INFORME DE CONCLUSIONES DE LA CONSULTA PRELIMINAR AL MERCADO PARA LA DEFINICIÓN DE ACTUACIONES DE IMPULSO DE LA CIBERSEGURIDAD DE INCIBE CORRESPONDIENTE A LA ACTUACIÓN 1 ‘PROGRAMAS DE I+D’

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El Instituto Nacional de Ciberseguridad (en adelante, INCIBE), sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, convocó en el mes de julio de 2021 una **Consulta Preliminar del Mercado** para la búsqueda de soluciones innovadoras relativas al desarrollo de tecnología en el ámbito de la ciberseguridad.

Esta consulta se enmarca en el impulso del INCIBE a la **Compra Pública de Innovación (CPI)** como instrumento para la ejecución de actuaciones y proyectos que logren acelerar el proceso de digitalización de las empresas españolas en todo lo relativo a la ciberseguridad, así como al desarrollo de una industria nacional competitiva en este campo.

Como resultado del proceso de Consulta Preliminar al Mercado se ha elaborado este **informe de conclusiones** de la misma en lo referente a la preparación de la potencial licitación de **Compra Pública Pre-comercial de Programas de I+D en el ámbito de la Ciberseguridad**. Se expone a continuación el desarrollo del proceso y sus conclusiones.

2. MARCO JURÍDICO

La **Directiva 2014/24/UE del Parlamento Europeo y del Consejo del 26 de febrero de 2014** sobre contratación pública recoge formalmente en su artículo 40, por primera vez, las **Consultas Preliminares al Mercado**, dentro de la sección relativa a la fase de preparación del contrato.

La **ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP)**, regula en su artículo 115 las **Consultas Preliminares al Mercado**. Pese a que las licitaciones de contratación pre-comercial están excluidas de la Ley 9/2017 de 8 de noviembre, de Contratos del Sector Público en virtud de su artículo 8, la realización de **Consultas Preliminares al Mercado** en las fases preparatorias del contrato se considera una buena práctica y son altamente recomendables. Esta herramienta de retroalimentación informativa entre las autoridades contratantes y el mercado debe formar parte del expediente de contratación, debe cumplir con los principios básicos inspiradores de la Directiva 2014/24/UE y la Ley 9/2017, es decir, deben garantizar la confidencialidad, la igualdad de trato y la libre competencia; y no es vinculante para ninguna de las partes.

3. CONSULTA PRELIMINAR AL MERCADO (CPM)

El 1 de julio de 2021 se puso en marcha el proceso de **Consulta Preliminar al Mercado (CPM)**, de acuerdo con lo establecido en el artículo 115 de la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público. El anuncio de la convocatoria fue publicado dicho día y difundido, a efectos de no distorsionar la competencia, en el Perfil del Contratante del Instituto Nacional de Ciberseguridad (INCIBE), en donde se incluían los siguientes aspectos:

- El objeto de la convocatoria.
- El órgano de contratación.
- Fecha de inicio, fecha de fin, fecha de publicación y estado.
- Las condiciones de presentación de las propuestas.
- La aplicación de los principios de transparencia, igualdad de trato y no discriminación ni falseamiento de la competencia.
- Plazo y actualizaciones de la Consulta Preliminar al Mercado.

Todo lo anterior se lleva a cabo a efectos de que puedan tener acceso y posibilidad de realizar aportaciones todos los posibles interesados, en cumplimiento de lo previsto en el artículo 115 de Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

INCIBE, con el fin de garantizar la transparencia del procedimiento y participación de las empresas, creó un apartado en el portal web de INCIBE específico del proyecto de Compra Pública de Innovación donde se ha publicado toda la documentación relativa a la **Iniciativa Estratégica de Compra Pública de Innovación (IECPI)**, incluyendo videos, presentaciones, preguntas frecuentes, etc.

A continuación se detalla el cronograma de actividades en torno a la CPM:

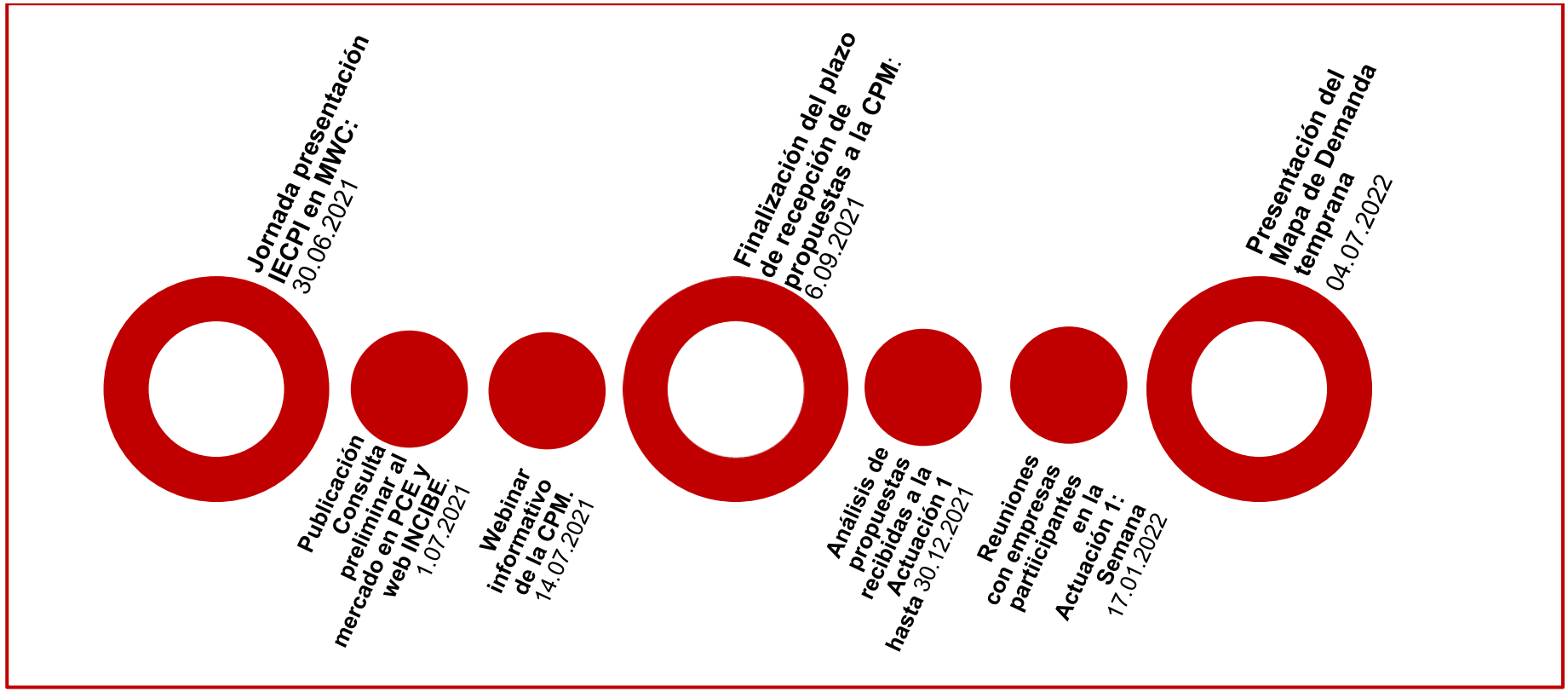

Ilustración 1: Cronograma de acciones de la Consulta Preliminar al Mercado.

3.1. Jornada de presentación de la Iniciativa Estratégica de la CPI (IECPI) de INCIBE en ciberseguridad

La ciberseguridad fue protagonista del ***Mobile World Congress*** **(MWC)** de Barcelona en junio del 2021, esta vez no solo por las novedades tecnológicas, sino también por el impulso que el Gobierno de España ha decidido dar al sector de la ciberseguridad como uno de los sectores protagonistas de la recuperación, transformación y resiliencia del país tras la pandemia del COVID-19.

El MWC fue el marco elegido por la **Secretaría de Estado de Digitalización e Inteligencia Artificial**, para presentar públicamente una inversión sin precedentes en la industria de la ciberseguridad. A lo largo de los próximos tres años, el Instituto Nacional de Ciberseguridad, dependiente de dicha Secretaría de Estado, canalizará al mercado 224 millones de euros mediante contratos de Compra Pública de Innovación.

Con esta inversión, la Secretaría de Estado de Digitalización e Inteligencia Artificial y el INCIBE pretenden transformar la ciberseguridad en el conjunto del sector público, en las PYMES y en sectores estratégicos como el transporte, la energía, las infraestructuras y otros; fomentando la creación de soluciones diversas en todos estos ámbitos y su incorporación en entornos reales por Administraciones Públicas y empresas.

Junto a ello, el uso de la **Compra Pública de Innovación** como instrumento para la ejecución de estas actuaciones, permitirá a INCIBE desarrollar una política industrial y de innovación claramente enfocada a fortalecer las capacidades y la competitividad de la industria española, que creará productos y soluciones basadas en tecnologías disruptivas y altamente competitivas dentro y fuera de España.

Para ello, INCIBE ha decido impulsar, al menos, siete tipos diferentes de actuaciones:

- Actuación 1: Programas de I+D estratégicos para el desarrollo de proyectos de tecnologías disruptivas por empresas de la industria de la ciberseguridad, que den respuesta a retos a largo plazo.
- Actuación 2: Contratación de soluciones tecnológicas para impulsar la ciberseguridad en las PYMEs.
- Actuación 3: Contratación de soluciones tecnológicas para impulsar la ciberseguridad en sectores estratégicos de la *Network and Information Security* (NIS2).
- Actuación 4: Contratación de soluciones tecnológicas para los retos de ciberseguridad del sector público.
- Actuación 5: Contratación de productos y soluciones para la creación de infraestructuras estratégicas de ciberseguridad y la mejora del equipamiento del propio INCIBE.
- Actuación 6: Soluciones tecnológicas vinculadas a la formación o al desarrollo de capacidades y de habilidades de las personas.
- Actuación 7: Compra pública de innovación de pequeños proyectos impulsados por empresas de nueva creación, micropymes y PYMES.

Para llegar a la definición concreta de los contratos que serán objeto de licitación, INCIBE anuncia la realización de una **Consulta Preliminar al Mercado**, que fue publicada el 1 de julio y estuvo abierta a la presentación de proyectos por las empresas y otros operadores económicos hasta el día 13 de agosto. Este plazo fue ampliado hasta el 6 de septiembre posteriormente.

Tras el análisis de las propuestas presentadas, INCIBE presentará el listado de contratos, conocido como **Mapa de Demanda Temprana**.

Esta inversión situará a INCIBE como uno de los principales protagonistas de la compra pública de innovación en España y a la ciberseguridad como un sector puntero en el uso de instrumentos de fomento de la industria mediante la demanda pública.

La jornada de presentación de esta **Iniciativa Estratégica de la Compra Pública de Innovación** en ciberseguridad se realizó de forma presencial y por *streaming.*

Se presentó y discutió la iniciativa por un panel representado por:

- Lola Rebollo, Subdirectora de I+D+I e impulso a la industria de INCIBE.
- Santiago Soley, CEO de PILDOLABS.
- Ana Ayerbe, representante de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC).
- Jose Ignacio Cases, Novadays S.L., como moderador.

Los objetivos de este panel fueron:

1. Reforzar la presentación de las actuaciones de CPI de INCIBE con una conversación entorno a la ciberseguridad y a los instrumentos que existen para impulsarla desde el sector público.
2. Compartir experiencias entre la AA.PP y empresa privada.

El panel finalizó con una intervención individual de **Carme Artigas, Secretaria de Estado para la Digitalización e Inteligencia Artificial** que enmarcó esta iniciativa entre las inversiones previstas por el **Plan de Recuperación, Transformación y Resiliencia "España Puede"**.

Se puede acceder a esta jornada de presentación de la IECPI en la página web de INCIBE. En la misma página se presentan los pasos previos realizados por INCIBE y la fecha de publicación de la **Consulta Preliminar al Mercado** para la definición de actuaciones de impulso de la ciberseguridad y la elaboración del **Mapa de Demanda Temprana**.

Posteriormente, la convocatoria para la consulta se publica en:

- La Plataforma de Contratación del Sector Público (PLACSP).
- La web de INCIBE.

De igual forma, se realiza difusión de la Iniciativa y de la Consulta Preliminar al Mercado a través de las redes sociales de INCIBE y con la publicación de notas de prensa en medios especializados en Tecnologías de la Información y Comunicación (TIC), y ciberseguridad en junio y julio del 2021. A continuación se recogen algunas de estas publicaciones.

Publicación de la Consulta Preliminar al Mercado (CPM) en redes sociales de INCIBE:

Ilustración 2: Publicación de la CPM.

Revista SIC:

Ciberseguridad: De ideación estratégica a ejecución real de las colaboraciones público-privadas para impulsar a la industria y a la innovación nacional: https://revistasic.es/revista-sic/sic-146/colaboraciones/inversiones/

Red Seguridad:

INCIBE anuncia la mayor compra pública innovadora en ciberseguridad: 224 millones de euros:

https://www.redseguridad.com/actualidad/organismos-ciberseguridad/incibe-anuncia-la-mayor-compra-publica-innovadora-de-europa-en-ciberseguridad-224-millones-de-euros_20210702.html

CINCO DÍAS:

El Gobierno invertirá 224 millones de euros en compra pública en ciberseguridad a través del INCIBE:

https://cincodias.elpais.com/cincodias/2021/06/29/companias/1624959552_804284.html

IT Digital Security:

INCIBE invertirá 224 millones de euros en compra pública innovadora en ciberseguridad:

https://www.itdigitalsecurity.es/actualidad/2021/07/incibe-invertira-224-millones-en-compra-publica-innovadora-en-ciberseguridad

3.2. Publicación de la Consulta Preliminar al Mercado (CPM)

Toda la información relacionada con la **Consulta Preliminar al Mercado** se publica el día 1 de julio de 2021 en la web de INCIBE en el apartado dedicado a la CPI y en la Plataforma de Contratación del Estado. Los documentos que se incluyen en la publicación son:

- Consulta Pública al Mercado y Anexos de las actuaciones.
- Ficha básica de participación en la Consulta Pública al Mercado.

Este informe de conclusiones se centra en la cuestión relativa al interés y propuestas sobre la Actuación 1 denominada: **Programas de I+D estratégicos para el desarrollo de proyectos de tecnologías disruptivas por empresas de la industria de la ciberseguridad, que den respuesta a retos a largo plazo**.

Estos Programas de I+D, tal y como se describía en la propia consulta (página 9 del documento de la Consulta Pública al Mercado) tiene como objeto:

Programas de I+D con empresas de la industria de la ciberseguridad, cuyo objeto sea el desarrollo de un conjunto de proyectos de I+D estratégicos para la empresa promotora, siendo esta una empresa creadora y comercializadora de tecnologías de la ciberseguridad. Estos programas deberán ser susceptibles de desarrollo en un plazo de dos años. Los proyectos deberán partir desde TRLs bajos (4-5) y no superar el TRL8. Deberán tener el liderazgo de una empresa tractora con una clara capacidad de comercialización industrial; y una significativa participación de PYMES y centros de conocimiento como subcontratistas de la misma. Deberán dar respuesta a retos de ciberseguridad de entidades públicas, PYMES o sectores estratégicos, a largo plazo.

Las cuestiones concretas que se formulaban se recogían en una 'Ficha básica para la presentación de propuestas', siendo estas:

- Datos básicos de la propuesta: denominación, entidad líder, entidades participantes, nombre y datos de la persona representante.
- Datos de clasificación de la entidad líder y de otros miembros del consorcio: tipo de entidad, sector de actividad, facturación de los últimos tres años (tanto total como en materia de ciberseguridad) e inversión de los últimos tres años en I+D.
- Roles en los que participa cada entidad, atendiendo a los seis roles definidos por INCIBE.
- Tipo de actuación en la que se clasifica la propuesta, entre las siete actuaciones definidas por INCIBE.
- Clasificación de la propuesta en los retos tecnológicos definidos por INCIBE.
- Valoración económica de la propuesta.

Además de esta ficha básica, se solicitó una descripción detallada de cada propuesta en la forma de una memoria descriptiva, con una extensión máxima de 20 hojas, que debía atender a lo solicitado para cada tipo de actuación.

En el caso de la actuación 'Programas de I+D', la información que se solicitó como contenido de estas memorias por proyecto (página 22 del documento de la CPM), fue:

1. Contenido del Programa de I+D propuesto: proyectos, tecnologías y resultados (incluyendo productos y soluciones, TRLs de partida y de llegada).
2. Alineación del Programa con la estrategia, mercados y clientes presentes y futuros de la empresa. Capacidad de comercialización futura.

3. Retos de la AA.PP. o de sectores estratégicos a los que darían respuesta los productos y soluciones que son objeto del Programa. Entidades participantes o asociadas como posibles usuarias futuras.
4. Efectos e impactos del Programa. Subcontratación de PYMES, Universidades, Organismos de Investigación y Centros Tecnológicos.
5. Descripción económica del Programa. Volumen de inversión total. Contribución pública solicitada. Programación presupuestaria anual.

En las páginas 11, 12, 13 y 14 del documento de la Consulta Preliminar al Mercado se incluye el apartado 4.5. Retos tecnológicos. En él se identifican los principales retos tecnológicos que, sin carácter exhaustivo y sin que su enumeración suponga ningún límite, pueden utilizar los operadores para la presentación de las propuestas.

3.3. Jornada divulgativa de la Consulta Preliminar al Mercado

INCIBE organizó el 15 de julio de 2021 un *webinar* para presentar los puntos principales de la **Consulta Preliminar al Mercado** y resolver todas las dudas que pudieran surgir dentro de las actuaciones de **Compra Pública de Innovación**.

Ilustración 3: Imagen de la invitación al Webinar

La agenda de este *webinar* fue la siguiente:

Ilustración 4: Agenda de la Presentación realizada en el Webinar

Se registraron **545 personas** pertenecientes a distintas entidades y asistieron **413 personas**. Se atendieron las consultas recibidas durante la jornada y posteriormente de forma individual y a través de la publicación del Documento de Preguntas Frecuentes. Este documento fue publicado en la Plataforma de Contratación del Sector Público (PLACSP) y en la web de INCIBE. El vídeo y la presentación se publicaron en la web de INCIBE.

3.4. Finalización de la Consulta Preliminar al Mercado (CPM)

Inicialmente, la fecha de finalización de la convocatoria era el 13 de agosto del 2021, pero se extendió hasta el 6 de septiembre del 2021 atendiendo a las solicitudes recibidas de ampliación del plazo por los operadores económicos interesados en participar en la consulta.

La **Consulta Preliminar al Mercado** fue de carácter abierto, dirigiéndose por tanto a todos los operadores económicos del ecosistema de ciberseguridad, así como a operadores de otros ámbitos o sectores que pudieran tener interés en alguna de las actuaciones impulsadas por INCIBE. En este sentido, no se limitó la participación de ningún actor ni por naturaleza jurídica, ni por tamaño, ni por ningún otro aspecto que pudiera diferenciar a unos operadores económicos de otros.

4. RESULTADO DE LA CPM PARA LA ACTUACIÓN 1: PROGRAMAS DE I+D CONJUNTOS

4.1. Respuestas a la consulta

Una vez finalizado el plazo de recepción de propuestas, se procedió a su análisis.

4.1.1. Datos obtenidos

En la siguiente tabla se listan las **18 entidades** que participaron en la Actuación 1 de Programas de I+D presentando un total de **26 propuestas**:

Nº	ENTIDAD LÍDER	NÚMERO DE PROPUESTAS
1	ABACUS CONSULTING TECHNOLOGIES S.L.	1
2	ACCENTURE S.L.U.	2
3	CIC CONSULTING INFORMÁTICO S.L.	1
4	CONSORCIO RED ALASTRIA	1
5	CORPORATE PROTECTIVE INTELLIGENCE S.L. ACCENTURE S.L.U.	1
6	DXC TECHNOLOGY SPAIN	2
7	GRADIANT	1
8	INDRA SISTEMAS S.A.	1
9	INNOTEC SYSTEM S.L.U.	3
10	INTEGRATED TECHNOLOGY SYSTEMS	2
11	IZERTIS	1
12	NAVANTIA S.A.	1
13	OPEN CLOUD FACTORY S.L.	1
14	S2 GRUPO DE INNOVACIÓN EN PROCESOS ORGANIZATIVOS S.L.U	1
15	SISTEMAS AVANZADOS DE TECNOLOGÍA, S.A. (SATEC)	1
16	TELEFÓNICA DE ESPAÑA, S.A.U.	4
17	VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.	1
18	313 ICAN FUTURA S.L.	1

Tabla 1: Entidades líderes participantes de la Actuación 1 - Programas de I+D Conjuntos

Las propuestas recibidas a la Actuación 1, Programas conjuntos de I+D, son lideradas por operadores económicos de diferente tamaño.

- Gran Empresa.
- PYME.
- Start-up.
- Centros Tecnológicos.
- Consorcios.

En el siguiente gráfico se presenta las categorías identificadas y número de propuestas recibidas:

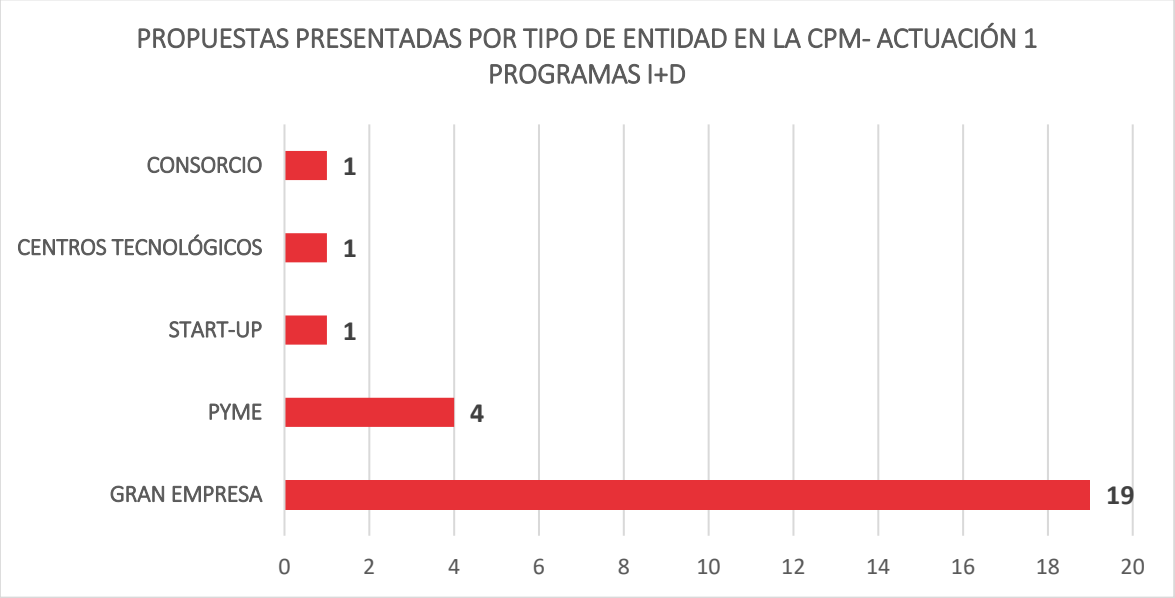

Ilustración 5: Propuestas presentadas por tipo de entidad

Asimismo, se han identificado **95 entidades** adicionales que participan en estos programas en algunas de las propuestas.

Para el cálculo de estos datos solamente se han tenido en cuenta las entidades que han sido identificadas en las fichas básicas de participación de las propuestas, si bien en las memorias descriptivas se identifican muchas más entidades como usuarios y fabricantes, tanto públicos como privados, interesados en participar en los programas de I+D propuestos.

A continuación, se muestra de forma resumida por Rol de Participación a la CPM, el número de entidades incluidas en esta actuación:

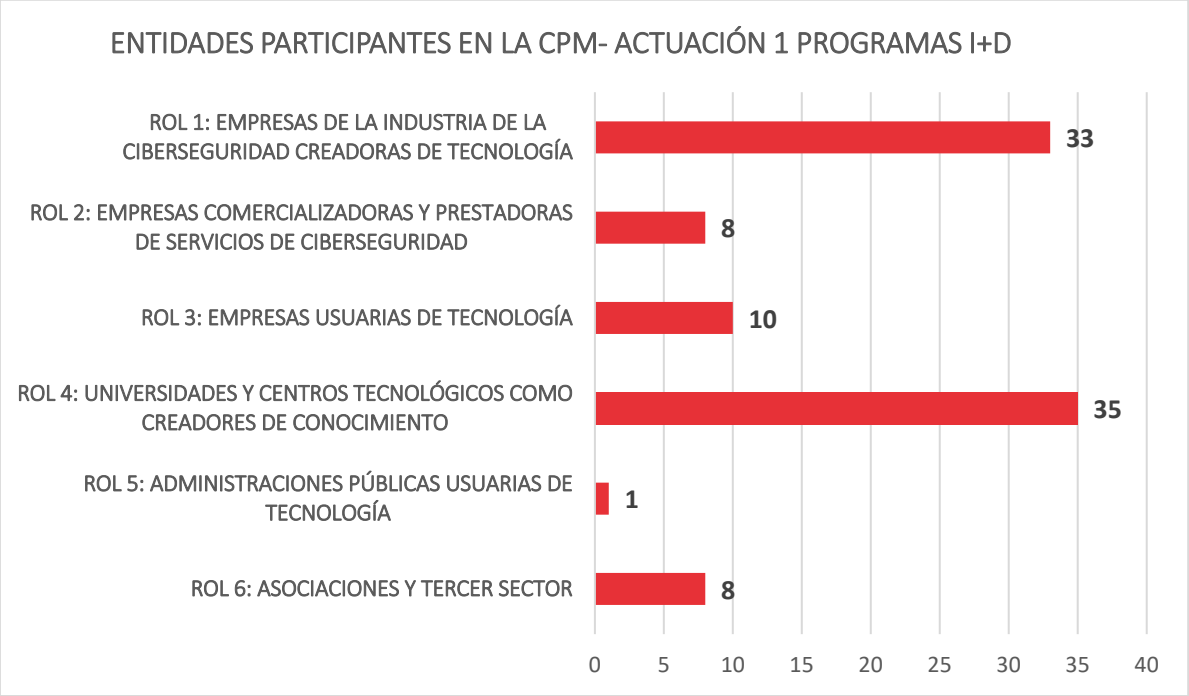

Ilustración 6: Resumen de operadores económicos y entidades por RoI

Destacar el alto grado de interés mostrado por las universidades y centros tecnológicos en esta Actuación.

Las propuestas presentadas han abordado uno o varios de los retos tecnológicos propuestos en la CPM. A continuación se presentan los datos agregados de los retos identificados en las propuestas:

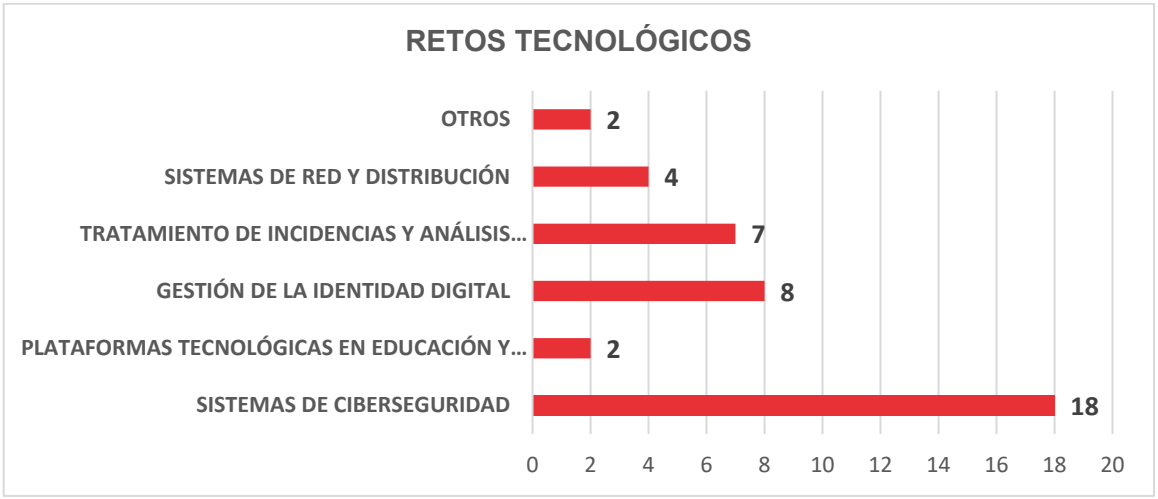

Ilustración 7: Retos tecnológicos identificados en las propuestas

4.1.2. Análisis de los datos

A continuación se expone un listado de conclusiones obtenidas del análisis de los datos.

De las 26 propuestas relativas a esta actuación, una parte muy mayoritaria son **propuestas provenientes de grandes empresas**, aunque también se detecta una alta participación de PYMES, Organismos de Investigación, Universidades o Centros Tecnológicos.

Estas propuestas suman una inversión total de **158.887.906,38 €**, y estiman una inversión pública de **122.093.383,91** € (0,30 € por cada euro público). Las empresas se muestran dispuestas a cofinanciar.

En cuanto al mayor o menor grado de innovación de los programas, es pertinente señalar que **existe suficiente número de programas innovadores como para validar el modelo de actuación** y que aquellos que hoy podrían parecer poco innovadores podrán modificarse sustancialmente durante el proceso de licitación.

Existen proyectos que tratan sobre las mismas temáticas, esto da lugar a que el mensaje sobre el tipo de proyectos que se solicita en la convocatoria ha sido correctamente trasladado.

Muchas propuestas abordan temáticas de Ciberseguridad desde puntos de vista de la Inteligencia Artificial, en particular el *Machine Learning*; computación cuántica y *blockchain*, principalmente poniendo foco en sectores específicos, como el de las tecnologías de la operación (OT, *Operation Technology*).

Un alto porcentaje de propuestas están en la línea de la automatización de tareas para minimizar curvas de aprendizaje, descargar a técnicos de tareas recurrentes y posibilitar el fácil acceso a herramientas potentes, pero a la vez sencillas.

4.2. Entrevistas realizadas

Entre los días 18 y 20 de enero de 2022, se celebraron reuniones entre INCIBE y algunos de los operadores económicos que han presentado propuestas dentro de la Actuación 1. El objetivo de las reuniones fue aclarar y contrastar aspectos de las propuestas presentadas a esta actuación. Las entrevistas se realizaron en sesiones individuales de 55 minutos de duración y con el siguiente el orden del día:

1. Presentación de la actuación por parte de INCIBE (15’).
2. Visión y alineación estratégica de la empresa respecto a la actuación (15’).
   a. Líneas tecnológicas propuestas.
   b. Cofinanciación y participación de PYMES y centros.
   c. Productos y resultados esperados.
3. Discusión abierta (25’).

Las entidades entrevistadas fueron las siguientes:

Nº	OPERADOR ECONÓMICO	FECHA DE ENTREVISTA
1	ACCENTURE S.L. UNIPERSONAL	18/01/2022
2	INDRA SISTEMAS S.A.	18/01/2022
3	OPEN CLOUD FACTORY, S.L.	18/01/2022
4	INNOTEC SYSTEM S.L.U.	18/01/2022
5	TELEFÓNICA DE ESPAÑA, S.A.U.	18/01/2022
6	IBERMÁTICA (INTEGRATED TECHNOLOGY SYSTEMS)	19/01/2022
7	GRADIANT	19/01/2022

Nº	OPERADOR ECONÓMICO	FECHA DE ENTREVISTA
8	S2 GRUPO DE INNOVACIÓN EN PROCESOS ORGANIZATIVOS S.L.U.	20/01/2022
9	NAVANTIA	20/01/2022

Tabla 2: Entrevistas realizadas- Actuación 1 Programas I+D

Como resultado de las reuniones, se extraen las siguientes conclusiones:

- En general se ha comprendido el planteamiento de los Programas Conjuntos de I+D, pero todavía hay entidades que no tenían del todo claro el objetivo de la actuación y por tanto, no se han ajustado completamente al modelo propuesto en la CPM, especialmente en lo relativo a la presentación de programas como un conjunto de proyectos (en lugar de un único proyecto), la necesidad de coinversión y sobre todo la exigencia de tracción al ecosistema, con la necesidad de conformar grandes consorcios. En este sentido se realizarán acciones específicas de comunicación dirigidas a difundir entre el ecosistema los aspectos clave de la licitación de Programas Conjuntos de I+D, los resultados y efectos perseguidos.
- En relación con el requisito de tracción al ecosistema y la composición de consorcios, algunas empresas no tienen identificado un ecosistema de ciberseguridad con intereses comunes o tienen dificultad para acceder a él. Por ello, se pondrán en marcha de acciones de *networking* que faciliten el contacto entre las diferentes entidades que conforman el ecosistema.
- Las entidades participantes han formulado sus propuestas basándose en los requisitos fijados en la CPM para la primera actuación, en concreto para la duración de los proyectos (24 meses). En general, coinciden en que un plazo más largo permitiría conseguir mayores resultados. Por tanto, la duración de los proyectos será de 2 a 3 años.
- Los proyectos que conforman los programas son muy heterogéneos en cuanto a la madurez tecnológica y los TRLs de partida y de llegada, aunque en cualquier caso hay que establecer un TRL mínimo de llegada de 7.
- Se prevé dotar de flexibilidad a los Programas a través de un sistema de gestión de cambios y con la posibilidad de la modificación de los contratos, incluyendo ambos aspectos en el pliego de la licitación.

4.3. Metodología utilizada

Se realizó un primer análisis de las propuestas llevado a cabo por un **Comité de Expertos en CPI y Ciberseguridad** a nivel interno de INCIBE. Para ello, se ha utilizado la siguiente metodología divida en dos fases:

1. Análisis individual de las propuestas:
    a. Verificar que es CPI.
    b. Verificar que responde al modelo planteado en cada actuación.
    c. Retos funcionales a los que da respuesta.

   d. Identificación de los usuarios públicos y privados de la solución propuesta.
   e. Presupuesto total.
   f. Cofinanciación privada.
   g. Grado de interés de la propuesta.
   h. Comentarios.
   i. Próximos pasos.

2. Análisis global de la actuación:
   a. Número de propuestas válidas a nivel de actuación.
   b. Retos públicos a los que da respuesta.
   c. Presupuesto total de las propuestas válidas.
   d. Cofinanciación privada de las propuestas válidas.
   e. Sectores usuarios.
   f. Demanda suficiente para licitar.
   g. Competencia suficiente para licitar.
   h. Modelo final de la actuación a licitar.
   i. Tipología de procedimiento.
   j. Retos a los que responde.
   k. Usuarios públicos.

Posteriormente, un equipo de asesores externos especialistas en Compra Pública de Innovación, la empresa Sidi Consultoria y Gestión, S.L., con la colaboración de especialistas en ciberseguridad de la Universidad de Deusto, ha evaluado esencialmente la idea del proyecto presentado y la componente de I+D de éste.

Este análisis se ha realizado con el fin de diseñar el primer **Mapa de Demanda Temprana de CPI en Ciberseguridad a nivel nacional** y el diseño de la estrategia de licitación, en este caso de la Actuación 1 Programas de I+D.

5. CONCLUSIONES

De acuerdo con la información recibida del mercado y como resultado de la Consulta Preliminar del Mercado, se identifica que existen retos en ciberseguridad en los públicos objetivos identificados en la Consulta (entidades públicas, PYMES o sectores estratégicos).

Estos retos se pueden cubrir mediante la adquisición de determinados servicios de I+D para alcanzar los objetivos propuestos por la Iniciativa Estratégica de Compra Pública de Innovación de INCIBE.

Por este motivo, se considera adecuado **iniciar un procedimiento de Compra Pública Precomercial para la ejecución de la Actuación 1**.

La licitación se realizará mediante un **procedimiento de adjudicación competitivo de diálogo** con las empresas, en varias fases, en las que INCIBE irá obteniendo el mayor valor en términos de resultados, efectos e impactos de la aportación pública que vaya a comprometer.

El objeto del contrato se centrará en la contratación de servicios de I+D, en la que comprador y contratista compartirán, riesgos y beneficios, especialmente en materia de Derechos de Propiedad Intelectual e Industrial.

Los servicios de I+D contratados se englobarán fundamentalmente entre los TRL 4-5 (como situación de partida) y TRL 7- 8 (como situación de llegada).

Los servicios de I+D contratados se agruparán en forma de proyectos individuales de I+D y deberán dar respuesta a los retos tecnológicos indicados en este documento (y las actualizaciones que pueda sufrir fruto del procedimiento competitivo de diálogo).

Se creará un **Catálogo de Soluciones Innovadoras**, que concretará estos retos tras la fase inicial del citado procedimiento competitivo de diálogo. Este Catálogo podrá actualizarse en fases sucesivas.

No se contempla en el presente procedimiento la adquisición de productos, servicios u obras innovadores resultantes de los resultados de los proyectos de I+D.

Los proyectos individuales de I+D se ejecutarán por fases y serán supervisados y controlados por INCIBE aplicando la metodología Stage-Gate®.

Es un objetivo de INCIBE que se compre un número suficiente de proyectos de I+D y que el desarrollo de cada una de las soluciones del Catálogo sea al menos cubierto por dos contratistas.

El contrato busca maximizar el impacto socio económico, tanto en el sector público como en el privado, de los servicios contratados. Es por ello por lo que el contratista asumirá el compromiso de destinar una parte de su inversión económica a Actividades Adicionales con ese fin.

De acuerdo con las propuestas presentadas por las empresas, se consideran de interés los Programas de I+D, atendiendo a:

Los **resultados (*outputs*) de la Actuación 1**, que son:

- Ejecución de un conjunto de proyectos de I+D (el programa) individuales, pero coherentes estratégicamente.
- Obtención de un número llamativo de productos en TRL 7 y 8 de cara a su futura comercialización.

- Movilización de coinversión privada, de manera que la empresa promotora e INCIBE compartan los riesgos del programa conjunto de I+D.

Los efectos e impactos esperados, que son:

- Mejora de la competitividad internacional de la industria española de la ciberseguridad, medida en la participación en programas internacionales de I+D y las ventas en el exterior.
- Tracción de Start-ups, pequeñas y medianas empresas y de universidades, organismos de investigación y centros tecnológicos por las grandes empresas industriales, desarrolladoras y comercializadoras de productos y soluciones.

La industria española de ciberseguridad necesita avanzar en el conocimiento de las tecnologías y la exploración de soluciones y productos que la posicionen a nivel global como una industria de referencia y al mismo tiempo, tratar de alcanzar la soberanía digital mediante la creación de soluciones propias que no dependan en exceso de terceros, logrando así una mayor independencia tecnológica y siguiendo por tanto las recomendaciones propuestas desde la Comisión Europea.

Por todo ello, INCIBE, como gestor de la iniciativa de impulso de la industria de la ciberseguridad a través de la Compra Pública de Innovación, plantea esta serie **de retos y necesidade**s que deberán ser cubiertos por los Programas Conjuntos de I+D:

Reto 1	**Gestión de identidades digitales**
Descripción de la necesidad:	La gestión y protección de la identidad digital, entendida como la traslación de la identidad física del ciudadano para la creación de otra virtual, unívocamente relacionada con la primera, y a través de la cual puedan prestársele servicios digitales seguros, se ha convertido en un elemento crítico, y en continua actualización. No en vano los principales fabricantes globales de tecnología se encuentran en este momento apostando por un cambio total de paradigma de identificación, mucho más centrado en la perspectiva del usuario, y al que no es razonable sustraerse. Por ello, se considera necesario que el tejido empresarial, adopte asimismo esta forma de operar con dichas identidades digitales, de tal forma que puedan continuar desarrollando su actividad normalmente, y al mismo tiempo ofrecer sus servicios con unos mayores grados de seguridad y usabilidad. Con este reto se pretende poner de manifiesto la importancia de asegurar la identidad digital en cualquier circunstancia, en particular de forma independiente de la localización, del dispositivo de acceso, de la calidad de las comunicaciones o de los posibles riesgos de las conexiones. Las propuestas dirigidas a cubrir este reto deberán plantear soluciones basadas en tecnologías novedosas, que consideren en profundidad tanto el estado de la praxis del sector, como el estado del arte en la materia, y que permitan con ello mejorar de forma sustancial el estado general de la seguridad en este ámbito

Reto 1	Gestión de identidades digitales
	de la identificación, asegurando mantener la reputación digital y su inviolabilidad, así como prevenir modificaciones subversivas, no deseadas, u otras acciones maliciosas relacionadas con las identidades digitales. En particular, las propuestas que encaren este reto deberán considerar adecuadamente el problema de la suplantación de identidad digital.

Reto 2	Criptografía
Descripción de la necesidad:	Dada la innegable importancia de los sistemas criptográficos en múltiples ámbitos de la seguridad, éstos vienen experimentando continuos y relevantes avances basados, por una parte, en el desarrollo exponencial de las capacidades de los sistemas de computación y, por otra parte, en nuevos conceptos relacionados con el avance de ciencias básicas, en particular de la computación cuántica. Mediante este reto, se pretende plantear la necesidad de incorporar los últimos avances y mejoras en sistemas de computación con el objetivo de verificar la estabilidad y robustez de los sistemas criptográficos, y también aportar mejoras al respecto en diferentes aplicaciones, tales como gestión de documentación, gestión de datos, comunicaciones, almacenamiento en la nube o gestión de identidades, entre otros. En particular, de entre todos los diferentes sistemas o paradigmas de computación, la tecnología cuántica se postula actualmente como la línea más prometedora y con mayor proyección en este campo, si bien este reto también tomará en consideración otras tecnologías que los licitantes pudieran plantear en sus propuestas. En concreto, son dos los retos específicos que plantea lo cuántico en materia de ciberseguridad: (a) el aseguramiento/validación de la robustez de los sistemas criptográficos pre-cuánticos y el planteamiento de propuestas post-cuánticas, y (b) el desarrollo de todo un nuevo paradigma de Ingeniería del Software Cuántico, considerado desde los primeros pasos de la Computación Cuántica, desde su diseño, y que sirva para evitar que ésta herede automáticamente todas las problemáticas de seguridad de código desarrolladas durante las últimas tres décadas por el mundo hacker. En todo caso, las propuestas que encaren este reto (como todos los demás) deberán mostrar un conocimiento en profundidad del estado del arte en materia de computación (convencional, paralela, FPGA, vectorial, cuántica, etc.), sobre el que construir nuevas aportaciones al área, y también prestar cercana atención a las referencias universalmente aceptadas en el sector.

Reto 3	Gestión de incidentes
Descripción de la necesidad:	El correcto, rápido y certero tratamiento de incidentes de ciberseguridad resulta un elemento crítico para evitar fugas de información o ataques a sistemas, especialmente si dichos

Reto 3	Gestión de incidentes
	incidentes son detectados en los estadios iniciales, dado que las medidas mitigadoras podrán activarse, reaccionando así con anterioridad a que el daño sea mayor. Con este reto, se pretende impulsar la creación de nuevas soluciones, o plataformas, para el tratamiento de incidentes de ciberseguridad que permitan a los usuarios operadores responder, con más eficiencia, con un menor nivel de estrés, reduciendo el riesgo de error humano en los sistemas. Y asegurando de forma sistemática los pasos adecuados para reaccionar de la forma más efectiva posible. Aunque algunas propuestas pueden plantear desarrollos de tipo procedimental, el elemento esencial deberá basarse en el uso de nuevas tecnologías o nuevas aplicaciones de tecnologías existentes. Se considerarán soluciones de todo tipo, ya sean de detección, preventivas, reactivas o de análisis post-incidente (forense), siempre que se considere que existe un alto grado de innovación en la solución propuesta.

Reto 4	Protección de datos e información
Descripción de la necesidad:	Ciudadanos y empresas conectados se encuentran en una situación constante de exposición de su información ante posibles robos, pérdidas o secuestro de sus datos. Una buena securización y un correcto bastionado en cualquier sistema se convierten en algo imprescindible, siendo una de las formas más eficientes de evitar la pérdida dicha información sensible. Este reto se centrará en aportar soluciones cuya finalidad sea la de la proteger la información que reside en equipos y/o redes, de tal forma que estos sean más inaccesibles para los atacantes, haciendo menos vulnerables los sistemas que custodian y, por tanto, evitando que se produzcan ciberataques, o al menos reduciendo su probabilidad y eventual impacto. Asimismo, y atendiendo a la legalidad vigente en materia de protección de datos, también es importante aportar soluciones de cifrado capaces de mantener el secreto de la información incluso durante el procesado de la misma (como puede ser el caso del cifrado *homomórfico* u otros análogos). Otros retos tecnológicos actuales, como es el caso de la aplicación de Inteligencia Artificial a los modelos de negocio (como puede ser el caso del *Federated Learning*), simplemente no podrían ponerse en marcha sin este tipo de seguridad en el procesado de información.

Reto 4	Protección de datos e información
	De igual forma, guardar de forma estructurada y continua una correcta trazabilidad de las acciones que van sucediendo sobre los sistemas ayudará a la hora de realizar estudios posteriores y facilitará la gestión de análisis en frío, en caso de que se llegasen a producir ataques. Además, una forma cada vez más preocupante de atentado contra los datos es la que afecta a la privacidad de datos de carácter personal o corporativo; no sólo importan los documentos de los usuarios y organizaciones, sino también su *comportamiento digital*. A este respecto, este reto también aborda soluciones capaces de asegurar la privacidad y evitar el *trazado* de las acciones del usuario.

Reto 5	Protección de las comunicaciones
Descripción de la necesidad:	Las conexiones de un sistema con el exterior son el principal punto de riesgo en la ciberseguridad, en una actualidad tecnológica en la que el clásico concepto de *perímetro* prácticamente desaparece. La protección de los puntos que sirven de contacto con internet o de las redes por las que se accede a ellos es un elemento clave, que requiere consideraciones particulares de ciberseguridad. En el escenario actual, con un desarrollo acelerado de las comunicaciones, tanto en volumen como en diversidad y complejidad, con una enorme interdependencia de elementos diversos, incluyendo el marco de la IoT, y con grandes cantidades de intercambios de información con otras entidades, la protección frente a incidentes derivados de estos contactos se convierte en una prioridad de primer nivel, y si se gestiona de forma efectiva, en una potencial reducción del riesgo muy significativa. Las soluciones para plantear en este marco deben contemplar todo tipo de situaciones, tratando de abarcar éstas de forma holística, integral. Podrán ser, bien soluciones globales (para usuarios genéricos), o bien soluciones particulares para tipologías de usuarios concretos como, por ejemplo, entornos industriales, entornos logísticos, entornos sanitarios, etc.

Reto 6	Detección y análisis de amenazas y vulnerabilidades
Descripción de la necesidad:	Un elemento clave de la respuesta ante incidentes de ciberseguridad es la rapidez y la anticipación, y ambas dependen directamente de la flexibilidad de la organización atacada a la hora de poner en valor su conocimiento ante situaciones de compromiso de la seguridad. Desde este punto de vista, la detección temprana y análisis de amenazas y vulnerabilidades puede considerarse una característica primordial, para poder actuar en consecuencia y agotar las opciones de cara a prevenir que sucedan acciones no deseadas sobre los sistemas monitorizados. La detección y análisis de amenazas y vulnerabilidades es un reto en sí mismo, dada su naturaleza y múltiples ámbitos desde los cuales pueden sucederse los ataques: bien sea a nivel de red, conexiones físicas, sistemas internos, etc. Dicha detección puede también tener en cuenta el resto de actores participantes en la cadena de negocio, como son proveedores y clientes. No en vano la seguridad se concibe como una cadena, en la que la robustez del conjunto depende del eslabón más débil: todos los eslabones requieren atención. La ciberinteligencia se erige como un pilar básico para identificar, recoger, evaluar, analizar e interpretar gran cantidad de información sobre ciberamenazas, con el objetivo de predecir nuevos peligros. Conocer a los atacantes y poder asociar unas tácticas, técnicas y procedimientos (TTPs) a su modus operandi es un factor clave a la hora de realizar una detección temprana de amenazas. Igualmente, la detección de ataques, o lo que es lo mismo, la materialización de una amenaza mediante la explotación de una vulnerabilidad, es otro aspecto primordial para garantizar la seguridad de los sistemas, y por tanto, técnicas de identificación y análisis de vulnerabilidades cobran especial importancia. Las propuestas relacionadas con este reto deben plantear ideas y desarrollos innovadores para abordar una detección, lo más precoz posible, de ciberamenazas en uno o varios ámbitos.

Reto 7	Simulación de incidentes
Descripción de la necesidad:	Entre las formas de prevención de los ataques maliciosos, las técnicas basadas en simulación pueden jugar un papel relevante en diferentes tipos de eventos, tales como: • Simular incidentes para mejorar, desde un entorno controlado, los sistemas de defensa.

Reto 7	Simulación de incidentes
	• Simular elementos que sirvan de *señuelo* para atacantes reales y que permitan identificar riesgos y aprender las (nuevas) técnicas del enemigo, así como evitar que los sistemas principales se vean comprometidos. • Simular sistemas de protección ante diferentes intensidades de ataque, con fines de entrenamiento de los equipos humanos de especialistas. • Simular respuestas (individuales o coordinadas) para probar qué aproximaciones son más efectivas para cada tipo de ataque. • Otras formas de simulación dirigidas a la obtención de conocimiento espontáneo sobre técnicas y herramientas maliciosas. Con este reto se pretenden identificar soluciones basadas en técnicas de simulación que saquen partido de nuevas tecnologías para desarrollar soluciones que permitan mejorar la seguridad de diferentes tipos de usuarios. Entre los elementos clave de este reto se encuentra la flexibilidad para adaptar las simulaciones en escenarios futuros; es decir que el interés en el que se centra el presente reto no se limita a la simulación de problemáticas actuales, sino que pretende ir más allá, planificando acciones que se anticipen a riesgos emergentes y/o desconocidos en la actualidad.

Reto 8	Otros retos en materia de Ciberseguridad
Descripción de la necesidad:	Adicionalmente a los retos enumerados anteriormente, y con el objetivo principal de impulsar la industria de la Ciberseguridad a través de la Compra Pública de Innovación, se aceptarán propuestas de Proyectos de I+D que solucionen los retos y necesidades planteadas en las principales estrategias nacionales, europeas e internacionales en materia de Ciberseguridad. Como referencia, y entre otras, se podrán adoptar los siguientes documentos estratégicos y sus respectivos *topics*: • **Estrategia Nacional de Ciberseguridad:** *https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019* • **Estrategia Nacional de Inteligencia Artificial:** *https://portal.mineco.gob.es/es-es/ministerio/areas-prioritarias/Paginas/inteligencia-artificial.aspx* • **5G – Plan Nacional 5G** *https://avancedigital.mineco.gob.es/5G/Paginas/medidas-5G.aspx*

Reto 8	Otros retos en materia de Ciberseguridad
	• **ENISA - *Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation Needs and Priorities*:** *https://www.enisa.europa.eu/publications/research-and-innovation-brief* • **ENISA - *Artificial Intelligence Cybersecurity Challenges*:** *https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges* • **ENISA *Threat Landscape 2020 - Research topics:*** *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-research-topics* • **ENISA - *Good practices in innovation on cybersecurity under the NCSS:*** *https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss* • **Proyecto Quantum (sección Ciberseguridad):** *https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=536* • **Brújula estratégica de la EU:** *https://www.consilium.europa.eu/es/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/*

De conformidad con el artículo 115 de la LCSP, el presente informe se difundirá mediante publicación en la PLACSP, asegurando que esté al alcance de cualquier proveedor potencial y garantizado la transparencia y la igualdad de trato entre los futuros licitadores.

En León, a 21 de junio de 2022