso de transferencia de los resultados de la investigación hacia el mercado y la ya tradicional desconexión ciencia-mercado son temas recurrentes en el debate sobre el Sistema de Ciencia y Tecnología español.

Los niveles de transferencia al mercado, que no pueden ser evaluados objetivamente por falta de datos públicos, son relativamente escasos en opinión de los agentes y expertos participantes en el estudio, que apuntan a algunos elementos como causantes de esta situación:

- Desde el Sector Académico se apunta hacia los **escasos incentivos a los investigadores para hacer transferencia**. Sin embargo, **son los agentes de**

especializados en transferencia los que deben jugar el rol clave en el proceso de transferencia y comercialización de los resultados de la investigación hacia la industria.

- Otro de los elementos apuntados es la **facilidad que la cercanía entre empresas y centros de investigación** provee al proceso de transferencia, lo que, en el caso de las zonas geográficas alejadas de los grandes focos empresariales es complejo, ya que el tejido empresarial no suele tener cultura de I+D+i y está más centrado en sobrevivir a la crisis que en promoverlo.
- En el ámbito de la ciberseguridad se añade el hecho de que las **empresas y el mercado en general no son conscientes de la necesidad de protegerse y prevenir los ataques**.
- **La transferencia a nivel internacional es compleja**, ya que la soberanía de los países en ciberseguridad condiciona el proceso de transferencia, no sólo en aspectos militares y de inteligencia, sino también en las soluciones de ámbito civil.

La solución a la falta de transferencia pasa por tener en cuenta varios elementos:

- Realización de **proyectos conjuntos**, que presenten intereses comunes tanto para la ciencia como para la industria.
- **Dar a conocer la capacidad y potencial investigador** del Sector Académico a la industria.
- **Revisión del modelo de los agentes de transferencia**, estableciendo los incentivos que permitan una transferencia real.

3.3.3 Resultados

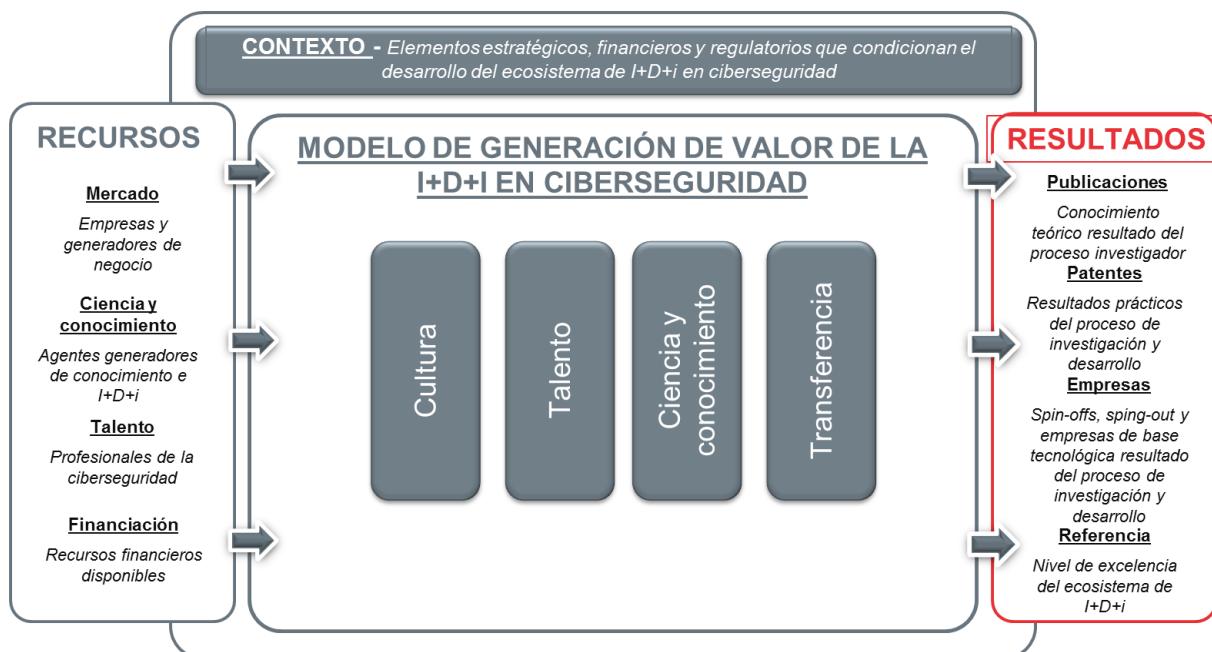


Figura 8: Resultados.

Los resultados reflejan cómo el ecosistema de I+D+i agrega o resta valor a los recursos disponibles. De acuerdo al modelo de análisis planteado, son cuatro las grandes tipologías de resultados a generar: *publicaciones, patentes, empresas de base tecnológica y referencia*, entendido éste último término como la capacidad del ecosistema para posicionarse como excelente y referente dentro del panorama científico-tecnológico de la ciberseguridad.

En general, la diversidad de áreas científico-tecnológicas (a pesar de que buena parte de los grupos de investigación se dedican a áreas relacionadas con la criptografía) y la desconexión y falta de colaboración entre los agentes del ecosistema de I+D+i, hace que **los resultados de la investigación se dispersen y no presenten fortalezas concretas y delimitadas**.

Como consecuencia, **el ecosistema español de I+D+i en ciberseguridad no presenta referencia a nivel internacional en ninguna de las áreas científico-tecnológicas** en las que puede ser desglosada la ciberseguridad (lo que no implica que no exista referencia a nivel individual de investigadores, universidades o grupos de investigación).

Los agentes participantes en el estudio perciben que los **resultados de la I+D+i en ciberseguridad son escasos**. Quizás la producción de publicaciones y patentes sean los elementos que más volumen presentan, si bien la falta de aplicabilidad y transferencia al mercado hace que en la práctica estos resultados no se transformen en valor económico ni lleguen al mercado. Esta baja aplicabilidad puede deberse a varios factores:

- **Falta de estrategias concretas de investigación**, con enfoques prácticos de aplicación.
- En el sistema investigador **no existen incentivos claros para la transferencia** al mercado y no existe un modelo de emprendimiento definido.

3.4 Modelo de relación del ecosistema de I+D+i en ciberseguridad

En este apartado se presenta el análisis del modelo de relación, entendiendo como tal las **dinámicas, modelos y relaciones colaborativas** entre los diferentes agentes del ecosistema de I+D+i en ciberseguridad.

Para ello, en primer lugar, se ha ilustrado la visión de los agentes participantes en la iniciativa sobre las dinámicas de relación en el ecosistema. Estas visiones serán complementadas con un **análisis de las principales redes colaborativas** identificadas en nuestro país. Finalmente se incluye, por su valor como fuente de buenas prácticas y experiencias inspiradoras, un análisis de las principales redes de ámbito internacional.

El **Anexo V REDES COLABORATIVAS ANALIZADAS** incluye el listado de las redes colaborativas nacionales e internacionales analizadas.

3.4.1 Principales redes o modelos colaborativos nacionales

En España, con carácter general, **la cultura colaborativa es relativamente escasa**, lo que supone un elemento limitante de partida en el desarrollo de la colaboración en I+D+i en ciberseguridad.

Como ya se ha apuntado anteriormente, el ecosistema de I+D+i en ciberseguridad se caracteriza por su **amplitud, diversidad y desconexión**, lo que hace complejo identificar de forma sistemática las dinámicas de colaboración y relación entre sus agentes. Las evidencias disponibles apuntan a un modelo de relación en el que las colaboraciones son puntuales entre los agentes, no existiendo indicios de **colaboraciones a nivel global e integral en el ecosistema**.

Los agentes participantes en la iniciativa consideran que en España, en comparación con otros países, la colaboración en I+D+i es reducida, debido principalmente a aspectos culturales, a los que se une un contexto de financiación que no ayuda a la creación de lazos de colaboración a través de la ejecución de proyectos de conjuntos entre los agentes del ecosistema.

Existe un cierto tono pesimista en cuanto a los modelos de colaboración existentes, al considerarse que no cumplen premisas de vital importancia tales como la existencia de un compromiso real por la I+D+i materializado en presupuestos económicos o la importancia de establecer **objetivos claros de negocio, que se traduzcan en colaboraciones** para el desarrollo de soluciones comercializables en el mercado.

Finalmente los participantes apuntan a la existencia de colaboraciones en los programas de financiación de la I+D+i europeos (Horizonte 2020 y anteriormente el Séptimo Programa Marco). Sin embargo, España no presenta retornos en estos programas de acuerdo con sus capacidades, por lo que debe seguir trabajando en **el desarrollo de una estrategia proactiva para el posicionamiento de España dentro de Horizonte 2020** y de los organismos de la Unión Europea implicados en el diseño de las prioridades de dicho programa.

Del análisis de las redes colaborativas en España se deriva la existencia de tres grandes tipos de colaboración:

- **Colaboraciones entre la ciencia** (universidades y grupos de investigación) **y la industria** cada vez más frecuentes, pero en un nivel inferior a otros sectores (quizás por ser la ciberseguridad un sector emergente) y con carácter más puntual que general⁸. Muchas de estas colaboraciones se organizan en torno a los programas de financiación (fundamentalmente Horizonte 2020), para el desarrollo de proyectos conjuntos.
- **Colaboración entre universidades**, siendo destacable la Alianza A-4U (asociación estratégica entre la Universidad Autónoma de Barcelona, la Universidad Autónoma

⁸ Se han identificado ejemplos concretos de alianzas como la Cátedra Ciberseguridad de INDRA y la Universidad Carlos III de Madrid o el convenio firmado por S21sec y el Instituto de las Ciencias Forenses y de la Seguridad perteneciente a la Universidad Autónoma de Madrid.

de Madrid, la Universidad Carlos III de Madrid y la Universitat Pompeu Fabra de Barcelona).

- En cuanto a las **redes colaborativas**, su principal objetivo es ser un punto de encuentro entre los agentes del ecosistema para lograr una visión global e integradora. La mayor parte de las redes contemplan la participación público-privada. No obstante, también se encuentran redes de colaboración con miembros pertenecientes exclusivamente al ámbito privado.

A modo de **caracterización general de los modelos de relación** en nuestro país se podría concluir lo siguiente:

- Dado el carácter emergente del sector de la ciberseguridad en nuestro país, las redes identificadas **son relativamente jóvenes** (en torno a diez años las más antiguas).
- La mayoría **se centra en actividades relacionadas con la difusión, la formación o la puesta en marcha de grupos de trabajo** sin que se hayan detectado redes con foco exclusivo en I+D+i.
- Las redes identificadas poseen un **carácter generalista** (tecnologías de la seguridad en general), sin un foco específico en la ciberseguridad.
- Las redes más avanzadas son las vinculadas al sector industrial, que se posiciona claramente como el sector más involucrado en cooperación.
- Tienen un **marcado carácter institucional si bien integran a todas las tipologías de agentes del ecosistema** (Administraciones Públicas, Sector Académico, Industria y Organismos de Soporte a la I+D+i).
- Se trata de **entidades sin ánimo de lucro** (sin que, con la información disponible, se haya podido identificar cuál es su forma jurídica) y están **abiertas a todos los agentes interesados**, sin que se haya detectado la existencia de criterios de admisión de miembros.
- En general se trata de redes que **se financian a través de cuotas de membresía y de patrocinios**, contando, en algunos casos, con ayudas gubernamentales.

Finalmente, es necesario destacar el relevante papel que tienen aquellos **eventos** que, con carácter puntual, aglutinan a los principales agentes del ecosistema y que suponen ocasiones excelentes de desarrollar conexiones interpersonales (networking) y poner en valor los activos y avances existentes en ciberseguridad.

En este sentido, merece especial mención, por ser un referente en el sector, el **Encuentro Internacional de Seguridad de la Información (ENISE)** organizado por INCIBE, que ya cuenta con su octava edición.

El Encuentro Internacional de Seguridad de la Información (ENISE) tiene un carácter eminentemente práctico y profesional, contando con la presencia de expertos y organizaciones que se sitúan a la vanguardia de la innovación en ciberseguridad; su principal objetivo es analizar colectivamente los avances más significativos relativos a las diferentes iniciativas públicas y privadas que se están produciendo en la actualidad siendo objeto de debate los avances de los agentes públicos, la eficacia de las fórmulas de cooperación público-privada disponibles, las amenazas y riesgos emergentes en la ciberseguridad global así como las tecnologías más innovadoras existentes.

Adicionalmente, en la actualidad, INCIBE organiza un evento con carácter anual, **Cybercamp**, que tiene como objetivo la captación de talento en el ámbito de la ciberseguridad a través de la realización de diversas pruebas técnicas y retos online; se trata, por tanto, de reunir a los mejores talentos en esta materia, contando con la participación de los alumnos más destacados de los programas formativos de ciberseguridad en España y los mejores talentos internacionales.

3.4.2 Principales redes o modelos colaborativos internacionales

En el ámbito internacional, las redes y modelos de colaboración se encuentran en un estadio más avanzado que en España, en buena parte debido a la **existencia de una cultura más cooperativa que en el caso español**.

El análisis de las redes se presenta organizado en torno a las iniciativas europeas, pasando a continuación a ilustrar las principales características de las redes a nivel internacional, centradas en los casos de éxito de Estados Unidos e Israel.

3.4.2.1 Redes o modelos colaborativos europeos

En Europa se han llevado a cabo numerosas iniciativas que buscan la generación de ideas y la puesta en común de los diferentes agentes con un rol activo en la ciberseguridad. Dentro de estas redes existen dos grandes tipologías:

- **Redes vinculadas a la industria:** Lideradas por la industria⁹ pero que aglutinan a miembros del sector académico, organismos de soporte a la I+D+i y asociaciones de consumidores. Básicamente, estas redes trabajan para la consecución de los siguientes objetivos:
 - Aumentar la competitividad, incubando ideas innovadoras para crear oportunidades de negocio.
 - Desarrollar una agenda estratégica para la I+D+i en Europa que presentan a la Unión Europea para favorecer el alineamiento entre sus objetivos y las principales líneas estratégicas fijadas en materia de I+D+i.
 - Fomentar de la interoperabilidad de las soluciones tecnológicas.
- **Redes vinculadas a la Unión Europea**, en la que ésta juega el rol de elemento cohesionador y propiciador de colaboraciones en el ámbito público–privado. Estas

⁹ Redes formadas por compañías TIC europeas, tales como Gemalto, Microsoft, Nokia, Philips y compañías vinculadas al sector energético como Alliander, E.ON, KPN y DNV KEMA.

redes se caracterizan por tener un marcado carácter político e institucional, integrando a todos los agentes activos en la ciberseguridad. Como principales objetivos de estas redes se encuentra el intercambio de información y la generación de buenas prácticas.

3.4.2.2 Otras redes o modelos colaborativos internacionales

La larga trayectoria de los países líderes en ciberseguridad (Estados Unidos, Israel), unida a la implicación y la concienciación de sus autoridades en el desarrollo de este tipo de redes ha contribuido a la existencia de **redes muy sólidas en estos países**.

Destaca el papel de **Estados Unidos** como referente mundial, al abordar la colaboración desde una perspectiva integral. Existen dos grandes tipos de redes, las lideradas por organismos gubernamentales y las redes sectoriales (lideradas por la industria y participadas por la administración); ambas cuentan entre sus miembros con las principales empresas referentes en el sector y están abiertas a cualquier tipo de agente que trabaje directa o indirectamente en el ámbito de la actividad de la red.

Los servicios ofrecidos suelen orientarse a la difusión de información, el asesoramiento y la formación.

Estas redes están orientadas a la potenciación de la I+D+i, poniendo especial foco en elementos estratégicos en el caso de las redes gubernamentales y estableciendo las demandas de ciberseguridad en el caso de las redes sectoriales.

En el caso de las **redes sectoriales**, éstas suelen orientarse al sector **industrial y energético**; recogiendo los principales intereses de la industria para canalizarlos a través de la I+D.

Por último, es necesario destacar la realización de numerosos eventos realizados en materia de ciberseguridad con carácter internacional, que de nuevo se orientan a conectar a los agentes del ecosistema internacional y propician el desarrollo de colaboraciones.

3.5 Factores limitantes a la competitividad de la I+D+i en ciberseguridad

Este apartado realiza una recopilación de las carencias y obstáculos detectados en relación a la I+D+i en ciberseguridad, constituyendo, junto al resto de conclusiones, la base a partir de la cual se elaborará el DAFO del ecosistema (presentado en el siguiente apartado). Para una mejor comprensión, estos elementos se han organizado en torno a dos grandes grupos:

- **Carencias y obstáculos generales y estructurales.** Se trata de elementos no específicos de la ciberseguridad sino de carácter general, que afectan principalmente a las bases de una economía y sociedad. En lo relativo a la presente iniciativa, se recogen fundamentalmente déficits del Sistemas Español de Ciencia y Tecnología y de la cultura de nuestro país (colaborativa y emprendedora principalmente).
- **Carencias y obstáculos específicos de la ciberseguridad**, que si bien pueden reproducirse en otras áreas, tienen un carácter más específico.

3.5.1 Carencias y obstáculos generales y estructurales

- **Escenario complejo para la realización de I+D+i en España**, a raíz de los fuertes recortes de fondos económicos en el Sistema de Ciencia y Tecnología que afecta no sólo a la ejecución de proyectos de I+D+i, sino también a la contratación de personal investigador.
- El Sistema de Ciencia y Tecnología presenta posibilidades de **mejora para la incentivación de la investigación**.
- La precariedad presupuestaria del Sistema de Ciencia y Tecnología no contribuye a generar una **imagen de la investigación como una opción profesional**.
- **Desconexión ciencia-empresa**.
- Sistema de **transferencia de resultados de la investigación con un funcionamiento realmente inadecuado** que requiere la revisión de los agentes dedicados a esta labor.
- **Complejidad en la transferencia a nivel internacional**, especialmente en las soluciones de ciberseguridad relacionadas con la defensa y la inteligencia de los gobiernos.
- **Cultura de aversión al riesgo**, que laстра el emprendimiento.

3.5.2 Carencias y obstáculos específicos de la ciberseguridad

- **Contexto General. Escasez de datos y estadísticas de carácter público** que permitan la realización de un análisis y diagnóstico exhaustivo y estructurado de la ciberseguridad en España.
- **Contexto Cultural. Baja cultura de la ciberseguridad**, tanto en la propia Administración como en empresas y ciudadanía, que limita la demanda y desarrollo de soluciones por parte de la industria.
- **Contexto estratégico**
 - Las estrategias españolas sobre la ciberseguridad la establecen como una prioridad de Estado. Sin embargo, es necesario **aterrizar estos planteamientos** en actuaciones, prioridades y focos concretos.
 - **Inexistencia de un programa específico para la I+D+i en ciberseguridad**.
- **Contexto normativo**. Desarrollos normativos **aún incipientes** en algunos elementos que deben ser impulsados como elemento catalizador de la demanda y del desarrollo de soluciones en esta materia.
- **Contexto económico**
 - **Recortes de fondos económicos** en el Sistema de Ciencia y Tecnología que afectan a la ciberseguridad.
 - **Niveles de inversión en I+D+i inferiores a otros países europeos** y a los líderes de la ciberseguridad, lo que sitúa a nuestro país en un situación de clara desventaja, al tiempo que laстра la competitividad del sector a medio y largo plazo.

- **Mercado. Reducido tamaño del mercado de la ciberseguridad** en España debido a la baja demanda de soluciones, tanto por parte de las empresas como por parte de la Administración, siendo ésta última un importante agente tractor de soluciones en esta materia.
- **Caracterización del ecosistema**
 - **España no tiene un claro posicionamiento en la ciberseguridad a nivel internacional**, encontrándose por detrás de los países líderes y de buena parte de los países europeos de referencia (reino unido, Francia, Alemania y Holanda).
 - **Ecosistema amplio, diverso, fragmentado, desconectado**, sin unas dinámicas claras de relación entre sus agentes, sin foco concreto y con bajos niveles de colaboración. Amplio margen de aprovechamiento y puesta en valor de las capacidades, a través de la colaboración y generación de sinergias entre agentes.
 - **Escasa colaboración** entre el Sector Académico y la industria.
 - **Complejidad en la transferencia a nivel internacional**, especialmente en las soluciones de ciberseguridad relacionadas con la defensa y la inteligencia.
 - **Escasos resultados y valorización de los resultados** de la I+D+i en ciberseguridad en España.
 - **Proceso de fuga de talento** hacia otros países, que presentan mejores oportunidades y retribución.
 - **Procesos formativos y de capacitación que deberían ser revisados** para adaptarse a las necesidades del mercado.

3.5.3 Conclusiones

Realizando una valoración de los factores limitantes en función de su impacto, se observa que una gran cantidad de estos tienen un impacto alto en la competitividad de la I+D+i en ciberseguridad, en concreto, aquellos relativos a:

- **Contexto socioeconómico**, tales como los recortes de fondos económicos, la inexistencia de estrategias operativas o planes específicos de I+D+i y aspectos culturales relacionados con la ciberseguridad.
- **Escasos resultados** y valorización de la I+D+i.
- **Posicionamiento internacional** y el reducido **tamaño del mercado** doméstico.
- **Limitaciones de talento**, debido a la fuga del mismo o el desalineamiento de los perfiles existentes con la demanda de los mismos por parte de la industria.

Carácter	Factor Limitante	Impacto
General/Específico	Recortes de fondos económicos que limitan la ejecución de proyectos I+D+i.	
General/Específico	Recortes de fondos económicos que limitan la contratación y atracción de talento investigador.	
Específico	Niveles de inversión en I+D+i inferiores que en otros países europeos o líderes de la ciberseguridad.	

Específico	Baja cultura de la ciberseguridad.	
Específico	Estrategia de ciberseguridad sin concretar y hacer operativas.	
Específico	Inexistencia de un plan específico de I+D+i en ciberseguridad.	
Específico	Escasos resultados de la I+D+i en ciberseguridad.	
Específico	Escasa valorización de los resultados de la I+D+i.	
Específico	Débil posicionamiento de España en la ciberseguridad a nivel internacional.	
Específico	Reducido tamaño del mercado de la ciberseguridad en España (baja demanda de soluciones de ciberseguridad).	
Específico	Fuga de talento hacia otras localizaciones.	
Específico	Procesos formativos y de capacitación no adaptados a las necesidades del mercado.	
Estructural	Desconexión ciencia – empresa.	
Estructural	Baja cultura cooperativa.	
Estructural	Sistema ineficiente de transferencia de resultados de la investigación.	
Estructural	Cultura de aversión al riesgo.	
Específico	Inexistencia de datos y estadísticas de carácter público.	
Específico	Desarrollos normativos incipientes	
Específico	Complejidad de transferencia a nivel internacional.	

Tabla 1- Valoración del impacto de los factores limitantes identificados en términos de competitividad

De manera secundaria, y con un impacto menor en la competitividad, destaca el **carácter emergente de la ciberseguridad** (lo que se traduce en la falta de desarrollo normativo), la dificultad de acceso a datos para caracterizar la ciberseguridad y la dificultad de realizar transferencia internacional.

Finalmente, existen factores **limitantes estructurales del Sistema de Ciencia y Tecnología** que dificultan el desarrollo de la I+D+i en general, tales como la tradicional desconexión ciencia-empresa (agudizada por un funcionamiento ineficiente de transferencia de resultados de la investigación) o la existencia de una baja cultura cooperativa que impide poner en valor el potencial y las sinergias existentes en el ecosistema.

3.6 Análisis DAFO del ecosistema de I+D+i en ciberseguridad

En este apartado se presenta el análisis interno y externo del ecosistema de I+D+i en ciberseguridad materializado a través de la técnica DAFO (por sus siglas, Debilidades, Amenazas, Fortalezas y Oportunidades).

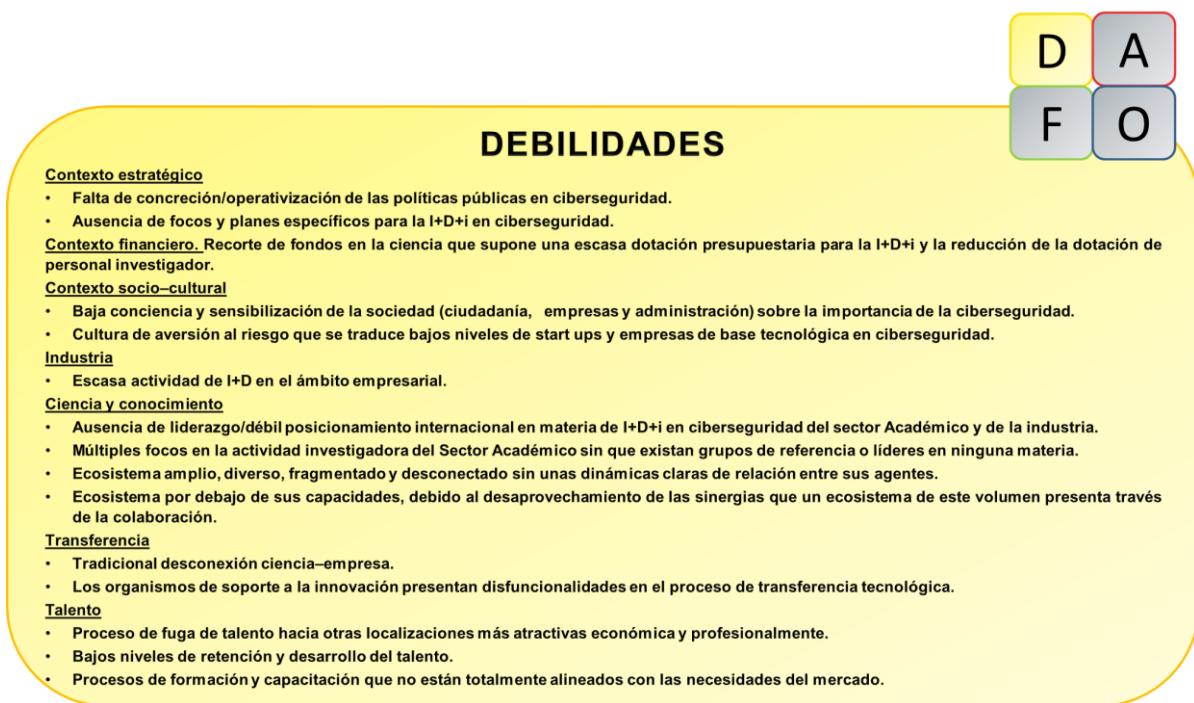
- **Fortaleza** es la capacidad competitiva de España que proporciona al ecosistema de I+D+i en ciberseguridad una ventaja.
- **Debilidad** son las cualidades de las que adolece el ecosistema de I+D+i en ciberseguridad, que es incapaz de dominar y que pone al ecosistema en una situación de desventaja competitiva.

- **Oportunidad** es una característica favorable que resulta del uso efectivo de las fortalezas para mejorar el posicionamiento del ecosistema.
- **Amenaza** se define como un competidor externo, evento o fuerza que trabaja en contra del posicionamiento del ecosistema.

Antes de presentar el análisis DAFO, es necesario poner de relieve una serie de **premisas y condicionantes de partida** específicos de la ciberseguridad y que por tanto forman parte intrínseca de las dinámicas a las que está sometido el ecosistema de I+D+i:

- Sector cambiante, tanto por el avance constante de las ciberamenazas como por la propia evolución de la tecnología.
- Industria con alta fragmentación (grandes empresas vs. empresas de nicho) que muestra una alta tendencia a la concentración.
- Fuerte necesidad de talento especializado cuyo proceso de formación es largo en el tiempo, necesitando de cierta madurez en el ejercicio de la profesión.
- No son necesarias grandes inversiones en infraestructuras para el desarrollo de actividades de I+D+i en ciberseguridad.

Se muestra a continuación el análisis DAFO:





AMENAZAS

Competencia.

- Países líderes con fuertes inversiones a largo plazo en I+D+i y con políticas y focos de investigación claros, que sitúan comparativamente a España en la cola de la apuesta a largo plazo por la ciberseguridad.

Mercado doméstico limitado por la ausencia de tracción de la Administración en la demanda temprana de soluciones punteras y la escasa demanda de soluciones por parte de los ciudadanos y empresas.

Ciencia y conocimiento

- Limitaciones del Sistema de Ciencia y Tecnología en el desarrollo e impulso del personal investigador.
- Enfoques de investigación con cierto continuismo y limitaciones de adaptación a los cambios, que limita el aprovechamiento de los nichos de oportunidad en ciberseguridad.
- Escaso impulso en los incentivos al personal investigador para la transferencia de la investigación al mercado.

Talento.

- Mayor atractivo de los países líderes, que aceleran el proceso de fuga de talento en España



FORTALEZAS

Ciencia y conocimiento.

- Sector Académico con masa crítica y capacidades investigadoras amplias y demostradas. Amplio margen de recorrido para la explotación y puesta en valor de las capacidades investigadoras en el ámbito de la ciberseguridad.

Talento.

- Cíerto nivel en el talento profesional e investigador, que presenta oportunidades para su retención, explotación y puesta en valor.

Agentes del ecosistema de I+D+i.

- Excelente predisposición de agentes del ecosistema para impulsar la ciberseguridad.



OPORTUNIDADES

Contexto estratégico.

Ciberseguridad como asunto clave en las agendas gubernamentales.

Contexto normativo incipiente, con amplias oportunidades de catalizar la demanda de soluciones de ciberseguridad (delimitación de obligaciones y requisitos técnicos que deberán ser de obligado cumplimiento).

Contexto financiero.

Aprovechamiento del entorno europeo con trampolín para incrementar la excelencia.

Mercado.

- Ciberseguridad como sector emergente, dinámico y en crecimiento, con grandes potenciales de crecimiento en los próximos años.
- Grandes oportunidades en la comercialización de soluciones en Latinoamérica.
- Identificación de sectores que puedan actuar como grandes tractores de la I+D+i (early adopters), con grandes necesidades de soluciones de ciberseguridad y con capacidad de exportar estas soluciones al ámbito internacional.

3.7 Plan de actuaciones para el incremento de la competitividad del ecosistema de I+D+i en ciberseguridad

En este apartado se presentan las actuaciones identificadas para promover la investigación, el desarrollo tecnológico y la innovación en ciberseguridad. La base para la identificación de estas actuaciones lo constituyen dos grandes elementos ya ilustrados en este documento:

- De un lado, los **[Factores limitantes** a la competitividad de la I+D+i en ciberseguridad], que deberán ser afrontados a través de actuaciones que permitan su mitigación.
- De otro, el **[Análisis DAFO del ecosistema de I+D+i en ciberseguridad]**. A partir de él se han identificado una serie de actuaciones orientadas a:

- **Corregir** las debilidades. **Estrategias de reconversión.**
- **Afrontar** las amenazas. **Estrategias defensivas.**
- **Mantener** las fortalezas. **Estrategias de mantenimiento de ventajas competitivas.**
- **Explorar** las oportunidades. **Estrategias de fortalecimiento.**

		ANÁLISIS INTERNO	ANÁLISIS EXTERNO
A eliminar	DEBILIDADES	Estrategias de Reconversión	AMENAZAS
	Afrontar	C orregir	Estrategias Defensivas
A potenciar	FORTALEZAS	Estrategias de Mantenimiento	OPORTUNIDADES
	A potenciar	M antener	Estrategias de Fortalecimiento
			E xplotar

Figura 9: Matriz de definición de actuaciones “CAME”.

A continuación se muestra cada una de las actuaciones definidas, encuadradas dentro la tipología de estrategia correspondiente y con una valoración del grado de impacto y dificultad de implantación (alto, medio, bajo). Finalmente, se indica qué actuaciones están (total o parcialmente) al alcance de la red:

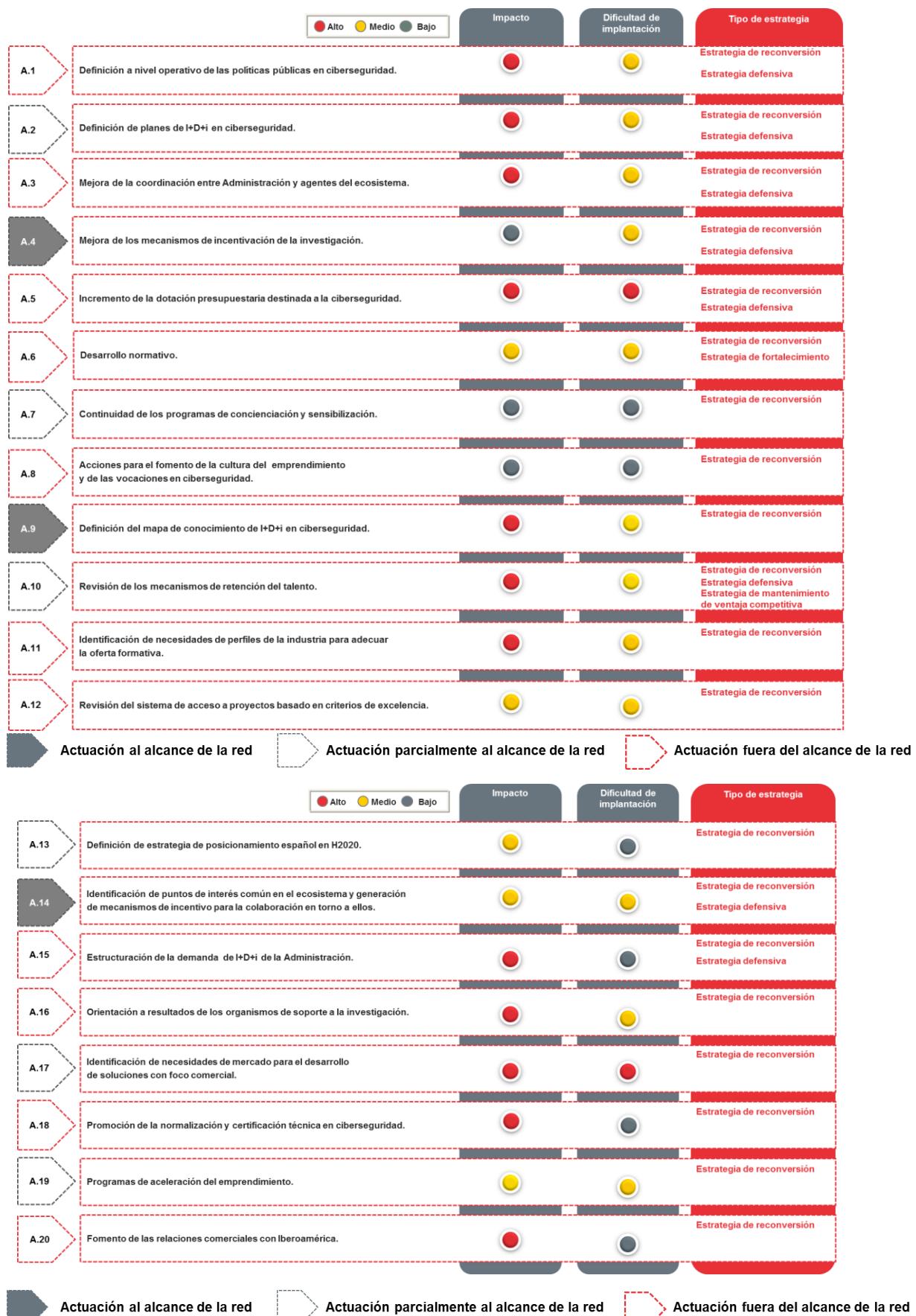


Figura 10: Caracterización de las actuaciones.

De la caracterización de las actuaciones se desprende que **la mayoría están enmarcadas dentro de las llamadas estrategias de reconversión**, es decir, se orientan a corregir las debilidades, algunas de las cuales son estructurales del Sistema de Ciencia y Tecnología.

A su vez, estas actuaciones pueden tener un rol activo en las **estrategias defensivas** (actuaciones para afrontar las amenazas existentes) ya que en muchos casos las amenazas identificadas son fruto de las debilidades existentes en el ecosistema de I+D+i en ciberseguridad.

Los resultados de esta caracterización se muestran en una **matriz de posicionamiento** que permitirá, de una forma amigable y gráfica, identificar el posicionamiento de cada una de las actuaciones.

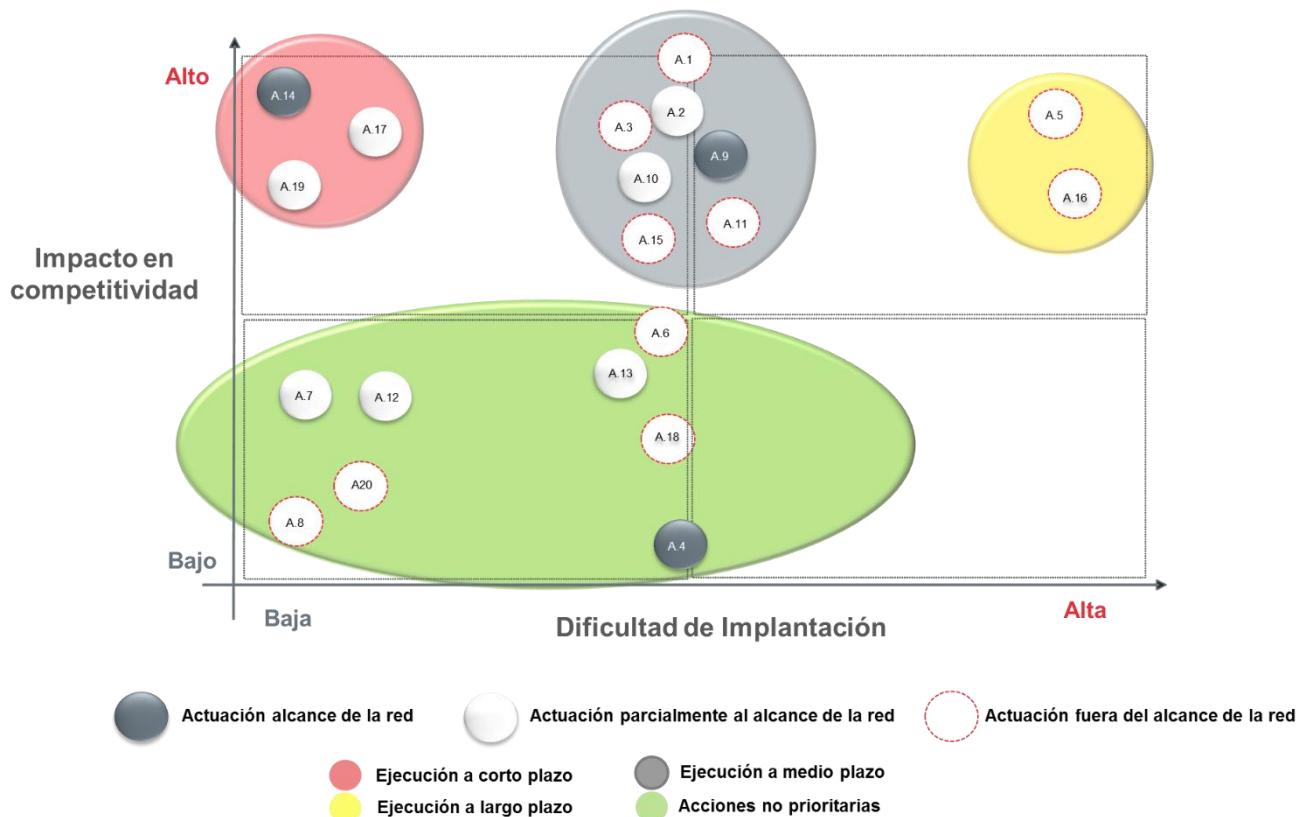


Figura 11: Matriz de priorización de las actuaciones del Plan de Actuación.

Tal y como se observa en la matriz, atendiendo al impacto y a la dificultad de implantación, las actuaciones pueden organizarse en torno a cuatro grandes grupos:

- **Actuaciones de inmediata aplicación:** Se llevarán a cabo en el corto plazo, ya que su impacto en la competitividad del ecosistema es alto y su dificultad de implantación es baja. En concreto, son actuaciones relativas a la identificación de puntos de interés común en el ecosistema, de necesidades de mercado para generar colaboración, así como relativas a la definición de programas para la aceleración del emprendimiento.
- **Actuaciones de aplicación a medio plazo:** Son factibles de realizar a medio plazo, debido a que la dificultad de implantación es media. Se trata de actuaciones

encaminadas a hacer operativa la estrategia país en ciberseguridad, identificar focos de investigación, identificar los activos existentes y las necesidades por parte de la industria y las actuaciones orientadas a retener el talento.

- **Actuaciones estratégicas a largo plazo:** Pese a que su realización tendría un impacto alto en la competitividad, son difíciles de llevar a cabo dada su complejidad de implantación. Se trata de actuaciones relativas al aumento de fondos dedicados a la I+D+i en ciberseguridad y la mejora en la eficiencia y orientación a resultados de los organismos de soporte a la investigación existentes.
- **Actuaciones no prioritarias:** Dado su medio o bajo nivel de impacto no su ejecución no son consideradas prioritarias.

4

ANÁLISIS DE OPORTUNIDAD Y DAFO DE LA CREACIÓN DE UNA RED DE CENTROS DE EXCELENCIA EN I+D+I EN CIBERSEGURIDAD

En este apartado se identifican los factores de oportunidad para la creación de una red de centros de excelencia en I+D+i en ciberseguridad en España.

4.1 Análisis de Oportunidad

Debido a la escasez de redes y modelos de colaboración globales específicos para la I+D+i en ciberseguridad, existe una clara oportunidad para la creación de una red de centros de excelencia en esta materia en España.

Esta red puede jugar un papel clave no sólo para agrupar y valorizar las capacidades del ecosistema, sino también para mejorar el posicionamiento de España en el panorama internacional.

Todos los agentes participantes en el estudio muestran un **acuerdo general sobre la necesidad de establecer una red** en España que ponga en común todos los recursos de la I+D+i.

Se considera que la red debiera tener unos objetivos concretos, tanto a largo como a corto plazo, una clara orientación a la **practicidad** y foco en la I+D+i y la transferencia, al tiempo que identifique problemáticas y oportunidades y los canales para su abordaje.

Se desataca la importancia de **identificar las capacidades y expertise de todos los agentes del ecosistema, así como un objetivo común** entre todos los integrantes, creando un clima de confianza para favorecer la generación de ideas, el intercambio de conocimiento y el desarrollo de proyectos conjuntos.

4.2 Análisis DAFO

El análisis DAFO ilustra de forma esquemática la visión de los agentes participantes en el estudio sobre la oportunidad y viabilidad en la creación de una red de centros de excelencia en I+D+i en ciberseguridad en España.

Debilidades	Amenazas
<ul style="list-style-type: none"> • Ecosistema fragmentado y desconectado. • No existen focos temáticos en materia de ciberseguridad (estrategias no operativas e inexistencia de planes específicos de I+D+i para el sector). • Falta de concreción de las políticas públicas. • Baja cultura de colaboración. • Falta de alineación Universidad-Empresa. • Baja coordinación entre Ministerios y agentes en ciberseguridad. • Bajo nivel de retención del talento. • Los programas de retribución del personal investigador ofrecen pocos incentivos a la carrera investigadora. 	<ul style="list-style-type: none"> • Entorno complejo y cambiante, tanto en amenazas como en tecnologías, que requiere de alta flexibilidad y capacidad de respuesta. • Crisis económica, que supone un escenario de restricción financiera, tanto público como privado. • La fuerte inversión de otros países en ciberseguridad, posiciona a la red en desventaja respecto a las redes de estos países para su posicionamiento en la arena global.
Fortalezas	Oportunidades
<ul style="list-style-type: none"> • Masa crítica investigadora. • Buen talento profesional e investigador. • Ciento nivel en la excelencia en el sistema investigador en ciberseguridad. • Capacidades del ecosistema para producir I+D+i, tanto a nivel del Sector Académico como de la industria. • Alta actividad de concienciación y sensibilización a la sociedad en ciberseguridad por parte de agentes del sector público. 	<ul style="list-style-type: none"> • Ausencia de redes similares en España. • Interés de la Unión Europea en esta iniciativa, que puede resultar una buena oportunidad de posicionamiento para España. • Los agentes del ecosistema consideran que es una necesidad, lo que produce buena disposición a participar. • Oportunidades en materia cultural y educativa, en relación con el emprendimiento y fomento de las vocaciones en ciberseguridad. • Margen para ganancias de eficiencia en el sistema de transferencia de resultados de la investigación. • Amplios márgenes de puesta en valor en el mercado de los resultados de la investigación. • Signos de mejora en el proceso de conexión de la universidad y la empresa, así como en la colaboración entre agentes públicos y privados. • Amplio foco de la ciberseguridad en el programa europeo de fomento de la I+D+i (Horizonte 2020). • Posicionamiento de España en las estrategias comunitarias y objetivos europeos en I+D+i en ciberseguridad, tanto a nivel país como a nivel agente. • Desarrollo y adopción de estándares y procesos para la certificación técnica.

Tabla 2 Análisis DAFO sobre la creación de una red de centros de excelencia en I+D+i en ciberseguridad

5

ALTERNATIVAS DE MODELOS DE RED DE EXCELENCIA

La propuesta de alternativas de modelos de red de Excelencia se ha realizado teniendo en cuenta la visión de los distintos agentes participantes en el estudio sobre cuál puede ser el mejor modelo de red.

Según dichos agentes el modelo de red debe cumplir dos premisas de partida:

- **Participación de todos los tipos de agentes** del ecosistema (Administraciones Públicas, Organismos de soporte a la I+D+i, la Industria y el Sector Académico).
- Permitir **distintos modelos de colaboración** (público – privado, privado – privado, público-público).

En lo relativo al modelo de red más adecuado no existe una opinión unánime: mientras algunos agentes entrevistados apuntan a la idoneidad de un **modelo abierto**, la opinión mayoritaria, estableciendo como estandarte el término **excelencia**, apuntan a la necesidad de un **modelo cerrado**.

Las reflexiones adicionales que realizan los agentes participantes recogen los siguientes elementos:

- Importancia de la presencia de los **key players** sectoriales.
- **Modelo cerrado** (filtros de entrada).
 - Núcleo selectivo y “excelente” con los mejores de su clase, los que más contribución pueden hacer (medición en base a criterios objetivos).
 - Capacidad de I+D+i contrastada.
 - Excelencia, rigor, expertise. Sólo pueden estar los agentes que aporten: capacidades, competencias y potencial.
- Los modelos muy abiertos pueden presentar **baja actividad y resultados**.
- Un **modelo mixto** permitiría la participación de todo el ecosistema y la generación de excelencia simultáneamente.
- Con respecto a la existencia de **subredes (nodos)**, los agentes apuntan:
 - No deben construirse necesariamente a partir de áreas de conocimiento.
 - Deben contar con actividades concretas en función de las necesidades.

- Los nodos deben apartar un valor claro.
- Finalmente, en lo relativo al **liderazgo y coordinación de la red**, la figura de INCIBE se perfila como candidata, siempre que mantenga un rol dinamizador y poco intervencionista. Algunas reflexiones adicionales de la inteligencia colectiva apuntan a:
 - Modelo de gestión de la red distribuido y compartido.
 - Rol conector entre nodos (hub).
 - La red debe evolucionar por sí misma con el impulso y apoyo de la administración (liderazgo “desde fuera”).

A partir de estas reflexiones, se han elaborado las distintas alternativas posibles de modelo de Red:

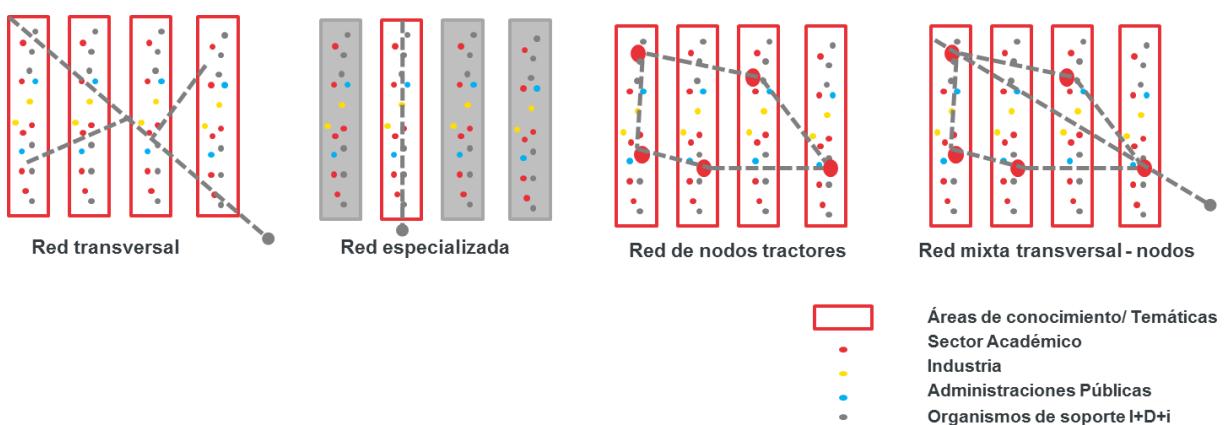


Figura 12 Alternativas de modelos de red

Red transversal: Orientada a múltiples áreas científico-tecnológicas¹⁰, aglutinaría a todos (o parte) de los agentes del ecosistema, buscando la conexión horizontal de todos ellos¹¹.

Esta tipología de red, dado su carácter abierto, podría tener una actividad generalista (ya que cubre múltiples áreas científico-tecnológicas). Los resultados de dicha actividad, en consecuencia, también serán previsiblemente de carácter general, imposibilitando la generación de masa crítica y referencia en áreas concretas.

La participación masiva de agentes podría dar lugar a cierta inoperatividad, tanto en la toma de decisiones como en la operación.

10 Tales como investigación, movilidad, hardware, ciberdefensa/ciberataque, secure coding y procedimientos y operaciones.

11 Se han identificado un total de 314 agentes: 20 Administraciones Públicas, 110 grupos de investigación en 42 Universidades, 3 Centros de Investigación, 2 Centros Tecnológicos, 43 Oficinas de Transferencia de Resultados de Investigación (OTRI), 8 Asociaciones empresariales, 3 Organismos certificadores y 125 empresas (identificadas en el marco del proyecto “Estudio de viabilidad, oportunidad y plan estratégico integrador de un polo tecnológico en ciberseguridad”).

Red especializada en una o varias áreas científico-tecnológicas, aglutinando a todos (o parte) de los agentes del ecosistema de I+D+i especializados en dicha área/s.

Este modelo busca la conexión vertical de los agentes – que trabajan en el área de especialización, permitiendo un foco claro, concentrando esfuerzos y recursos

Red de nodos tractores: Variante del modelo de red especializada, se trata de un modelo compuesto por hubs (nodos) especializados:

- La filosofía de los nodos es la orientación a la excelencia, de modo que sus miembros serán los “mejores de su clase”, garantizando una máxima aportación de valor al ecosistema. De esta forma, sólo podrían acceder aquellos agentes que son referentes y excelentes en el área de especialización de cada nodo.
- Los nodos estarán interconectados, componiendo una “trama de nodos” que, a modo de gran red, conecte a diferentes partes del ecosistema, creando una masa crítica global excelente.
- Se podrían distinguir dos tipos de nodos:
 - Especializados en áreas científico-tecnológicas, sectoriales, por aplicaciones de la ciberseguridad, etc.
 - Generales o transversales, tales como el emprendimiento, la financiación, etc.

La creación de los nodos (especialmente en lo relativo a la temática), su desarrollo y evolución, dependerá en gran medida de la evolución del ecosistema, de sus agentes así como de las prioridades y actividades que se determinen como clave en la red.

Este tipo de redes permite la orientación hacia la excelencia, si bien, en el contexto de la ciberseguridad, puede requerir cierto tiempo, pues será necesario determinar cuáles son las temáticas o áreas más excelentes o estratégicas sobre las que desarrollar los nodos, decisión que deberá consensuarse con el ecosistema, siempre bajo el paradigma de la excelencia.

Red Mixta (transversal-nodos). Se trata de un modelo híbrido que combina la red transversal con la red de nodos tractores. De este modo se permite simultáneamente aglutinar a todo el ecosistema a través de la parte transversal y considerar a los agentes excelentes a través de los nodos en temáticas concretas. Por tanto, combina las ventajas y bondades de los modelos transversal y nodal, salvando los inconvenientes de la red transversal a través de los focos establecidos en los nodos.

5.1 Valoración multicriterio de alternativas del modelo de red de Excelencia

Cada una de las alternativas posee ventajas y desventajas, que servirán de base para priorizar las alternativas y apoyar a la decisión final sobre el futuro modelo de Red:

Red trasversal	Ventajas	Inconvenientes
	<ul style="list-style-type: none"> Integra a todos los agentes del ecosistema. Actividad generalista: actividades genéricas y comunes a todos los miembros. Abarca la ciberseguridad con carácter general. 	<ul style="list-style-type: none"> Imposibilidad de creación de masa crítica y referencia en áreas concretas. Alto número de participantes: inoperatividad en la actividad y en la toma de decisiones. Servicios comunes que puedan no ser estratégicos. No hay foco en la excelencia.
Red Especializada	Ventajas	Inconvenientes
	<ul style="list-style-type: none"> Integra a todos los agentes del ecosistema dentro del área temática. Focalizada en las áreas prioritarias. Permite concentrar esfuerzos y recursos en áreas prioritarias. Desarrollo de actividades a medida para la temática en concreto. 	<ul style="list-style-type: none"> Pérdida de visión global. Desarrollo desigual de temáticas. No existe foco en la excelencia.
Red de nodos tractores	Ventajas	Inconvenientes
	<ul style="list-style-type: none"> Existencia de nodos tractores que lideren las actividades de la red. Orientación a la excelencia. Permite poner el foco en las áreas de excelencia prioritarias. Miembros excelentes en base a unos criterios (máxima aportación de valor). 	<ul style="list-style-type: none"> Agentes que no estén conectados a ningún hub. Puede requerir tiempo para desarrollarse. No resulta posible predecir la evolución de los nodos. Dificultad en la selección de nodos adecuados.
Red mixta Transversal - nodos	Ventajas	Inconvenientes
	<ul style="list-style-type: none"> Parte transversal de la red: Integración de todos los agentes de la red. Parte nodal de la red: especialización como elemento de liderazgo y excelencia en temáticas concretas. 	<ul style="list-style-type: none"> Mayor esfuerzo y complejidad en el funcionamiento.

Figura 13 Valoración de alternativas del modelo de red de excelencia

5.2 Presentación y validación de alternativas con los interesados

A partir del ejercicio de reflexión colectiva, se procedió a validar los principales hallazgos y alternativas de modelo de red con un grupo reducido de agentes (Focus Group), concluyéndose que el modelo más idóneo es un **modelo mixto que contenga una parte generalista y una parte especializada** articulada en nodos tractores.

- La parte transversal podría aglutinar a todos los agentes que así lo deseen. Es esta parte de la red la que podría encargarse de colaborar en la redacción del Plan Estratégico de I+D+i en ciberseguridad / Agenda Española de I+D+i en ciberseguridad así como en otros documentos de carácter estratégico nacional.
- La parte nodal sería un modelo cerrado que integraría tan sólo a los mejores dentro de cada nodo (el acceso a cada nodo contaría con criterios de entrada y

permanencia, por lo que un agente que deje de cumplir las condiciones de permanencia saldría del nodo).

Según INCIBE, la red es concebida como una **“Red de Excelentes para ofrecer servicios a todo el ecosistema”** donde “los grandes ayudan a los pequeños”; de este modo, el grupo de excelentes (miembros, con capacidad de decisión) podrán dar servicios a toda la comunidad (de no excelentes/asociados, sin capacidad de decisión), obteniéndose un ecosistema que paulatinamente vaya alcanzando unas mayores cotas de excelencia.

NOTA: Cabe destacar que el modelo de red seleccionado (**modelo mixto**) ha contado con un alto consenso entre los agentes participantes, si bien podría estar sujeto a modificaciones durante el desarrollo y definición de la Red.

6 MODELIZACIÓN DE LA RED

En línea con el **enfoque colaborativo** que se ha venido manteniendo a lo largo de todos los trabajos realizados en el marco de la presente iniciativa, la modelización estratégica se ha realizado partiendo de los elementos identificados durante el ejercicio de reflexión colectiva. Dichos elementos fueron validados con un grupo reducido de agentes (Focus Group), constituyendo la aproximación a la modelización estratégica detallada en este apartado.

No obstante, este enfoque de partida deberá ser aterrizado y, concretado en un Plan Estratégico de la red, que sentará las bases para la operación de la red en los próximos años. Dicho plan, una vez elaborado, deberá contar con un amplio respaldo de los agentes del ecosistema de I+D+i.

Finalmente, tanto la modelización estratégica como el Plan Estratégico de la red deberán estar alineados con los resultados del “Estudio de viabilidad, oportunidad y plan estratégico integrador de un polo tecnológico en ciberseguridad”, buscando el aprovechamiento de sinergias y complementariedades entre ambas iniciativas.

Como punto de partida, se muestran los principales resultados tanto de la inteligencia colectiva de los agentes del ecosistema como de la visión de INCIBE en relación a la modelización estratégica de la red.

En general, los agentes participantes en el estudio muestran un **alto interés** en la creación de una red y en la participación en ella, reconociendo al mismo tiempo la **complejidad en el diseño y la puesta en marcha** de una iniciativa de esta índole.

- Se deberán tener en cuenta los siguientes aspectos:
 - Puesta en común de los recursos de I+D+i (posicionamiento-país), incluyendo el reaprovechamiento de redes e iniciativas existentes para lograr sinergias (nexo conector: INCIBE).
 - La red no puede quedarse en una declaración de intenciones.
 - Liderazgo de alto nivel.
 - Incentivos y compromiso real (presupuesto).
 - Conexión internacional.
- Con respecto a los **objetivos**, los agentes apuntan a:
 - Objetivos generales y comunes, no particulares.
 - Foco en objetivos concretos, evitando la dispersión dispersión. Foco en I+D y transferencia (llevar productos al mercado) a medio y largo plazo y en gestación y generación de proyectos de I+D+i.

- Enfoque global (no regionalismos) y enfoque de negocio (orientación a resultados).
- Marcar el rumbo: identificar necesidades y darles solución.
- Colaboración práctica, más allá de acuerdos sin contenido.
- Colaborar en la definición de la estrategia en ciberseguridad a través de un Plan Estratégico de I+D+i en ciberseguridad o Agenda Española de I+D+i en ciberseguridad.
- Formación: alinear las necesidades formativas con la industria: definición del perfil del profesional en ciberseguridad.

- **Servicios** a ofrecer por la red:

- Foco en I+D y transferencia.
- Modelo en base a proyectos y retos concretos, prácticos.
- Financiación de propuestas excelentes, exigencia en el proceso de selección.
- Programa específico de I+D (Plan Nacional u otros mecanismos).
- Enfoque tipo H2020, propuestas y panel de expertos para diseñar planes de trabajo en cada temática.
- Paneles early-adopters para diseñar líneas de trabajo y resolver problemas de mercado.
- Factoría de ideas que acaben en consorcios y colaboraciones conjuntas.
- Infraestructura mínima (acceso a H2020, apoyo administrativo...).
- No es necesaria la vigilancia tecnológica.
- Evitar diluciones en networking, lobby y puesta en común sin objetivos concretos.
- Transferencia y flujo entre agentes y personas.
- Captación de talento (profesional e investigador).
- Formación.
- Encuentros permanentes.
- Intercambio de conocimiento.

Según INCIBE, la red debería caracterizarse por:

- Red con foco en resultados de I+D+i dirigidos a la industria.
- Orientación a la excelencia en I+D+i.
 - Orientación a la detección, atracción, retención y promoción del talento investigador.
 - Valor diferencial de la red. Capacidad de influencia en la Unión Europea (a través de la presencia de INCIBE en grupos de trabajo europeos).
 - Puesta en valor de los recursos para resolver las necesidades de la industria.
 - La red deberá contar con un marcado enfoque comercial (no orientada a la investigación teórica).

- En relación a los **servicios** que puede ofrecer la red, desde INCIBE se destaca:
 - Realización de proyectos diferenciales.
 - Homologación de prestadores de servicios (consultoría, valorización tecnológica, ...)
 - Estudios/Prospectivas: tendencias, estudios anuales...
 - Inteligencia competitiva.
 - Homologación de grupos de investigación.
 - La red no va financiará proyectos, sino que facilitará el acceso a financiación.
 - Puesta a disposición del ecosistema de recursos (infraestructuras, BBDD...).
 - Dotación de fondos para proyectos disruptivos (“sin viabilidad”) que provean de garantías a los emprendedores.
- INCIBE considera que la red debe ser **auto-sostenible** (tendrá apoyo en su lanzamiento, pero tras éste, debe ser autónoma a través de acuerdos, u otras actuaciones). Se hace necesario, por tanto, definir cómo recuperar los resultados/retornos de la financiación en la red.

6.1 Formulación estratégica de la red

La formulación estratégica de red se ha elaborado tomando como base la metodología de **Balance Score Card**, que permite definir la estrategia desde un punto de vista global (misión, visión y valores) y hacerla operativa en objetivos estratégicos, líneas de actuación y medidas.



Figura 14: Proceso de formulación estratégica de la red.

Cada uno de estos elementos ha sido sometido a un proceso de validación, concreción y consenso con un grupo de agentes del ecosistema (sesión de Focus Group).

6.1.1 Misión, visión y valores

6.1.1.1 Misión

La misión de la red de excelencia estará guiada por los siguientes aspectos clave:

- Competitividad.
- Puesta en valor y explotación de capacidades y recursos.
- Desarrollo de soluciones para el mercado.
- Transferencia.
- Excelencia en I+D+i.
- Contribución a la cooperación y colaboración entre agentes, cohesionando el ecosistema de I+D+i

Los agentes participantes del estudio ponen de manifiesto la idoneidad de incluir la palabra **excelencia** en el nombre de la red, dado que permite facilitar el proceso de captación de fondos y el posicionamiento de la red. Asimismo la excelencia no sólo debe ir orientada a la ciencia sino a poner en el mercado soluciones.

En lo referente a al concepto de I+D+i se puntualiza que Investigación no sólo incluye la investigación aplicada, sino también la básica, claramente necesaria en la ciberseguridad.

Algunas aproximaciones a la misión de la red de Centros de Excelencia en I+D+i en ciberseguridad serían:

1. “**Puesta en valor de los recursos investigadores excelentes** de I+D+i en ciberseguridad en España, logrando el desarrollo de soluciones que respondan a necesidades del mercado mejorando la competitividad del sector, y aunando esfuerzos para superar la fragmentación existente”.
2. “**Potenciar la I+D+i en ciberseguridad** a través de la puesta en común de los **recursos excelentes** del ecosistema para impulsar la ciberseguridad en España y lograr la **transferencia** de los resultados de la investigación al mercado”.
3. “**Identificar** las necesidades y prioridades del ecosistema **y definir y explotar** las capacidades del ecosistema”.

6.1.1.2 Visión

La visión de la red de Excelencia debe estar regida por **lograr un posicionamiento en el ecosistema internacional**.

Los participantes del estudio consideran básico trascender las fronteras españolas y dotar a la red de una dimensión internacional (Europa y otras geografías) y proponen que desarrolle un Plan para el desarrollo relaciones institucionales con agentes internacionales.

Posibles alternativas de la definición de la visión de la red son las siguientes:

1. “Posicionar a España como uno de los **referentes en ciberseguridad** en el entorno internacional”.

2. **“Posicionar el ecosistema de I+D+i en ciberseguridad dentro de la arena global como un ecosistema competitivo, con altos niveles de transferencia y valorización tecnológica y con un alto grado de colaboración y conexión entre sus agentes”.**

6.1.1.3 Valores

Excelencia, practicidad, rigor, transparencia¹², confianza, espíritu de equipo, dimensión internacional.

6.1.2 Objetivos estratégicos, líneas de actuación y medidas

Los objetivos estratégicos, líneas de actuación y medidas de la red deben estar totalmente alineados con la misión, la visión y los valores, ya que constituyen el aterrizaje y concreción de los mismos.

Los objetivos finalmente identificados (consensuados con los agentes del ecosistema que han asistido a las sesiones de Focus Groups) son:

1. **Posicionar** la I+D+i en el ámbito de la ciberseguridad a nivel europeo e internacional.
2. **Desarrollar** soluciones innovadoras a través de la I+D+i
3. Potenciar la **transferencia tecnológica** desde la investigación al mercado en colaboración con el Polo Tecnológico de Ciberseguridad.
4. Identificar, atraer, generar y retener el **talento** de profesionales en ciberseguridad a nivel nacional

Los objetivos estratégicos se perfilan en líneas de actuación y en medidas que concretan las actividades específicas a realizar por parte de la Red.

NOTA: Las **líneas de actuación y medidas** o actividades concretas a realizar por parte de la red son, a fecha de creación de este documento, objeto de debate y de consenso entre los colaboradores de esta iniciativa. Puesto que es trabajo en curso puede sufrir modificaciones. El **Anexo II LÍNEAS ESTRATÉGICAS Y MEDIDAS** contiene una descripción de estas líneas y medidas con más detalle.

Se han identificado, con carácter general, diferentes tipologías de medidas:

- **Estudios y prospectivas** que ayuden a clarificar aspectos importantes y puedan guiar futuras iniciativas concretas.
- Realización de **eventos específicos** que sirvan de escaparate en el que tanto la red en particular como el ecosistema en general, puedan mostrar las capacidades del ecosistema español en esta materia.
- **Premios** a la investigación de excelencia.

¹² Se indica la necesidad de la existencia de diferentes niveles de transparencia y confidencialidad por parte de la red.

- **Comunicación, difusión y relaciones institucionales** para establecer la estrategia de relación y posicionamiento de la red dentro el ecosistema tanto nacional como europeo.
- Detección de las **ideas/proyectos** de investigación excelentes y de alto potencial, diseñando un mecanismo para su valoración y desarrollo en proyectos de I+D+i.
- **Catálogo o repositorios** con las investigaciones disponibles y sus derechos de explotación asociados, para facilitar su comercialización.
- **Apoyo administrativo** a la gestión de proyectos, poniendo en contacto a los agentes del ecosistema y apoyando la fase de preparación de propuestas de proyectos de I+D+i.

6.2 Alineamiento estratégico con el proyecto del polo tecnológico en ciberseguridad

Las iniciativas que INCIBE está desarrollando en materia de ciberseguridad deben estar conectadas, coordinadas y sincronizadas aprovechando las sinergias y economías de escala. En este sentido, es destacable la estrecha relación de la red de Excelencia con la iniciativa Polo Tecnológico en ciberseguridad.

En este apartado se detallan, a grandes rasgos, los **principales puntos de intersección y sinergias entre ambas iniciativas**; no obstante, al estar ambas en proceso de desarrollo, la coordinación deberá ser dinámica y constante a lo largo del tiempo.

- El objetivo estratégico de la red de Excelencia **1. Posicionar la I+D+i en el ámbito de la ciberseguridad a nivel europeo e internacional**, deberá contar con la participación de aquellos agentes relevantes de la industria del Polo, de modo que el posicionamiento contemple una visión extendida de las necesidades de la industria, y ésta quede convenientemente reflejada en las estrategias en ciberseguridad.
- El objetivo estratégico de la red de Excelencia **4. Identificar, atraer, generar y retener el talento de profesionales en ciberseguridad a nivel nacional**, también es foco de la iniciativa Polo Tecnológico, por lo que ambas iniciativas deberán poner un foco especial de coordinación y cooperación en este ámbito.
- En lo relativo a la formación, la red de Excelencia, durante el proceso de validación colectivo de los objetivos estratégicos y medidas, **descartó la realización directa de acciones de formación**, que ya son provistas por otros agentes del ecosistema. En su lugar se acordó que la red deberá jugar un papel activo en la detección de las necesidades de formación y capacitación. En caso de que el Polo decida finalmente desarrollar acciones en materia de formación, éstas deberán estar estrechamente coordinadas y alimentadas con las necesidades que la red detecte.
- **Actuaciones vinculadas al emprendimiento**. Durante la validación de los objetivos de la red con los agentes del ecosistema, **se acordó que lo relativo a este tema debería ser liderado y coordinado por el Polo Tecnológico**.

- La red deberá trabajar estrechamente con el Polo en todo lo relacionado con el objetivo estratégico de la red **3. Potenciar la transferencia tecnológica desde la investigación al mercado en colaboración con el Polo Tecnológico de ciberseguridad**. Para medidas concretas relativas a la incubación de proyectos (búsqueda y selección de resultados de investigación para su transferencia al mercado), es necesario destacar amplias posibilidades de colaboración entre ambas iniciativas, de forma que la red pudiera realizar los primeros filtros (seleccionar aquellas ideas con potencial, realizar una validación tecnológica) apoyándose en el polo para realizar la validación de negocio.
- En las medidas relacionadas con **networking, eventos y otras acciones de posicionamiento**, ambas iniciativas deberán analizar las medidas a ejecutar, buscando las sinergias e incluso la posibilidad de celebración conjunta de este tipo de actividades.
- Finalmente, será altamente recomendable que todas las medidas a implementar por parte de la red en materia de **estudios y análisis, estén coordinadas con el Polo Tecnológico** en todos aquellos casos en los que dichos estudios tengan impacto o relación con la industria de la ciberseguridad.

7

PLAN DE ACCIÓN: HOJA DE RUTA DE ACTUACIONES A CORTO, MEDIO Y LARGO PLAZO

El Plan de acción para la puesta en marcha de la red consta de cuatro grandes fases. Las fases 0 y 1 se llevarán a cabo durante el **primer año de vida de la red (2015)**, de manera que al finalizar este año la red habrá comenzado sus actividades. A partir de 2016 la red pasará a la plena operación.

A continuación se ilustran las fases del Plan de Acción así como las actividades a ejecutar en cada una de ellas:



Figura 15: Fases del Plan de Acción.

El **Plan Estratégico de la red** constituye el eje principal de actividad, estableciendo los objetivos estratégicos, líneas de actuación y medidas a ejecutar. Cabe destacar que las medidas de dicho plan, que actualmente se encuentran en proceso de definición, tendrán un horizonte temporal de dos años (2015 y 2016). A partir de 2017 el Plan Estratégico deberá ser revisado, a fin de definir las nuevas actuaciones que, en el marco de la estrategia, ejecute la red.

7.1 Fase 0: Definición colaborativa

Esta fase constituyó el **proceso colaborativo y participativo con el ecosistema** para la definición, consenso y respaldo de los temas clave de la red, habiéndose acordado las siguientes premisas clave:

- La idoneidad de una red **mixta**, con una parte transversal y otra formada por nodos especializados.
- La **participación en la red de todos los tipos de agentes** existentes en el ecosistema (ciencia, administración, industria, agentes de soporte a la I+D+i).
- La necesidad de fijar **criterios de entrada y salida**, basados en la excelencia, de los miembros en los nodos especializados.
- La idoneidad de crear un **Plan Estratégico de I+D+i** en ciberseguridad.
- **Nombre** de la red.
- **Formulación estratégica**. Misión, visión y valores, objetivos estratégicos, líneas de actuación y medidas a ejecutar durante 2015.
- **Servicios o actividades** aponer en marcha.
- **Modelo de sostenibilidad**, entendido como las fuentes de ingresos así como las necesidades de financiación. Será necesario seguir reflexionado sobre este tema en el futuro, dada su complejidad.
- **Modelo de participación y expansión**: definición de criterios de entrada y de salida de miembros, tanto en su parte transversal como en su parte nodal. Será necesario seguir reflexionado sobre este tema en el futuro, dada su complejidad.

7.2 Fase 1: Arranque del piloto

Las actividades a desarrollar durante esta fase servirán de punto de partida para el inicio de las actividades y se concretarán en el **Plan Estratégico de la red para 2015**. Durante esta fase, INCIBE actuará como ente coordinador.

El mencionado Plan Estratégico contemplará dos grandes tipos de actuaciones:

- **Implementación de las medidas** a ejecutadas en año 2015.
- Actividades de **creación de la red** en sus aspectos jurídicos y operativos:
 - **Constitución** de la forma jurídica.
 - **Modelo de gobierno**. Esta actividad incluirá la selección de los miembros del comité ejecutivo, la constitución de los órganos de gobierno y la redacción formal de los Estatutos de la Red.
 - **Modelo de gestión**, a través de la definición del Comité de Dirección, sus roles y funciones así como las áreas de actividad que tendrá la red en el nodo transversal.
 - Realización de **otras actividades** necesarias para la puesta en marcha de la red tales como la preparación de infraestructuras físicas y tecnológicas.
 - Creación del **nodo transversal**.

7.3 Fase 2: Despliegue

Esta fase, que se extenderá a lo largo de 2016, se orientará a la ampliación de la actividad. Por un lado se dará continuidad a las medidas establecidas en el Plan Estratégico que

comenzaron en 2015 y de otro, se definirán los **nodos temáticos** que conformarán la red. En lo relativo a los nodos, se deberán abordar las siguientes actividades:

- Las **prioridades y objetivos estratégicos** de cada nodo, en alineación con las estrategias nacionales y europeas en materia de ciberseguridad.
- A partir de los objetivos estratégicos de cada uno de los nodos, se definirán las medidas a ejecutar y las **áreas de actividad** que serán necesarias para dar respuesta a los mismos.
- El **modelo de colaboración y cooperación**.
- El **modelo de participación y expansión** (criterios de acceso y permanencia).

Finalmente, en esta fase se continuará con el despliegue de las infraestructuras lógicas, ya iniciado durante la fase 1 y se reclutará el personal de la red.

7.4 Fase 3: Estabilización

Durante esta fase la red procederá a **estabilizarse y a estar en plena operación**, tanto en la parte transversal como nodal.

Durante esta fase **no pueden anticiparse las actividades** que, a parte de la operativa diaria y la actualización del Plan Estratégico de la red puedan derivarse, dado que estará sujeto a la propia evolución de la red.

7.5 Fase transversal: Gestión de la implantación

La gestión de la implantación se extenderá durante todas las fases a excepción de la fase de estabilización y se orienta a dotar a la red de un modelo para la gestión, evaluación y seguimiento de la estrategia de la red.

Para la ejecución de estas actividades se recomienda la **creación de una oficina estratégica**, que permitirá disponer de una visión global de la red, más allá de la ejecución de medidas concretas, aportando las metodologías, herramientas, técnicas y el modelo de gestión para el soporte de la estrategia. Esta oficina actuará en tres niveles:

- **Gestión estratégica.** A partir de la estrategia de la red definida para los próximos años, la oficina gestionará la ejecución de los objetivos estratégicos.
- **Gestión táctica**, orientada a la definición de las medidas concretas, su presupuesto y recursos asociados.
- **Gestión operativa**, orientada a la gestión, supervisión y control de las medidas a ejecutar, así como de las actividades a ejecutar dentro de cada medida. También se orientará a ejecutar aquellas actividades que den soporte a la operativa diaria de la red.

7.6 Calendario Plan de Acción

En este apartado se muestran el cronograma general del Plan de Acción.

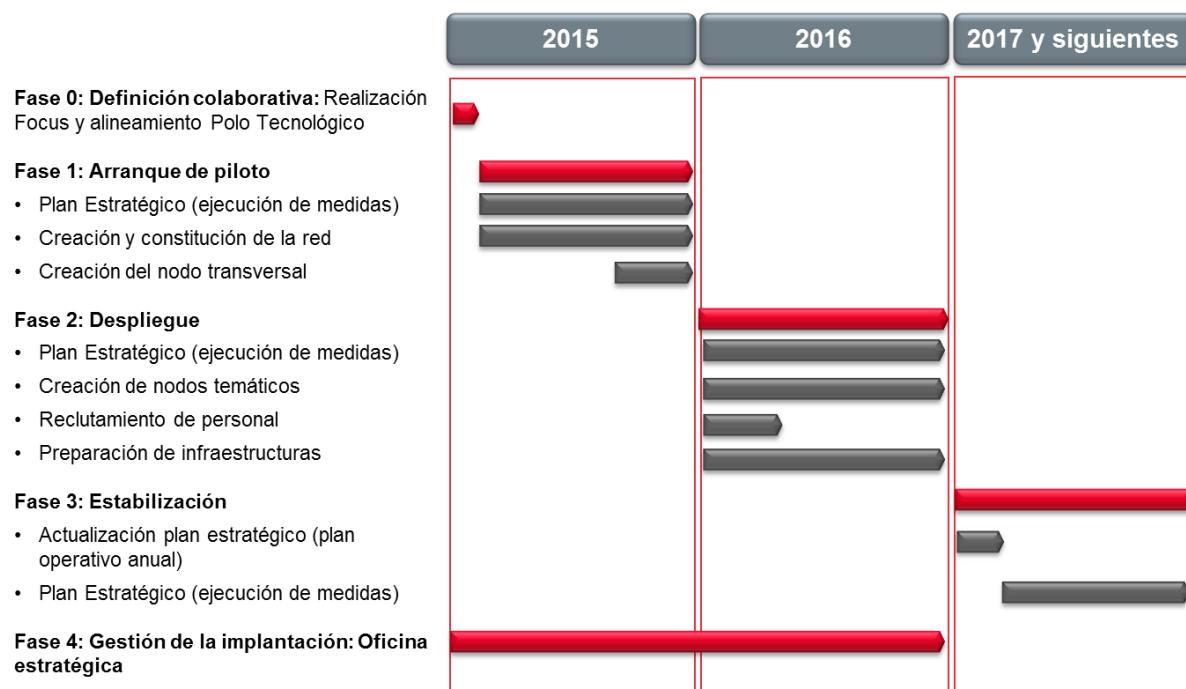


Figura 16: Cronograma general del Plan de Acción.

ANEXO I PARTICIPANTES EN EL ESTUDIO

AI.1 ENTREVISTAS

Organismo / Institución / Empresa	Persona entrevistada	Cargo
Agencia de Innovación, Financiación e Internacionalización Empresarial de Castilla y León	Carlos Escudero Martínez	Director de Departamento
Agencia de Innovación, Financiación e Internacionalización Empresarial de Castilla y León	Javier García Díez	Director de Departamento
Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas	Tomás Castro	Presidente
Axencia Galega de Innovación	Manuel Varela Rey	Director
Axencia Galega de Innovación	Sonia Pazos Álvarez	Directora Área Centros
Carnegie Mellon University (Software Engineering Institute - CERT Division)	Robert C. Seacord	Secure Coding Manager
Centro de Ciberseguridad Industrial	Samuel Linares	Director
Comisión Europea – Directorate-General for Communications Networks, Content and Technology Trust and Security	Martin Muehleck	Programme Officer - EU policies at DG CNECT
Consejo Superior de Investigaciones Científicas	Luis Hernández Encinas	Científico Titular
CriptoLab. Laboratorio de Criptología de la Universidad Politécnica de Madrid	Jorge Dávila Muro	Director
IE Business School	Peter Bryant	Assistant Professor of Entrepreneurship
Indra	Jorge López Hernández-Ardieta	Jefe del grupo de Investigación en Ciberseguridad
Inixa Security	Julio Rilo	Director
Instituto Nacional de Ciberseguridad (INCIBE) – Ministerio de Industria, Energía y Turismo	Raúl Riesco Granadino	Gerente de I+D+i
S21sec	José Alemán	Law Enforcement and Defence Line of Business Manager
S2GRUPO	Miguel Juan	Socio Director
Tecnalia	José Javier Larrañeta	Responsable del área de seguridad en infraestructuras
Universidad Carlos III – Computer Security Lab	Juan Manuel Estévez Tapiador	Profesor Titular de Universidad
Universidad de Granada	Pedro García Teodoro	Catedrático adscrito al Grupo Ciberseguridad UGR
Universidad de Oviedo	Santos González Jiménez	Catedrático de Álgebra
Universidad de Vigo	Fernando Pérez-González	Catedrático Universidad de Vigo
Universidad de Vigo	Juan Ramón Troncoso	Investigador Postdoctoral Universidad de Vigo
Universidad Europea de Madrid	Mª Teresa Villalba de Benito	Profesora Titular/investigadora y

Organismo / Institución / Empresa	Persona entrevistada	Cargo
		Directora del Máster Universitario en Seguridad TIC
Universidad Politécnica de Madrid	Victor Villagrá	Profesor Titular e Investigador en Gestión y Seguridad de Redes y Servicios de Telecomunicación.

AI.2 CUESTIONARIOS

Organismo / Institución / Empresa	Persona encuestada	Cargo
Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas	Roberto Vidal	Vicepresidente
Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas	Tomás Castro	Presidente
Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales	Javier Vendrell García	Gerente de I+D
Asociación Nacional de Ciberseguridad y Pericia Tecnológica(ANCITE)	José Luis Narbona	Presidente
Centro Nacional para la Protección de las Infraestructuras Críticas	Miguel Ángel Abad	Jefe del Servicio de Ciberseguridad
Centro para el Desarrollo Tecnológico Industrial	Maite Boyero Egido	Delegada española de Sociedades Seguras y punto de contacto nacional y del Programa Marco H2020
Centro Tecnológico Cartif	Mónica Antón	Coordinadora de Proyectos Internacionales
CITIC - Centro Andaluz de Innovación y Tecnologías de la Información y las Comunicaciones	Desireé Bellido	Subdirectora
Confederación Española de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica	Gloria Díaz	Gerente
Consejo Superior de Investigaciones Científicas	Victor Antonio Gayoso Martínez	Doctor
Innovation 4 Security	Rafael Ortega	Director General
PANDA	Salvador Sánchez Taboada	Cyber Defense Strategic Sales Director
S21SEC	Irene Eguinoa	Research Manager

Organismo / Institución / Empresa	Persona encuestada	Cargo
Tecnalia	Ana Ayerbe	Directora de Área IT Competitiveness
Universidad Autónoma de Madrid	Jorge E. López de Vergara Méndez	Profesor Titular de Universidad
Universidad Castilla La Mancha	Francisco Ruiz	Catedrático de Informática
Universidad Complutense de Madrid - Grupo de Análisis, Seguridad y Sistemas (GASS)	Luis Javier García Villalba	Director
Universidad de Alcalá	Juan Ramón Velasco Pérez	Catedrático
Universidad de Alicante	Antonio Zamora Gómez	Profesor, Doctor y Director del grupo de Criptología y Seguridad Computacional
Universidad de Alicante	Francisco Maciá Pérez	Vicerrector de Tecnologías de la Información
Universidad de La Laguna	Pino Caballero Gil	Doctora
Universidad de Málaga	José Mª Troya Linero	Catedrático
Universidad de Málaga, NICS Lab	Javier López	Director
Universidad de Mondragón	Roberto Uribeetxeberria	Coordinador de Investigación y Transferencia
Universidad de Murcia	Gregorio Martínez Pérez	Catedrático de Universidad
Universidad de Sevilla	Rafael Martínez Gasca	Profesor Titular
Universidad del País Vasco / Euskal Herriko Unibertsitatea	Begoña Blanco Jáuregui	Profesora
Universidad del País Vasco / Euskal Herriko Unibertsitatea	Eduardo Jacob	Profesor
Universidad del País Vasco / Euskal Herriko Unibertsitatea	José Luis Martín González	Catedrático de Tecnología Electrónica
Universidad Europea de Madrid	Juan José Escribano	Director Académico ITIA: Industriales, Telecomunicaciones Aeroespacial e Informática
Universidad Politécnica de Madrid	Ana Gómez Oliva	Catedrática E.U.
Universidad Politécnica de Madrid	Julio Berrocal	Doctor
Universidad Pública de Navarra	Eduardo Magaña Lizarrondo	Profesor titular
Universitat Autònoma de Barcelona	Jaume Pujol Capdevila	Catedrático de Escuela Universitaria
Universitat de les Illes Balears	Guillem Femenias Nadal	Investigador Principal

Organismo / Institución / Empresa	Persona encuestada	Cargo
Universitat Oberta de Catalunya	David Megías Jiménez	Doctor
Universitat Politècnica de Catalunya	Javier Herranz	No disponible
Universitat Politècnica de Catalunya	Jorge García Vidal	No disponible
Universitat Politècnica de Catalunya	Miguel Soriano	Catedrático
Universitat Politècnica de València	Carlos Miguel Tavares Calafate	Profesor Titular
Universitat Rovira i Virgili	Josep Domingo-Ferrer	Catedrático

AI.3 PARTICIPANTES EN LOS FOCUS GROUP

AI.3.1 PRIMER FOCUS GROUP

LISTADO DE ASISTENTES AL FOCUS GROUP 1	
ORGANISMO	ASISTENTE
Agencia de Innovación, Financiación e Internacionalización Empresarial de Castilla y León (ADE)	Carlos Escudero Martínez
Agrupación Empresarial Innovadora en Ciberseguridad y Tecnologías Avanzadas (AEI Ciberseguridad)	Tomás Castro
Consejo Superior de Investigaciones Científicas (CSIC)	Luis Hernández Encinas
Indra	Jorge López Hernández-Ardieta
Inixa Security	Julio Rilo Blanco
S21sec	José Alemán
S2GRUPO	José M. Rosell
Universidad Carlos III - Computer Security Lab (COSEC)	Juan Manuel Estévez Tapiador
Universidad de Oviedo	Santos González Jiménez
Universidad de Vigo	Fernando Pérez-González
Universidad de Vigo	Juan Ramón Troncoso

AI.3.2 SEGUNDO FOCUS GROUP

LISTADO DE ASISTENTES AL FOCUS GROUP 2	
ORGANISMO	ASISTENTE
Agencia de Innovación, Financiación e Internacionalización Empresarial de Castilla y León (ADE)	Carlos Escudero Martínez
Consejo Superior de Investigaciones Científicas (CSIC)	Luis Hernández Encinas
Indra	Jorge López Hernández-Ardieta
Inixa Security	Julio Rilo Blanco
Tecnalia	José Javier Larrañeta
S21sec	José Alemán
S2GRUPO	Miguel Juan
Tecnalia	Ana Ayerbe
Universidad de León	Miguel Carriegos Vieira
Universidad de Vigo	Fernando Pérez-González
Universidad de Vigo	Juan Troncoso

ANEXO II LÍNEAS ESTRATÉGICAS Y MEDIDAS

Este anexo enuncia, para cada uno de los objetivos o ejes estratégicos definidos, las líneas de actuación y describe brevemente las medidas asociadas. El Plan Estratégico de la red una vez terminado, incluirá una mayor descripción y concreción de cada una de estas medidas.

NOTA: Las **líneas de actuación y medidas** o actividades concretas a realizar por parte de la red son,

La formulación estratégica resultante hace un total de **4 objetivos estratégicos, 9 líneas de actuación y 22 medidas**:

MEDIDAS ASOCIADAS A LOS OBJETIVOS ESTRATÉGICOS DE LA RED		
OBJETIVO ESTRATÉGICO	LÍNEA DE ACTUACIÓN	MEDIDA
1. Posicionar la I+D+i española en el ámbito de la ciberseguridad a nivel europeo e internacional	L.1 Caracterización del sector I+D+i de Ciberseguridad en España y su posición a nivel global	<p>M.1 Definición del mapa de conocimiento de la I+D+i en ciberseguridad desde una doble perspectiva: Nivel macro: Caracterización general del ecosistema, a través de las dinámicas de actividad, el contexto y el marco de actuación en el que se desenvuelve el ecosistema. Nivel micro: Mapa de agentes que permita conocer, para cada agente del ecosistema, cuáles son su capacidades, conocimientos, competencias, experiencia y potencial en materia de I+D+i en ciberseguridad</p>
	L.2 Desarrollo de una Agenda Estratégica Nacional de I+D+i en ciberseguridad	<p>M.2 Análisis y diagnóstico de las barreras o inhibidores (condicionantes o retos) así como impulsores e incentivos sociales, tecnológicos, económicos o regulatorios para incentivar la investigación en I+D+i en ciberseguridad.</p> <p>M.3 Detectar problemáticas y necesidades no resueltas en el mercado por parte de los usuarios finales (administraciones públicas, Defensa, FCSE empresas, sectores estratégicos, ciudadanos) para la generación de proyectos de I+D+i conjuntos entre la industria y la ciencia. Cabe destacar la relevancia de la demanda sofisticada (CERTs, Defensa, Finanzas, etc.) cuyos retos no cubiertos suponen oportunidades y modelos de negocio con elevado potencial a nivel global.</p> <p>M.4 Identificación de prioridades en investigación de I+D+i en ciberseguridad (focos y líneas de actuación en I+D+i)</p>

MEDIDAS ASOCIADAS A LOS OBJETIVOS ESTRATÉGICOS DE LA RED		
OBJETIVO ESTRATÉGICO	LÍNEA DE ACTUACIÓN	MEDIDA
		<p>M.5 Definición y propuesta de creación de los nodos de especialización de la red en base a los resultados de la Agenda Estratégica. Revisión y alineamiento del Plan Estratégico de la Red (I+D+i / Transferencia / Internacionalización) acorde a las Agendas Estratégica Española y Europea de I+D+i en ciberseguridad</p>
		<p>M.6 Definición del Plan de Comunicación y Modelo de Relaciones de la Red.</p>
		<p>M.7 Plan de publicaciones y participación en congresos y plataformas de referencia internacional.</p>
	L.4 Estímulo a la innovación	<p>M.8 Apoyo para la puesta en marcha de incubadoras de ideas y programas de identificación y resolución de retos en ciberseguridad (crowdsourcing y acceso a retos de elevado potencial de mercado -- identificados por la demanda sofisticada en ciberseguridad).</p>
2. Desarrollar soluciones innovadoras a través de la I+D+i	L.5 Impulso y estímulo al desarrollo de Proyectos I+D+i en base a la Agenda Estratégica	<p>M.9 Actuar como facilitador, mediador o dinamizador para encontrar fórmulas de financiación a proyectos de I+D+i.</p> <p>M.10 Apoyo administrativo a la gestión de proyectos. Mecanismos de networking y puesta en contacto entre agentes del ecosistema, así como apoyo y consultoría en la preparación y mejora de propuestas para convocatorias de proyectos de I+D+i en concurrencia competitiva.</p>
	L.6 Reconocimiento a la I+D+i de excelencia	<p>M.11 Facilitar infraestructura tecnológica que habilite la gestión y ejecución (laboratorio remoto) de proyectos de I+D+i entre los participantes de la Red, potenciando un aumento de la actividad y cooperación en proyectos de I+D+i en ciberseguridad.</p> <p>M.12 Premios a la investigación de excelencia. Diseño de mecanismos de evaluación y selección de candidaturas, convocatoria para la presentación de propuestas de reconocimiento, celebración del evento y acciones de comunicación</p>
3. Potenciar la transferencia tecnológica desde la investigación al mercado en colaboración con el Polo Tecnológico	L.7 Apoyo a la valorización y transferencia tecnológica en colaboración con el Polo Tecnológico	<p>M.13 Programa de aceleración de proyectos empresariales (detección de los resultados de I+D+i excelentes y con alto potencial de transferencia al mercado) en colaboración con el Polo Tecnológico</p> <p>M.14 Creación de un repositorio de resultados de investigación nacional en Ciberseguridad. Repositorio con las investigaciones disponibles y sus derechos de explotación asociados, para</p>

MEDIDAS ASOCIADAS A LOS OBJETIVOS ESTRATÉGICOS DE LA RED		
OBJETIVO ESTRATÉGICO	LÍNEA DE ACTUACIÓN	MEDIDA
Nacional de Ciberseguridad		<p>facilitar la comercialización y valorización de estas investigaciones.</p> <p>M.15 Colaboración con el Polo Tecnológico para la creación de un catálogo de proveedores de servicios de valoración tecnológica y transferencia que cumplan con determinados requisitos exigidos por la Red. Repositorio para los agentes del ecosistema que necesiten de estos servicios, garantizando el acceso a proveedores que cumplen determinados requisitos de calidad y solvencia.</p> <p>M.16 Realización de Jornadas/eventos para emprendedores (Pitch Elevator, Pitch To Market, etc.). Preparación y celebración del evento y acciones de comunicación asociadas.</p> <p>M.17 Jornadas nacionales de I+D+i en Ciberseguridad. Punto de encuentro científico en el que tanto la red en particular como el ecosistema en general, puedan mostrar las capacidades tanto en conocimiento y talento como en resultados de investigación y su potencial de transferencia al mercado. Sinergia con otras iniciativas y medidas de la Red.</p>
4. Identificar, atraer, generar y retener el talento investigador en ciberseguridad a nivel nacional	<p>L.8 Identificación de necesidades para la promoción del talento investigador en ciberseguridad</p>	<p>M.18 Definir el perfil y competencias del investigador en ciberseguridad. Proceso participativo para determinar cuáles son los skills, capacidades y habilidades básicas que deberá tener el perfil investigador en ciberseguridad de la Red, es especial en los campos de la I+D+i, la enseñanza y el perfil emprendedor.</p> <p>M.19 Análisis diferencial de la oferta formativa en ciberseguridad para cubrir las necesidades para el desarrollo del talento en ciberseguridad, tanto curriculares (perfiles demandados tanto en la ciencia como en la industria) como formativas. Colaboración Administración - Ciencia - Mercado</p>
	<p>L.9 Detección y revisión de los mecanismos de retención del talento</p>	<p>M.20 Colaboración con otros agentes del ecosistema en actividades para la promoción, detección, captación, atracción y retención de talento sobre las salidas profesionales de la ciberseguridad</p> <p>M.21 Captación/intercambio de talento dentro del ecosistema. Identificar y concretar los mecanismos para retener, captar e intercambiar talento investigador dentro y hacia el ecosistema nacional.</p> <p>M.22. Promocionar y facilitar el acceso al talento investigador de la Red por parte del Polo Tecnológico. Colaboración de profesionales</p>

MEDIDAS ASOCIADAS A LOS OBJETIVOS ESTRATÉGICOS DE LA RED		
OBJETIVO ESTRATÉGICO	LÍNEA DE ACTUACIÓN	MEDIDA
		investigadores con la Industria para el desarrollo de soluciones y servicios innovadores de ciberseguridad.

ANEXO III FUENTES DOCUMENTALES CONSULTADAS

- Agencia Española de Protección de Datos (AEPD) (<http://www.agpd.es/>).
- Agencia Europea de Defensa (EDA) (<http://www.eda.europa.eu/>).
- Agencia Europea de la Seguridad de las Redes y la Información (ENISA) (http://europa.eu/abouteu/agencies/regulatory_agencies_bodies/policy_agencies/enisa/index_es.htm).
- Agenda Digital Europea. Unión Europea.
- Agenda Digital para España. 2013/2014. Ministerio de Industria, Energía y Turismo, Ministerio de Hacienda y Administraciones Públicas.
- Centro Criptológico Nacional (CCN) (<https://www.ccn.cni.es/>).
- Centro de Ciberseguridad Industrial (<https://www.cci-es.org/>).
- Centro de Excelencia para la Cooperación en Ciberdefensa (CCDCOE) (<https://www.ccdcoe.org/>).
- Centro Nacional de Inteligencia (CNI) (<http://www.cni.es/>).
- Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) (<http://www.cnpic-es.es/>).
- Centro para el Desarrollo Tecnológico Industrial (CDTI) (<https://www.cdti.es/>).
- Cibersecurity Coordination Group (CSCG) (<http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx>).
- Ciberseguridad en España: una propuesta para su gestión. Enrique Fojón Chamorro y Ángel F. Sanz Villalba. Real Instituto Elcano.
- Comisión Europea (http://ec.europa.eu/index_es.htm).
- Competitive analysis of the UK cyber security sector. 29 de julio de 2013. Pierre Audoin Consultants.
- [Congreso Cybercamp 2014](http://cybercamp.es/) (<http://cybercamp.es/>).
- [Cybercamp](https://cybercamp.es/) (<https://cybercamp.es/>).
- Cybercrime Centres of Excellence Network for Training Research and Education (<http://www.2centre.eu/>).
- Cybersecurity policy making at a turning point, Analysing a new generation of national cybersecurity strategies for the Internet economy. 2012. Organización para la Cooperación y el Desarrollo Económico (OCDE).
- CyberTech Israel (<http://www.cybertechisrael.com/>).
- ENISA (<http://www.enisa.es/>).
- Estrategia de Seguridad Marítima Nacional. 2013. Departamento de Seguridad Nacional, Presidencia del Gobierno.
- Estrategia de Seguridad Nacional. 2013. Presidencia del Gobierno.
- Estrategia Española de Ciberseguridad. 2013. Presidencia del Gobierno.
- Estrategia Europea de Ciberseguridad. 2012. European Union Agency for Network and Information Security (ENISA).

- Estrategia Regional de Investigación e Innovación para una Especialización Inteligente. RIS3 de Castilla y León. 2014- 2020. 16 de abril de 2014.
- European Association for e-identity and Security EEMA (<https://www.eema.org/>).
- European Network for Cybersecurity (<https://www.enics.eu/>).
- European Public Private Partnership for Resilience (<http://www.enisa.europa.eu/>).
- European Research Council (ERC) (<http://erc.europa.eu/>).
- European Technology Platform on Industrial Safety (<http://www.industrialsafety-tp.org/>).
- Europol (<https://www.europol.europa.eu/>).
- Grupo de Expertos de Alto Nivel de la Agenda Digital para España. Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la Agenda Digital para España. 18 de junio de 2012.
- Guía rápida Horizonte 2020. Centro para el Desarrollo Tecnológico Industrial (CDTI).
- Horizon 2020. Work Programme 2014 – 2015. Leadership in enabling and industrial technologies. Unión Europea.
- Horizon 2020. Work Programme 2014 – 2015. Leadership in enabling and industrial technologies. Information and Communication Technologies. Unión Europea.
- Horizon 2020. Work Programme 2014 – 2015. Secure societies – Protecting freedom and security of Europe and its citizens. Unión Europea.
- Horizonte 2020 (<http://www.eshorizonte2020.es/>).
- IETF (<https://www.ietf.org/>).
- II Plan Autonómico de Investigación, Desarrollo y Transferencia de Conocimientos. Gobierno de Aragón.
- III Plan Riojano de I+D+i. 2008-2011. Gobierno de la Rioja.
- Information Technology Service Management Forum (<http://www.itsmf.es/>).
- Informe anual 2012. Centro para el Desarrollo Tecnológico Industrial (CDTI).
- Informe SISE 2010. Análisis de las convocatorias del Plan Nacional 2008-2011 correspondientes al año 2010. Ministerio de Ciencia e Innovación.
- Instituto Nacional de Ciberseguridad (<http://www.incibe.es/>).
- Interactive energy Roadmap (<https://www.controlsystemsroadmap.net/>).
- Interpol (<http://www.interpol.int/>).
- INTERPOL World (<http://www.interpol-world.com/>).
- ISMS Forum Spain (<https://www.ismsforum.es/>).
- IV Plan Regional de Investigación Científica e Innovación Tecnológica 2005-2008. Comunidad de Madrid.
- La ciberseguridad en la Unión Europea. 2014. Henning Wegener-Instituto Español de Estudios Estratégicos.
- La nueva Ley de la Ciencia, la Tecnología y la Innovación. Aspectos relativos a la propiedad industrial e intelectual. Gonçalves Pereira. Cuatrecasas.
- Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) (<http://www.emad.mde.es/CIBERDEFENSA/>).

- Mapa de ruta de la Ciberseguridad Industrial en España 2013–2018. 2013. Centro de Ciberseguridad Industrial (CCI).
- Ministerio de Defensa (<http://www.defensa.gob.es/>).
- Ministerio de Economía y Competitividad (<http://www.mineco.gob.es/portal/site/mineco/>).
- Ministerio de Hacienda (<http://www.minhap.gob.es/es-ES/Paginas/Home.aspx>).
- Ministerio de Industria (<http://www.minetur.gob.es/es-ES/Paginas/index.aspx>).
- Ministerio de Interior (<http://www.interior.gob.es/>).
- Ministerio de Presidencia (<http://www.mpr.gob.es/Paginas/index.aspx>).
- MSP on ICT standardization (<https://ec.europa.eu/digital-agenda/en/european-multi-stakeholder-platform-ict-standardisation>).
- Network and information Security Public-Private Platform (<http://www.enisa.europa.eu/>).
- Organización de Naciones Unidas (ONU) (<http://www.un.org/es/>).
- Organización del Tratado del Atlántico Norte (OTAN) (<http://www.nato.int/>).
- Organización para la Cooperación y el Desarrollo Económico (OCDE) (<http://www.oecd.org/centrodemexico/inicio/>).
- Organización para la Seguridad y la cooperación en Europa (OSCE) (<http://www.osce.org/>).
- Parlamento Europeo (<http://www.europarl.es/>).
- Plan Andaluz de Investigación, Desarrollo e Innovación 2007-2013. Junta de Andalucía.
- Plan Avanza 2 Ministerio de Industria, Turismo y Comercio; Secretaría de Estado de Telecomunicaciones y Sociedad de la Información.
- Plan de actuación 2013 del Plan Estatal de Investigación Científica, Técnica y de Innovación. 2013–2016.
- Plan de Ciencia Tecnología e Innovación 2013-2017. Septiembre de 2013. Principado de Asturias.
- Plan de Ciencia, Tecnología e Innovación 2009-2012. Illes Balears.
- Plan de Ciencia, Tecnología e Innovación. 2011-2014. 2011. Región de Murcia.
- Plan de Confianza en el Ámbito Digital. 2013. Ministerio de Industria, Energía y Turismo.
- Plan de Desarrollo e Innovación del Sector TIC. 2013. Ministerio de Industria, Energía y Turismo.
- Plan de Innovación de 2014 – 2016. Cantabria.
- Plan de Internacionalización de Empresas Tecnológicas. Junio 2013. Ministerio de Industria, Energía y Turismo.
- Plan de Investigación e Innovación 2010-2013. Generalitat de Catalunya.
- Plan Estatal de Investigación Científica, Técnica y de Innovación. 2013–2016. Ministerio de Economía y competitividad.
- Plan Galego de Investigación, Innovación e Crecemento 2011-2015. Xunta de Galicia.
- Plan General Estratégico de Ciencia y Tecnología 2010-2015. Generalitat Valenciana.

- Plan Regional de Investigación Científica: Desarrollo Tecnológico e Innovación 2011-2015. Castilla - La Mancha.
- Plataforma Tecnológica Española de Seguridad Industrial (<http://www.pesi-seguridadindustrial.org/>).
- Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza (<http://esec.imasdtic.es/>).
- Proyecto Fire (<http://www.trustworthyictonfire.com/>).
- Proyecto Forward (<http://www.ict-forward.eu/>).
- Red Temática de Criptografía y Seguridad de la Información (<http://www.criptored.upm.es/criptored.htm>).
- Servicio Europeo de Acción Exterior (EEAS) (<http://www.eeas.europa.eu/>).
- Syssec Network of Excellence (www.syssec-project.eu/).
- The 2013 (ISC), Global Information Security Workforce Study. Frost & Sullivan.
- The National Energy Sector Cybersecurity Organization (<http://www.energysec.org/>).
- The Networking and Information Technology Research and Development Program (<https://www.nitrd.gov/>).
- Trust In Digital Life (<http://www.trustindigitallife.eu/>).
- V Plan Regional de Investigación, Desarrollo Tecnológico e Innovación 2014 – 2017. Gobierno de Extremadura.

ANEXO IV AGENTES DEL ECOSISTEMA DE I+D+I EN CIBERSEGURIDAD EN ESPAÑA

Este anexo muestra un listado de agentes del ecosistema español identificados en el transcurso del presente estudio y que completa el apartado del documento [3.1 Mapa de Agentes].

Administraciones Públicas
Organismos militares
Ministerio de Defensa: Centro de Inteligencia de las Fuerzas Armadas (CIFAS)
Ministerio de Defensa: Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD)
Organismos civiles
Consejo de Seguridad Nacional: Comité Especializado de Seguridad Marítima
Consejo de Seguridad Nacional: Comité Especializado de Situación
Ministerio de Economía y Competitividad: Centro para el Desarrollo Tecnológico Industrial (CDTI)
Ministerio de Hacienda y AAPP
Ministerio de Industria, Energía y Turismo: ENISA
Ministerio de Industria, Energía y Turismo: Instituto Nacional de Ciberseguridad (INCIBE)
Ministerio de Justicia: Agencia Española de Protección de Datos (AEPD)
Ministerio de Presidencia. Centro Nacional de Inteligencia (CNI): Centro Criptológico Nacional (CCN)
Ministerio del Interior: Centro Nacional de Protección de Infraestructuras Críticas (CNPIC)
Ministerio del Interior: Fuerzas y Cuerpos de Seguridad del Estado
Otros organismos autonómicos: Agencias de Protección de Datos Autonómicas (Madrid, Cataluña y País Vasco)
Otros organismos autonómicos: Consejerías y Agencias con competencias en materia de I+D+i
Otros organismos autonómicos: Fuerzas y Cuerpos de Seguridad Autonómicos
Sector académico
42 universidades (Universidades censadas por el Ministerio de Educación, Cultura y Deporte que trabajan en disciplinas relacionadas con la ciberseguridad)

Grupos de investigación	Organismo / Institución
• Grupo de investigación en Criptografía y Seguridad de la Información (GiCSI)	Consejo Superior de Investigaciones Científicas
• Grupo de Integración de Redes y Servicios	Escola Universitària Politècnica de Mataró
• Grupo de Ingeniería de Servicios Telemáticos • Grupo de Heurísticos Modernos de Optimización y Diseño de Redes de Comunicaciones • Grupo de Ingeniería Electrónica aplicada a Espacios Inteligentes y Transporte • Information Engineering Research Unit	Universidad Alcalá
• Grupo del Departamento de Electrónica y Sistemas	Universidad Alfonso X El Sabio
• High Performance Computing and Networking • Digital System Lab	Universidad Autónoma de Madrid
• Grupo de Seguridad de las Tecnologías de la Información y de las Comunicaciones • SoftLab • Redes y Servicios de Comunicaciones • Grupo Universitario de Tecnologías de Identificación	Universidad Carlos III de Madrid
• Grupo de Análisis, Seguridad y Sistemas • Diseño y Análisis Formal de Sistemas de Software	Universidad Complutense de Madrid
• Grupo de Criptología y Seguridad Computacional • Grupo de Redes y Middleware • Informática Industrial y Redes de Computadores	Universidad de Alicante
• Grupo de Informática Aplicada	Universidad de Almería
• Informática de Gestión • Laboratorio de Comunicaciones Móviles y Diseño de Redes	Universidad de Cantabria
• Grupo Alarcos • Arquitectura y Redes de Computadores • Grupo de Investigación de Seguridad y Auditoría de Sistemas de Información • Redes y Arquitecturas de Altas Prestaciones	Universidad de Castilla la Mancha
• Prinia (Proyectos de Ingeniería Informática y Automática)	Universidad de Córdoba
• Grupo de arquitectura de computadores y diseño lógico • Grupo de investigación de Ingeniería Telemática Aplicada y Comunicaciones Avanzadas	Universidad de Extremadura
• Telemática y Comunicaciones	Universidad de Granada
• Grupo de Criptología	Universidad de la Laguna
• Grupo de Ingeniería de Sistemas y Automática	Universidad de la Rioja
• Sistemas de información y comunicaciones	Universidad de las Palmas de Gran Canaria
• Organización y Uso de contenidos digitales • Supervisión, Control y Automatización de Procesos Industriales • Sistemas inteligentes de Gestión • Ingeniería del Conocimiento • Sistemas de Información Flexibles • Robótica	Universidad de León

Grupos de investigación	Organismo / Institución
<ul style="list-style-type: none"> Visión Artificial y Reconocimiento de Patrones Ingeniería de los Procesos de Fabricación Sistemas Avanzados de Información 	
<ul style="list-style-type: none"> Grupo de Ingeniería del Software Grupo de Aplicación de las Tecnologías de la Información y Comunicaciones 	Universidad de Málaga
<ul style="list-style-type: none"> Grupo de Telemática Teoría de la Señal y Comunicaciones 	Universidad de Mondragón
<ul style="list-style-type: none"> Arquitectura y Computación Paralela Sistemas Inteligentes y Telemática Sistemas de Información y Comunicación 	Universidad de Murcia
<ul style="list-style-type: none"> Centro de Innovación Grupo de Sistemas de Distribución Multimedia Grupo de Álgebra, Codificación y Criptografía Grupo de Teoría de la Señal y Comunicaciones Grupo de Comunicaciones e Ingeniería del Software Grupo de Ingeniería Web Grupo de Servicios, Nuevas Tecnologías y Desarrollo Regional Grupo de Técnicas Estadístico-Económicas de Modelización Económica Asociación Temática de Investigación de Telecomunicaciones Criptografía, Seguridad Informática y Auditoría de los Sistemas de Información Instituto Universitario de Tecnología Industrial de Asturias 	Universidad de Oviedo
<ul style="list-style-type: none"> Grupo de Biomedicina, Sistemas Informáticos Inteligentes y Tecnología Educativa Criptografía, Seguridad de la Información y Matemática Discreta 	Universidad de Salamanca
Grupo QUIVIR	Universidad de Sevilla
Equipo de Lenguajes, Sistemas Informáticos y Enseñanza Asistida por Computador	Universidad de Vigo
<ul style="list-style-type: none"> Grupo de Tecnología de las Comunicaciones. Grupo de Visión por Computador y Redes Neuronales Grupo de Ingeniería de Sistemas de Eventos Discretos Robotics, Perception and Real Time Group Group of Distributed Information Systems 	Universidad de Zaragoza
<ul style="list-style-type: none"> Grupo NQAS Grupo I2T Redes de Computadores Grupo de Investigación en Electrónica Aplicada 	Universidad del País Vasco / Euskal Herriko Unibertsitatea
<ul style="list-style-type: none"> DEUSTEK2 D4K - Deusto for Knowledge 	Universidad Deusto
Grupo de investigación en Sistemas Inteligentes	Universidad Europea de Madrid
Estructura de Sistemas y Tecnologías de Comunicaciones Móviles e Inalámbricas	Universidad Miguel Hernández de Elche
Ingeniería de Software y Sistemas	Universidad Nacional de Educación a distancia
<ul style="list-style-type: none"> Ánalysis y Desarrollo de Sistemas de Energía Eléctrica División de Sistemas e Ingeniería Electrónica Ingeniería Telemática 	Universidad Politécnica de Cartagena

Grupos de investigación	Organismo / Institución
<ul style="list-style-type: none"> • Grupo de Sistemas Telemáticos para la Sociedad de la Información y el Conocimiento • Grupo de laboratorio de Criptología • Grupo de Redes y Servicios de Telecomunicación e Internet • Grupo del laboratorio de Sistemas Integrados • Grupo de Investigación en Tecnología Informática y de las Comunicaciones • Internet de Nueva Generación • Seguridad y Mejora de Procesos • Automatización en Señal y Comunicaciones • Internet de Nueva Generación • Redes y Servicios de Telecomunicación e Internet • Grupo de Microondas • Grupo de Privacidad y Seguridad en Sistemas de Información 	Universidad Politécnica de Madrid
<ul style="list-style-type: none"> • Sistemas Informáticos 	Universidad Pontificia de Comillas
<ul style="list-style-type: none"> • Grupo de Redes, Sistemas y Servicios Telemáticos 	Universidad Pública de Navarra
<ul style="list-style-type: none"> • Grupo del Departamento de Ingeniería de la Información y de las Comunicaciones 	Universitat Autònoma de Barcelona
<ul style="list-style-type: none"> • Comunicacions i Sistemes Distribuïts 	Universitat de Girona
<ul style="list-style-type: none"> • Ingeniería Telemática • Grupo de Mejora de Procesos de Software • Seguridad y Comercio Electrónico 	Universitat de les Illes Balears
<ul style="list-style-type: none"> • Criptografia i Grafs 	Universitat de Lleida
<ul style="list-style-type: none"> • K-ryptography and Information Security for Open Networks • Privacy and IP Protection 	Universitat Oberta de Catalunya
<ul style="list-style-type: none"> • Grupo de Seguridad en red • Redes de Computadores y Sistemas Distribuidos • Matemática Aplicada a la Criptografía • Servicios Telemáticos 	Universitat Politécnica de Catalunya
<ul style="list-style-type: none"> • Grupo de Redes de Computadores • INGENIO 	Universitat Politècnica de Valencia
<ul style="list-style-type: none"> • Wireless Communications • Grupo de Investigación en Tecnologías y Estrategias de las Telecomunicaciones • Grupo de Investigación en Redes y Comunicaciones 	Universitat Pompeu Fabra
<ul style="list-style-type: none"> • Grupo CRISES 	Universitat Rovira i Virgili

Centros de Investigación
Centro de Investigación para la Gestión Tecnológica del Riesgo (CIGTR)
Centro de Investigación Vicomtech-IK4
Centro de Investigación: Tecnalia
Consejo Superior de Investigaciones Científicas (CSIC)

Organismos de soporte a la I+D+i

Centros tecnológicos: Gradiant

Oficinas de transferencia de resultados de la investigación (OTRI). Se ha inventariado una oficina en cada una de las 42 universidades identificadas como universidades relacionadas con la ciberseguridad. A éstas se añade la OTRI del Consejo Superior de Investigaciones Científicas (CSIC)

Industria**Asociaciones empresariales**

AEI Ciberseguridad

Agrupaciones Empresariales Innovadoras (AEI)

Asociación Española de Empresas Tecnológicas de Defensa, Aeronáutica y Espacio (TEDAE)

Asociación Nacional de Ciberseguridad y Pericia Tecnológica (ANCITE)

Asociación para la Protección de las Infraestructuras Críticas (APIC)

Asociación Vasca de Privacidad y Seguridad de la Información (Pribatua)

Confederación Española de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica (Conectic)

No cON Name

Organismos certificadores

European Committee for Electrotechnical Standardization (CENELEC)

European Committee for Standardization (CEN)

European Telecommunications Standards Institute (ETSI)

Anexo V REDES COLABORATIVAS ANALIZADAS

Este apartado ofrece un listado de las redes colaborativas analizadas en el presente estudio:

- Redes colaborativas **nacionales**
 - Plataforma tecnológica española de tecnologías para seguridad y confianza (esec-ametic)
 - Plataforma Tecnológica Española de Seguridad Industrial (PESI)
 - Centro de Ciberseguridad Industrial (CCI)
 - ISMS Forum Spain
 - Red temática de criptografía y seguridad de la información (Criptored)
 - Information Technology Service Management Forum (itSMF Forum)
- Redes colaborativas **Europeas**
 - SysSec Network of Excellence
 - European Public Private Partnership for Resilience
 - Cybercrime Centres of Excellence Network for Training Research and Education
 - Trust in Digital Life
 - European Network for Cybersecurity
- Redes colaborativas **internacionales**
 - The Networking and Information Technology Research and Development Program (NITRD)
 - The National Energy Sector Cybersecurity Organization (EnergySec)
 - Interactivity energy Roadmap (ieRoadmap)
 - The Open Web Application Security Project (OWASP)