GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia

Consultas al Mercado para la definición de actuaciones de impulso de la Ciberseguridad y la elaboración del Mapa de Demanda Temprana de Incibe

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

1. RESUMEN

INCIBE está impulsando la Compra pública innovadora (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, a la vez que apoyar el desarrollo de una industria nacional competitiva en este campo.

*Para, **elaborar el Mapa de Demanda Temprana de INCIBE**, listado de necesidades sin solución actual en el mercado detectado en materia de ciberseguridad, en el que se identificarán actuaciones, instrumentos y posibles proyectos que licitar mediante Compra Pública de Innovación, se publica la presente Consulta Preliminar al Mercado.*

A lo largo de los próximos 3 años, INCIBE perseguirá no solamente obtener resultados en cuanto a la mejora de la ciberseguridad, sino también crear efectos e impactos duraderos que supongan una aportación a la recuperación, transformación y la resiliencia del modelo productivo.

*INCIBE ha identificado **siete tipos de actuaciones susceptibles de ser ejecutadas mediante compra pública de innovación.** Estas actuaciones deberán servir para financiar numerosos proyectos individuales ejecutados por empresas y centros de conocimiento.*

Como resultado de esta Consulta Preliminar al Mercado, se espera ejecutar actuaciones mediante Compra Pública de Innovación por valor de 224 millones de euros.

2. INTRODUCCIÓN

INCIBE está impulsando la **Compra pública innovadora (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, a la vez que apoyar el desarrollo de una industria nacional competitiva en este campo.

Para, **elaborar el Mapa de Demanda Temprana de INCIBE**, en el que se identificarán actuaciones, instrumentos y posibles proyectos que licitar mediante Compra Pública de Innovación se publica la presente Consulta Preliminar al Mercado.

Los **objetivos de estas consultas al mercado** son:

(1) Informar al mercado de las actuaciones que se impulsarán a través de la Compra Pública de Innovación;

(2) conocer las propuestas de proyectos concretos que —en cada una de esas actuaciones— permitan a INCIBE elaborar un Mapa de Demanda Temprana y diseñar los instrumentos para la ejecución de cada una de las actuaciones identificadas; y

(3) dotar a INCIBE de la información necesaria para el diseño detallado de los instrumentos de ejecución de las actuaciones (procedimientos, pliegos y contratos).

A lo largo de los próximos años, INCIBE perseguirá no solamente obtener resultados en cuanto a la mejora de la ciberseguridad, sino también crear efectos e impactos duraderos que supongan una aportación a la recuperación, transformación y la resiliencia del modelo productivo.

Las actuaciones que se diseñarán como resultado de esta Consulta Preliminar al Mercado —y que serán publicadas en un Mapa de Demanda Temprana en el mes de octubre de 2021— contarán con un presupuesto público aproximado de 224 millones de euros. Realizando una movilización de inversión público-privada que será calculada en la ejecución de cada proyecto.

3. CONTEXTO

3.1. Las políticas públicas de impulso de la ciberseguridad: UE y España.

La importancia que adquiere en la actualidad el diseño de políticas públicas para impulsar la ciberseguridad es creciente. Un fenómeno que está alineado con la prioridad estratégica de la Unión Europea en digitalizar la economía, pues ello comportará una mayor autonomía estratégica de su industria y sectores críticos. Ya en la Comunicación oficial de la **Comisión Europea "Configurar el futuro digital de Europa" (2020)** se prefiguraban iniciativas para promover las soluciones tecnológicas que permitirán a la UE liderar la transformación digital.

Por su parte, la **Estrategia Europea de Datos,** de febrero de 2020**,** establece cuatro pilares como requisitos previos esenciales para una sociedad empoderada por el uso de los datos, la protección de datos, los derechos fundamentales, la seguridad y la ciberseguridad.

En este marco de actuación, se lanzaba el nuevo **Programa Europa Digital (2021-2027)** con una inversión total de 8.200 M€, de los cuales 1.900 M€ se destinan al despliegue de capacidades para la ciberseguridad para administraciones públicas, empresas e individuos. Y, de forma complementaria, el **Plan de Recuperación Europeo** (*EU Recovery Plan*) apuesta por una presencia tecnológica más fuerte en ámbitos como la IA, la infraestructura de datos, las redes 5G y 6G, el blockchain y la ciberseguridad y ciber-resiliencia.

En este contexto, la reciente **Estrategia Europea de Ciberseguridad,** presentada el pasado 16 de diciembre de 2020 por la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, busca impulsar la resiliencia colectiva en Europa contra las amenazas cibernéticas y ayudar a garantizar a que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios fiables (4.500 millones de euros de inversión combinada entre la UE, los Estados miembros y la industria). Así, el objetivo 3 de la Estrategia pretende reforzar las capacidades industriales y tecnológicas de la UE en materia de ciberseguridad, incluso mediante proyectos financiados conjuntamente por los presupuestos nacionales y de la UE. Esta estrategia es un componente clave de otros planes y estrategias como el *Shaping Europe's Digital Future, la New Industrial Strategy, el EU Recovery Plan y la EU Security Union Strategy 2020-2025.*

El Gobierno de España está completamente alineado con la política industrial y digital europea y, en concreto, con la Estrategia Europea de Ciberseguridad, a través de:

- **Agenda España Digital 2025**, que tiene como cuarta medida de acción: "Reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial". Además, como ejes de la Agenda, se presentaron en diciembre de 2020, el Plan para la Conectividad y las Infraestructuras Digitales y la Estrategia de Impulso a la Tecnología 5G, dotados con 4.320 millones de euros hasta 2025. La **Estrategia Nacional de Ciberseguridad (2019)**, donde se incluye en su línea de acción 5 (Potenciar la industria española de ciberseguridad, y la generación y retención del talento, para

el fortalecimiento de la autonomía digital) la siguiente medida: impulsar programas de apoyo de I+D+I en seguridad digital y ciberseguridad en empresas, universidades y centros de investigación, facilitando el acceso a través de incentivos nacionales e internacionales y mediante programas de compra pública innovadora (CPI).

- Las Directrices Generales de la **Nueva Política Industrial 2030**, en concreto, en el eje 1. Digitalización, se hace hincapié en la promoción de la ciberseguridad como una de las acciones clave a llevar a cabo dentro de la actuación 1. Impulso a la transformación digital desde el Estado.
- La **Estrategia Española de Ciencia, Tecnología e Innovación (2021-2027)** incide en la necesidad de impulsar instrumentos de apoyo público en I+D+I para promover la ciberseguridad en la industria y en tecnologías clave, a través del Sector estratégico 4. Seguridad para la Sociedad (línea estratégica de ciberseguridad).
- Otras estrategias vinculadas: Estrategia de Seguridad Nacional (2017) y Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (2019-2023).

Como instrumento para impulsar la colaboración público-privado se creó, en julio de 2020 en España, el **Foro Nacional de Ciberseguridad,** para dar respuesta al objetivo 3 de la Estrategia Nacional de Ciberseguridad "Protección del ecosistema empresarial y social y de los ciudadanos", a través de la línea de acción 4 "Impulsar la ciberseguridad de ciudadanos y empresas". Liderado por el Consejo de Seguridad Nacional y en asistencia al Consejo Nacional de Ciberseguridad, integra a representantes de la sociedad civil, expertos independientes, centros de investigación, empresas, asociaciones, etc., para debatir y generar conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

De manera complementaria, y tras la crisis sanitaria y económica provocada por el COVID-19, el **Plan de Recuperación, Transformación y Resiliencia (PRTR)** es un proyecto país que orienta la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo, la reconstrucción sólida, inclusiva y resiliente, dando respuesta a los retos de la próxima década. España invertirá más de 140.000 M€ en los próximos años, a través del **Fondo de Recuperación Next Generation EU y e**l Plan guiará la ejecución de 72.000 millones de euros de fondos europeos hasta 2023 y movilizará en los próximos tres años el 50% de los recursos con los que cuenta España gracias al instrumento Next Generation EU.

El PRTR, alineado con España Digital 2025, incluye acciones orientadas **a promover la digitalización y la ciberseguridad en las Administraciones Públicas, empresas (incluidas pymes y start-ups) y en el modelo productivo** en general a través de los sectores estratégicos (Agroalimentario, Movilidad, Salud, Energía, Turismo, etc.). En concreto, la ciberseguridad forma parte de varios componentes del Plan.

Ilustración 1: Componentes del PRTR orientados a promover la digitalización y la ciberseguridad en las AAPP

Componente 11. Modernización de las Administraciones Públicas	Componente 15. Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G
Inversión 1: Modernización de la Administración General del Estado, y orientación al servicio del ciudadano: • Mejora de los servicios públicos digitales, mejorando las infraestructuras tecnológicas y la **ciberseguridad**, automatizando procesos y el desarrollo de servicios públicos basados en datos.	**Inversión 7: Ciberseguridad:** • Fortalecimiento de las capacidades de ciberseguridad de ciudadanos, pymes y profesionales. • Impulso del ecosistema del sector ciberseguridad. • Aumento de la visibilidad de España como actor clave internacional en materia de ciberseguridad.
Componente 19. Plan Nacional de Competencias Digitales (*digital skills*)	**Componente 21. Modernización y digitalización del sistema educativo, incluida la educación temprana de 0 a 3 años**
Inversión 4: Profesionales digitales: • Adaptación de la oferta formativa de formación profesional existente y el diseño de nuevas especialidades que permitan adquirir competencias digitales avanzadas y progresar en áreas clave como la **ciberseguridad**.	**Inversión 5: Mejora de infraestructuras digitales**, el equipamiento, las tecnologías, la docencia y la evaluación digitales universitarios, así como acciones para la reducción de brecha digital del personal académico y del estudiantado. Los "Proyectos de Infraestructuras" serán impulsados a través de RedIris e instituciones como el INCIBE.

En este contexto, el Ministerio de Asuntos Económicos y Transformación Digital, en concreto la Secretaría de Estado de Digitalización e Inteligencia Artificial ha decidido emplear la Compra Pública de Innovación como instrumento para alcanzar los objetivos de impulso de la ciberseguridad en España (componentes 15 y 19).

Así, INCIBE será el órgano de contratación de diversas actuaciones que, mediante procedimientos de Compra Pública de Innovación, permitan alcanzar los siguientes objetivos:

1) En el ámbito del impulso de la industria de Ciberseguridad:
   - Apoyar la I+D+I de la industria.
   - Promover iniciativas estratégicas de productos MVP con alto impacto.
   - Impulsar la internacionalización de la industria de ciberseguridad.
   - Crear plataformas y repositorio de retos de la industria y las AA.PP.
   - Diseñar nuevas soluciones y prototipado en entornos de usuario final.
   - Diseñar la cátedra de ciberseguridad.
2) En el ámbito del emprendimiento:
   - Promover el emprendimiento en ciberseguridad.
   - Diseñar programas de aceleración con las CC.AA.
   - Impulsar Start-Ups en ciberseguridad.
3) En el ámbito de las PYMEs y los ciudadanos:
   - Fortalecer las capacidades de ciberseguridad de ciudadanos,

- Fortalecer las capacidades de ciberseguridad de las PYMES y profesionales autónomos.
- Difundir y divulgar la importancia de la ciberseguridad en la sociedad.

4) En el ámbito de talento:

- Identificar y desarrollar el talento en ciberseguridad.
- Fomentar las competencias en ciberseguridad en gente joven.

En concreto, INCIBE destinará 224 millones de euros para ejecutar actuaciones a través de la Compra Pública de Innovación.

3.2. El Instituto Nacional de Ciberseguridad de España.

El INCIBE se constituye como el instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación, siendo la entidad de referencia para fomentar la ciberseguridad y la confianza y protección digital de los ciudadanos (en general y, en concreto, a menores de edad), la red académica y de investigación, profesionales, empresas, sectores estratégicos e infraestructuras críticas. Como tal, **el INCIBE es el organismo encargado de gestionar las inversiones en Ciberseguridad del Plan de Recuperación, Transformación y Resiliencia España Puede y de ejecutar las inversiones descritas a través de la Compra Pública de Innovación.**

INCIBE es una sociedad mercantil estatal dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Como centro de excelencia tiene como misión:

- Mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España.
- Proteger y defender a los ciudadanos, menores y empresas privadas de España.
- Potenciar la industria española de ciberseguridad.
- Impulsar la I+D+i española en ciberseguridad.
- Identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad.

Para acometer esta labor, INCIBE cuenta con amplias capacidades orientadas a dar respuesta a incidentes de seguridad abarcando desde la ciudadanía hasta el sector empresarial y al ámbito específico de RedIRIS. Asimismo, impulsa iniciativas de colaboración público-privada para la mejora de los niveles de ciberseguridad en España y hace un seguimiento y estudio continuados de los riesgos emergentes para poder anticipar necesidades, adoptar medidas preventivas y, en definitiva, disponer de mecanismos de alerta temprana.

En particular, las actividades desarrolladas por INCIBE se pueden clasificar de la siguiente forma:

- Ofrece servicios que permiten el aprovechamiento de las TIC y elevan la confianza digital, a través de mecanismos para la prevención y reacción a incidentes de

seguridad de la información, y promoviendo el avance de la cultura de la seguridad de la información a través de la concienciación, la sensibilización y la formación.

- Participa en proyectos complejos de diversa naturaleza y con una fuerte componente innovadora y con capacidad para generar inteligencia en ciberseguridad que revierta en la mejora de los servicios.
- Promociona e impulsa la I+D+I, el talento y el emprendimiento, a través de compra pública de innovación y de otros instrumentos.
- Participa en redes nacionales e internacionales de colaboración en el ámbito de la ciberseguridad, fundamentada en la experiencia y en el intercambio de información.

La actividad de INCIBE se enmarca en las políticas públicas de ciberseguridad del Gobierno español antes indicadas. En particular, el nuevo Plan Estratégico 2021-2025 de INCIBE se alinea con la Agenda España Digital 2025, tanto en lo que respecta a sus contenidos, objetivos y metas, como a su plazo temporal de ejecución; y, de forma específica, la Estrategia Nacional de Ciberseguridad de 2019 ha servido de base para formular los objetivos y acciones contemplados en el Plan Estratégico de INCIBE.

Además, el Plan de Recuperación, Transformación y Resiliencia -PRTR- (Plan España Puede) se constituye como un elemento clave para INCIBE como principal organismo ejecutor de la inversión en ciberseguridad.

4. LA CONSULTA PRELIMINAR AL MERCADO

4.1. Objetivos de esta consulta al mercado.

Los objetivos de estas consultas al mercado son tres:

1) Informar al mercado de las actuaciones que se impulsarán a través de la Compra Pública de Innovación;

2) Conocer las propuestas de proyectos concretos que —en cada una de esas actuaciones— permitan a INCIBE elaborar un Mapa de Demanda Temprana y diseñar los instrumentos para la ejecución de cada una de las actuaciones identificadas; y

3) Dotar a INCIBE de la información necesaria para el diseño detallado de los instrumentos de ejecución de las actuaciones (procedimientos, pliegos y contratos).

4.2. Actuaciones que se someten a la consulta al mercado.

INCIBE realizará un conjunto de actuaciones diversas. **La presente consulta se centra en aquellas actuaciones (siete) dirigidas a impulsar la I+D+i o a la creación de productos y soluciones en el ámbito de la ciberseguridad, a través de la compra pública de innovación**. En concreto, se solicita a los operadores económicos que presenten proyectos que pueden enmarcarse en las siguientes **siete actuaciones:**

- **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.

- **Soluciones tecnológicas a retos del sector público**, abarcando tanto la creación de las soluciones como su demostración y operación en el entorno real durante un periodo de tiempo suficiente para validar la calidad de los productos y soluciones creadas. Deberán ser propuestas por empresas o consorcios que cuenten con el compromiso de usuarios públicos concretos. Los proyectos deberán partir de TRL6 o TRL7 y finalizar en TRL 9.

- **Soluciones tecnológicas para la ciberseguridad en las PYMES**, llevadas a cabo por consorcios integrados por empresas industriales y empresas o entidades capaces de comercializar las soluciones al mayor espectro posible de PYMES, proponiendo modelos de negocio para la fase de implantación y comercialización de las soluciones creadas. Los proyectos deberán partir de TRL6 o TRL7 y finalizar en TRL 9.

- **Soluciones tecnológicas de ciberseguridad para sectores estratégicos (energía, transporte, infraestructura, entre otros) de la NIS2 (usuarios de la tecnología)**. Estos proyectos se realizarán a través de consorcios que integren empresas industriales o creadoras de tecnología y empresas usuarias de dichos sectores, incluyendo tanto la creación como el testado de las soluciones en entornos operativos reales. Los proyectos deberán partir de TRL6 o TRL7 y finalizar en TRL 9.
- **Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE**, incluyendo la creación y desarrollo de un centro demostrador. Los proyectos deberán partir de TRL6 o TRL7 y finalizar en TRL 9.
- **Soluciones tecnológicas vinculadas a la formación y/o al desarrollo de capacidades y de habilidades de las personas en ciberseguridad**.
- **Pequeños proyectos** altamente innovadores en ciberseguridad realizados por PYMES o por emprendedores con la voluntad de crear una nueva empresa.

4.3. Instrumentos mediante los que se ejecutará la inversión.

El instrumento que empleará INCIBE para la contratación de proyectos es la compra pública de innovación. En función de la información recibida en estas consultas, se diseñarán en detalle los instrumentos.

Se han identificado como posibles instrumentos de actuación:

- **Compra Pública Precomercial**, mediante la que se pretende contratar servicios de I+D para el avance en las tecnologías desde TRLs bajos hasta TRL7 u 8, dando respuesta a retos públicos y público-privados y generando un alto impacto industrial.
- **Compra Pública de Tecnología Innovadora y Asociación para la innovación**, para la creación de soluciones innovadoras que den respuesta a retos públicos o público-privados y permitan demostrar el funcionamiento de soluciones creadas en entornos reales, hasta TRL9.

4.4. Roles con los que participar en la Consulta.

En el marco de estos objetivos, cada entidad participante en las consultas deberá identificar el rol o posibles roles con los que podría participar en estas actuaciones:

- **Rol 1. Empresas de la industria de la ciberseguridad creadoras de tecnología y comercializadoras de tecnología, productos y soluciones:** Empresas del sector TIC, empresas consultoras de TIC, fabricantes de equipos, etc. con capacidad de I+D y generación de tecnología para su comercialización como tecnología o producto; distinguiéndose de las siguientes en que comercializan tecnología y no solamente servicios de ciberseguridad.

- **Rol 2. Empresas comercializadoras y prestadoras de servicios de ciberseguridad,** tanto para amplios colectivos —como pueden ser operadores de telecomunicaciones, entidades financieras, empresas aseguradoras— como para colectivos restringidos o sectores determinados.
- **Rol 3. Empresas usuarias de tecnología:** empresas usuarias de tecnologías para la ciberseguridad, especialmente de sectores estratégicos NIS2 (construcción, infraestructuras industriales, servicios urbanos y energía, gran industria, entidades financieras y aseguradoras, transporte y turismo, gran consumo, ocio y deporte, servicios profesionales, etc.); bien desarrollen soluciones internamente o bien lo hagan con empresas externas.
- **Rol 4. Universidades y centros tecnológicos** como creadores de conocimiento, mediante la participación en consorcios de I+D con empresas industriales.
- **Rol 5. Administraciones Públicas usuarias de tecnologías:** Administración General del Estado, gobiernos regionales, entidades locales y empresas públicas.
- **Rol 6. Asociaciones y tercer sector:** clúster y asociaciones de Ciberseguridad y TIC, asociaciones de otros sectores (eléctrico, hotelero), cámaras de comercio y colegios profesionales y tercer sector (asociaciones, fundaciones y confederaciones), como apoyo a los consorcios o empresas industriales que presenten grandes proyectos de I+D, que puedan tener impacto sobre la divulgación y la difusión de la ciberseguridad en su entorno.

4.5. Retos tecnológicos.

Se han identificado los principales retos tecnológicos que preocupan a la industria española de ciberseguridad y a las empresas y AA.PP. usuarias. La siguiente lista enumera los principales retos tecnológicos, sin carácter exhaustivo y sin que su enumeración suponga ningún límite para la presentación de las propuestas que se solicitan en esta Consulta Preliminar al Mercado. En este sentido, los proponentes podrán identificar cualesquiera otros retos tecnológicos que resulten de su interés.

4.5.1. Sistemas de ciberseguridad.

Este reto tecnológico tiene diversos ámbitos de actuación, en función de la finalidad a la que está orientada la seguridad:

- **Sistemas de categorización, detección temprana, prevención y predicción automatizada de ciberataques y ciberamenazas,** que permitan confiar en que un sistema operativo, un programa informático, un servicio, un proceso o una red funcionan o han sido diseñados para funcionar con el objetivo de seguridad deseado o de acuerdo con una política de seguridad definida.
- **Sistemas de inteligencia de ciberamenazas.** Estos sistemas buscan la mejora de la ciberseguridad mediante el conocimiento de los TTP's de las amenazas, de los recursos que utilizan y de la actividad de sus actores, así como la identificación lo

más temprana posible de las víctimas que provocan o van a provocar. En lo que a esta consulta preliminar al mercado se refiere, podemos distinguir estos sistemas de inteligencia de otros sistemas de ciberseguridad en que la investigación se realiza sin instalar ni software ni equipamiento en los sistemas TIC de las víctimas potenciales; es decir, la investigación se realiza en Internet o sobre los activos o recursos que usan los agresores. Un objetivo final de estos sistemas de inteligencia es que el conocimiento e información que generan se pueda usar para evitar o mitigar el daño que las amenazas puedan causar, por lo que la posible accionabilidad de la información y conocimiento que obtengan tendrá un peso significativo en su valoración. Otro objetivo es que ayuden en la definición de estrategias para la mejora de la ciberseguridad.

- **Seguridad integral en infraestructuras críticas**, para reducir y mitigar el riesgo de ciberataques y ciberamenazas en este tipo de infraestructuras: “infraestructuras estratégicas que proporcionan servicios esenciales cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales”.
- **Sistemas de seguridad y privacidad relacionadas con los datos** con el fin de preservar la privacidad, la confidencialidad, la integridad y la disponibilidad de la información, así como otros aspectos como la autenticidad, la responsabilidad y el no repudio. Todo ello sin perjudicar los fines del tratamiento de datos, o impedir el uso indebido de los datos una vez que las entidades autorizadas hayan accedido a ellos. Incluye tanto la criptografía y el criptoanálisis y, en general, todos los desarrollos matemáticos, algorítmicos, las arquitecturas infraestructurales, así como la implementación de metodologías, técnicas y herramientas criptoanalíticas.
- Sistemas de **seguridad en gobernanza y gestión** orientados a facilitar la **toma de decisiones y mejorar el rendimiento y la responsabilidad** a través de la recopilación, el análisis y la presentación de informes de datos relevantes relacionados con el impacto de la ciberseguridad.

INCIBE estaría interesada en recibir propuestas relacionadas con el desarrollo de sistemas de seguridad que:

- generen conocimiento sobre los TTP’s y recursos que usan las ciberamenazas, así como sobre la actividad maliciosa que realizan sus actores.

- permitan la prevención, predicción y detección temprana de ciberamenazas y ciberataques.

- permitan evitar la victimización o, si no llegan a tiempo, permitan identificar lo antes posible a las víctimas de las amenazas con el objeto de mitigar los daños.

- generen conocimiento sobre las ciberamenazas que ayude a INCIBE a definir las mejores estrategias para luchar contra ellas.

- faciliten la ayuda a las víctimas por parte de INCIBE

- garanticen el correcto funcionamiento de las infraestructuras críticas.

- garanticen la privacidad de los datos.

- optimicen la gobernanza, la gestión y la toma de decisiones.

4.5.2. Plataformas tecnológicas en educación y formación en ciberseguridad.

Plataformas orientadas al proceso de aprendizaje para adquirir los conocimientos, el saber hacer, las habilidades y/o las competencias necesarias para proteger los sistemas de red y de información, sus usuarios y las personas afectadas por las ciberamenazas y ciberataques (educación superior, formación profesional, cultura de la ciberseguridad, metodología educativa, herramientas de educación/formación, concienciación sobre ciberseguridad, etc.).

INCIBE estaría interesada en recibir propuestas relacionadas con el desarrollo de plataformas tecnológicas en educación y formación a la ciudadanía y empresas en todos aquellos aspectos críticos relacionados con la ciberseguridad.

4.5.3. Gestión de la identidad digital.

Tecnologías orientadas al diagnóstico de atributos de identidades conocidas, considerando los aspectos de la gestión del acceso, incluida la autenticación, la autorización y el control de acceso de las personas y los objetos inteligentes cuando acceden a los recursos. Estos aspectos pueden incluir elementos físicos y digitales de los sistemas de autenticación y aspectos legales relacionados con el cumplimiento y la aplicación de la ley.

INCIBE estaría interesada en recibir propuestas relacionadas con el desarrollo de soluciones tecnológicas orientadas a la seguridad en la identificación digital de las personas y objetos inteligentes.

4.5.4. Tratamiento de incidencias y análisis forense digital.

Este dominio se refiere a las técnicas, herramientas y procesos para la identificación, recolección, adquisición y preservación de evidencias digitales. Por ejemplo, tecnologías orientadas a mejorar el análisis de incidencias, comunicación, documentación, previsión, tiempo de respuesta, etc., así como para la identificación, recogida, atribución, adquisición, análisis y conservación de pruebas digitales (por ejemplo, identificación de la autoría del código y del atacante, garantía de procedencia, correlación de pruebas digitales, triaje de pruebas digitales, etc.)

INCIBE estaría interesada en recibir propuestas relacionadas con el desarrollo de soluciones tecnológicas que tengan como finalidad la optimización del tratamiento de incidencias y análisis forense digital.

4.5.5. Sistemas de red y distribución.

La seguridad de las redes tiene que ver con el hardware, el software, los protocolos básicos de comunicación, la estructura de la red y los factores de los mecanismos de comunicación de la red. La seguridad de la información en el contexto de la red se ocupa de la integridad,

la confidencialidad, la disponibilidad y el no repudio de los datos mientras se envían a través de la red.

En cuanto a los sistemas de distribución, es un modelo en el que los componentes situados en ordenadores en red se comunican y coordinan sus acciones mediante el paso de mensajes. En este contexto, la ciberseguridad se ocupa de todos los aspectos del cálculo, la coordinación, la integridad de los mensajes, la disponibilidad y la confidencialidad. La autentificación de los mensajes también entra en el ámbito de aplicación.

INCIBE estaría interesada en recibir propuestas relacionadas con el desarrollo de sistemas seguros de redes de comunicación y distribución de la información.

5. PRESENTACIÓN DE PROPUESTAS

5.1. Proceso y plazo de presentación de propuestas

Las consultas al mercado se presentarán a través de email: relaciones.industria@incibe.es

Las propuestas contendrán los siguientes documentos:

- **Ficha básica de la propuesta** que se adjunta más adelante y cuyo archivo electrónico puede descargarse de la web de INCIBE.
- **Memoria detallada de cada propuesta**, de acuerdo con lo establecido en el apartado 4.4 y en los anexos correspondientes a cada tipo de actuación.
- **En su caso, cualquier otra documentación que se estime de interés.** En el caso de adjuntar videos, se deberá incluir un link para la visualización o descarga del video.

El **plazo para el envío de las consultas al mercado** comienza el día de su publicación jueves 1 de julio y concluirá el viernes 13 de agosto de 2021 a las 19:00 horas.

Toda la documentación aportada por los participantes en las consultas será tratada de manera confidencial, de manera que no se hará uso público de la misma.

No obstante, los participantes aceptan, en los términos expresados en este documento, que la información aportada pueda ser empleada en el diseño de los procedimientos de contratación que se tramiten con ulterioridad bajo la fórmula de Compra Pública de Innovación.

5.2. Ficha básica para la presentación de propuestas

DATOS BÁSICOS DE LA PROPUESTA

(Una ficha por cada propuesta presentada)

Denominación de la propuesta	
Denominación social de la entidad líder o representante del consorcio	
Denominación de otras entidades que participan o colaboran en la propuesta junto a la entidad promotora del proyecto. *Rellenar sólo en caso de que varias entidades participen en el proceso.*	
Datos del responsable de contacto: (Nombre y cargo)	
Correo electrónico de contacto	
Teléfono de contacto	
Dirección física de contacto:	

DATOS DE CLASIFICACIÓN DE LA ENTIDAD LÍDER Y DE OTROS MIEMBROS DEL CONSORCIO

Tipo de entidad (empresa emergente, microempresa, Pyme, gran empresa, empresa pública, Universidad, Centro tecnológico, etc.)	
Sector de actividad del participante	
Facturación en los últimos años	*2020, 2019, 2018*
Facturación en materia de ciberseguridad en los últimos años	*2020, 2019, 2018*
En su caso, inversión en los últimos años en I+D+i	*2020, 2019, 2018*

Roles en el que presenta propuestas a estas consultas al mercado, incluyendo todos los componentes del consorcio y citando los nombres de la empresa o institución, persona de contacto y correo electrónico.

( ) Rol 1: Empresas de la industria de la ciberseguridad creadoras de tecnología.

Empresa o institución	*Persona de contacto*	*Correo electrónico*
-…		
-…		
-…		

( ) Rol 2: Empresas comercializadoras y prestadoras de servicios de ciberseguridad.

Empresa o institución	*Persona de contacto*	*Correo electrónico*
-…		
-…		
-…		

( ) Rol 3: Empresas usuarias de tecnología.

Empresa o institución	*Persona de contacto*	*Correo electrónico*
-…		
-…		
-…		

( ) Rol 4: Universidades y centros tecnológicos como creadores de conocimiento.

Empresa o institución	*Persona de contacto*	*Correo electrónico*
-…		
-…		
-…		

( ) Rol 5: Administraciones Públicas usuarias de tecnologías

Empresa o institución	***Persona de contacto***	***Correo electrónico***
-…		
-…		
-…		

( ) Rol 6: Asociaciones y tercer sector.

Empresa o institución	***Persona de contacto***	***Correo electrónico***
-…		
-…		

Tipo de actuación	**( ) Programa de I+D.** **( ) Soluciones PYMES.** **( ) Soluciones Sector Público.** **( ) Soluciones Sectores Estratégicos.** **( ) Soluciones Infraestructuras y Equipamiento.** **( ) Soluciones Formación.** **( ) Pequeños Proyectos**
Clasificación de la propuesta por retos tecnológicos:	**( ) Sistemas de ciberseguridad**. **( ) Plataformas tecnológicas en educación y formación en ciberseguridad.** **( ) Gestión de la identidad digital.** **( ) Tratamiento de incidencias y análisis forense digital.** **( ) Sistemas de red y distribución.** **( ) Otros**
Breve resumen	
Duración	

Valoración económica (en euros)	

DECLARACIONES OBLIGATORIAS Y AUTORIZACIÓN DE USO DE LOS DATOS APORTADOS.

Autorizo al Instituto Nacional de Ciberseguridad (INCIBE) al uso de los contenidos de la propuesta. Los contenidos se emplearán exclusivamente en el diseño de los procedimientos de contratación que se tramiten con ulterioridad bajo la fórmula de Compra Pública de Innovación. La no aceptación impedirá la inclusión de la propuesta en este proceso.	Sí () No ()
Autorizo expresamente el uso de los datos personales por parte del Instituto Nacional de Ciberseguridad (INCIBE), con la finalidad de gestionar los datos de los participantes en esta consulta preliminar al mercado y la creación de una base de datos del ecosistema de ciberseguridad en España. Para INCIBE es muy importante la protección de los datos personales. Por favor, lee la cláusula informativa de nuestra política de protección de datos https://www.incibe.es/proteccion-datos-personales. La no aceptación impedirá la inclusión de la propuesta en este proceso. Para ejercitar los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos, a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles), los interesados deberán dirigirse mediante carta a INCIBE, Avenida José Aguado, nº 41, de León o por correo electrónico a dpd@incibe.es. Siendo su Delegado de Protección de Datos el Secretario General de INCIBE, cualquier cambio al respecto será notificado vía correo electrónico al punto de contacto indicado por el contratista.	Sí () No ()

5.3. Descripción detallada de cada propuesta

La Ficha Básica deberá acompañarse, por parte de los participantes, de una **memoria descriptiva de la propuesta**, con una extensión máxima de 20 hojas (sin incluir la ficha básica). Cada entidad podrá presentar propuestas a las actuaciones que considere, **tantas propuestas como considere oportuno** y en tantos consorcios o agrupaciones como considere, sin limitaciones a la participación.

Cada Descripción Detallada deberá contener los puntos establecidos en el Anexo de detalle de cada una de las siete actuaciones.

5.4. Calendario previsto.

Las fechas clave de esta Consulta Preliminar al Mercado y del proceso de licitaciones públicas al que dará lugar, son las siguientes:

- Fecha de cierre de plazo para presentar proyectos: 13 de agosto del 2021.
- Fecha estimada de publicación del Mapa de Demanda Temprana: 11 de octubre del 2021.
- Fecha estimada de publicación de la primera o primeras licitaciones: octubre-diciembre de 2021.

ANEXOS

ANEXO 1: PROGRAMAS I+D

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Programas de I+D** tiene por objetivo la realización de programas conjuntos de I+D entre INCIBE y empresas industriales tractoras, capaces de crear conjuntos de productos, soluciones y tecnologías de alto impacto estratégico para la posición de la empresa en el mercado y que den respuesta a retos del sector público, de las PYMES o de los sectores estratégicos NIS2 a largo plazo. La duración de los programas será de 24 meses desde la firma de los contratos.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- La ejecución de un conjunto de proyectos de I+D (el Programa) individuales pero coherentes estratégicamente.
- La obtención de un número llamativo de productos en TRLs 6,7 y 8, de cara a su futura comercialización.
- La movilización de co-financiación privada, de manera que la empresa promotora y el INCIBE compartan los riesgos del programa conjunto de I+D.

Efectos e impactos.

- La 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. Por ello se valorará el volumen de ventas en el exterior del o de los proponentes y su experiencia en programas internacionales de I+D+i.
- La tracción de Pequeñas y Medianas Empresas y de Universidades, Organismos de Investigación y Centros Tecnológico por las grandes empresas industriales, desarrolladoras y comercializadoras de productos y soluciones. Para ello se valorará la alta participación de este tipo de entidades como subcontratadas en los Programas de I+D.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- La subcontratación de, al menos, un 30% de la financiación aportada por INCIBE a empresas PYMES, Organismos de Investigación, Universidades o Centros Tecnológicos.
- La partida de los proyectos desde tecnología básica y su evolución a TRLs avanzados, sin llegar al TRL9.

- Coherencia con otras propuestas presentadas por la empresa o consorcio en el marco de otras actuaciones. En este sentido, a las empresas que presenten Programas de I+D se les requerirá un mapa completo de proyectos presentados a las distintas actuaciones, identificando productos y TRLs, para garantizar la coherencia de todas las propuestas.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiarán Programas Conjuntos de I+D de alto volumen, considerándose la aportación pública de 86,7 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

La empresas o consorcios que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

1. **Contenido del Programa de I+D propuesto:** proyectos, tecnologías y resultados (incluyendo productos y soluciones, TRLs de partida y de llegada).
2. **Alienación 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.

ANEXO 2: SOLUCIONES PYMES

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Soluciones PYMES** tiene por objetivo la creación de soluciones que permitan atender en remoto las necesidades de ciberseguridad de amplios colectivos de PYMES. Cada proyecto presentado debe permitir no solamente el avance tecnológico hasta la creación de las soluciones, sino su operación y mantenimiento durante un periodo de tiempo suficiente para comprobar su funcionamiento efectivo en dicho colectivo. En este sentido, se firmarán contratos de desarrollo tecnológico, demostración y operación de la solución durante un periodo de entre 24 y 36 meses.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- Nº de centros de atención creados y soluciones tecnológicas disponibles.
- Nº de PYMES que son atendidas desde los centros de atención.
- Contratos a largo plazo de los operadores de los centros con las PYMES usuarias.

Efectos e impactos.

- La mejora de ciberseguridad en las PYMES españolas.
- El impulso de soluciones nacionales capaces de ser competitivas a nivel internacional y, por tanto, de la industria española de la ciberseguridad.
- El impulso de la cultura y el conocimiento de la ciberseguridad entre las PYMES.
- La creación de empleo en el sector de la ciberseguridad.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- Las propuestas deberán estructurar el proyecto en tres fases:
  - Fase 1: Creación de la solución.
  - Fase 2: Demostración y validación de la solución.
  - Fase 3: Operación y mantenimiento de la solución con un amplio colectivo de PYMES.
- Los consorcios proponentes deberán integrar empresas desarrolladoras de tecnología —con interés en la comercialización futura de la misma o de servicios tecnológicos vinculados— y empresas comercializadoras de los servicios de ciberseguridad a las PYMES, con acceso a amplios colectivos de PYMEs (operadores de telecomunicaciones, entidades financieras, seguros, etc.). No se considerarán propuestas que provengan ni de empresas industriales sin capacidad de comercialización a amplios colectivos; ni de empresas proveedoras de servicios básicos a PYMEs sin interés en el desarrollo industrial de la ciberseguridad.

- La Fase 3 de operaciones deberá incluir la operación en un colectivo mínimo de 5.000 PYMEs.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiará la creación de varias soluciones con el objetivo de garantizar la competencia futura en el mercado. La inversión pública estimada total para esta iniciativa se sitúa en 24,8 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

La empresas o consorcios que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

1. **Descripción de la solución propuesta:** tecnologías y elementos clave, estado de partida, requerimientos técnicos mínimos de la solución.
2. **Modelo de negocio para la comercialización de la solución**. Mercado estimado de PYMES, estrategia de comercialización, canales de comercialización, acceso al mercado (del consorcio).
3. **Compromisos mínimos asumidos:** Nº de PYMES que se ofrece, diferenciando entre la Fase 2 y la Fase 3. Tiempo máximo de desarrollo de la Fase 1.
4. **Propuesta de divulgación y difusión.** Actividades que se dedicarán a impulsar la cultura y el conocimiento de la ciberseguridad en las PYMES. Inversión (en €) en estas actividades.
5. **Descripción económica de la propuesta.** Volumen de inversión total. Volumen de inversión por fase. Co-financiación pública o privada. Modelo de comercialización futura de la solución (una vez terminado el contrato).

ANEXO 3: SOLUCIONES SECTORES ESTRATÉGICOS

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Soluciones Sectores Estratégicos** tiene por objetivo la creación de soluciones que permitan atender las necesidades de Ciberseguridad de las empresas públicas y privadas de los sectores estratégicos identificados por la Directiva NIS2.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- Nº de soluciones creadas para sectores estratégicos.
- Nº de empresas que participan como usuarias en las soluciones creadas.

Efectos e impactos.

- La mejora de ciberseguridad en los sectores estratégicos identificados por la NIS2.
- El impulso de soluciones nacionales capaces de ser competitivas a nivel internacional y, por tanto, de la industria española de la ciberseguridad.
- El impulso de la cultura y el conocimiento de la ciberseguridad entre las empresas españolas.
- La creación de empleo en el sector de la ciberseguridad, tanto entre los proveedores como en las empresas usuarias.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- Cada propuesta deberá dar respuesta únicamente a la necesidad de un sector estratégico; pudiendo las empresas presentar tantas propuestas como deseen. En este sentido, no se admitirán propuestas multisector, salvo que se demuestre la eficiencia y eficacia de crear una solución que afecte a sectores relacionados.
- Los consorcios proponentes deberán integrar empresas desarrolladoras de tecnología —con interés en la comercialización futura de la misma o de servicios tecnológicos vinculados— y empresas usuarias de los sectores estratégicos, que deberán participar como miembros del consorcio.
- Todo proyecto deberá dividirse en dos fases:
  - Fase 1: Creación de la Solución.
  - Fase 2: Validación de la Solución en un entorno real.
- Las empresas desarrolladoras de la tecnología y creadoras de la solución deberán mantener la propiedad total o parcial de la solución creada, garantizándose la comercialización de la misma más allá de las empresas de sectores estratégicos que participen como usuarias.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiará la creación de numerosas soluciones y en diversos sectores estratégicos, con el objetivo de alcanzar un catálogo de productos y soluciones de amplio espectro que permita dinamizar el mercado de la ciberseguridad en España e impulsar la competitividad de la industria nacional. En función del número de propuestas presentadas se determinará el presupuesto de la licitación y la posible diferenciación o no por sectores. La inversión pública estimada será de 40,5 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

La empresas o consorcios que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

6. **Descripción del sector estratégico, amenazas y necesidades en ciberseguridad.**
7. **Descripción de la solución propuesta:** tecnologías y elementos clave, estado de partida, requerimientos técnicos mínimos de la solución.
8. **Modelo de negocio para la comercialización de la solución**. Mercado estimado, estrategia de comercialización, canales de comercialización, acceso al mercado (del consorcio).
9. **Validación de la solución:** Nº de empresas que participarán como usuarias. Descripción del entorno real en que se validará la solución.
10. **Propuesta de divulgación y difusión.** Actividades que se dedicarán a impulsar la cultura y el conocimiento de la ciberseguridad en el sector estratégico. Inversión (en €) en estas actividades.
11. **Descripción económica de la propuesta.** Volumen de inversión total. Volumen de inversión por fase. Co-financiación pública o privada. Modelo de comercialización futura de la solución (una vez concluya el contrato)

ANEXO 4: SOLUCIONES SECTOR PÚBLICO

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Soluciones Sector Público** tiene por objetivo la creación de soluciones que permitan atender las necesidades del sector público y mejorar los servicios que ofrece. Cada uno de los proyectos presentados ha de estar orientado no sólo al desarrollo y avance tecnológico hasta la creación de las soluciones, sino también su demostración y operación en el entorno real durante un periodo de tiempo suficiente para validar la calidad de los productos y soluciones creadas. Así, se firmarán contratos de desarrollo tecnológico, demostración y validación durante un periodo entre 24 y 36 meses.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- Nº de soluciones creadas para cada uno de los retos del sector público.
- Nº de soluciones validadas en entorno real para cada uno de los retos del sector público.
- Nº de entidades públicas usuarias de las soluciones creadas.

Efectos e impactos.

- La mejora de los servicios públicos en materia de ciberseguridad.
- El impulso de soluciones nacionales capaces de ser competitivas a nivel internacional y, por tanto, de la industria española de la ciberseguridad.
- El impulso de la cultura y el conocimiento de la ciberseguridad en las empresas españolas y el sector público.
- La creación de empleo público y privado en el sector de la ciberseguridad.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- Cada propuesta deberá dar respuesta únicamente a un reto o conjunto de retos sectoriales del sector público, pudiendo las empresas presentar tantas propuestas como deseen. En este sentido, las empresas describirán los retos a los que dan respuesta, de la mano de usuarios públicos concretos. Estos retos podrán formar parte del Repositorio Nacional de Retos en Ciberseguridad del sector público.
- Las propuestas deberán ser presentadas por empresas o consorcios que cuenten con el compromiso de usuarios públicos concretos, recogidos en cartas de intención o de convenios.

- Todo proyecto deberá dividirse en dos fases:
  - Fase 1: Creación de la Solución.
  - Fase 2: Demostración y validación de la Solución en un entorno real.
- Los proyectos deberán partir de TRL6 o TRL7 y finalizar en TRL 9.
- Las empresas desarrolladoras de la tecnología y creadoras de la solución deberán presentar un modelo de gestión de los resultados de los DPI derivados del proyecto, que incluya el modelo de comercialización de la solución más allá de las entidades públicas que participen como usuarias.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiará la creación de soluciones para diferentes retos y usuarios del sector público, con el objetivo de alcanzar un catálogo de productos y soluciones de amplio espectro orientado a la mejora de los servicios públicos. En función del número de propuestas presentadas se determinará el presupuesto de la licitación y la diferenciación por retos del sector público. La inversión púbica estimada se sitúa en 30,4 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

La empresas o consorcios que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

1. **Descripción de las necesidades, retos y usuarios públicos de la tecnología y solución desarrollada.**
2. **Descripción de la solución propuesta:** tecnologías y elementos clave, estado de partida, requerimientos técnicos mínimos de la solución.
3. **Modelo de gestión de los Derechos de Propiedad Intelectual relacionados con el proyecto.** Tipo de resultados, modelo para compartir resultados (royalties, etc.)
4. **Modelo de negocio para la comercialización de la solución**. Mercado estimado, estrategia de comercialización, canales de comercialización, acceso al mercado (del consorcio).
5. **Validación de la solución:** Nº de entidades públicas que participarán como usuarias. Descripción del entorno real en que se validará la solución.
6. **Propuesta de divulgación y difusión.** Actividades que se dedicarán a impulsar la cultura y el conocimiento de la ciberseguridad en el sector público y privado. Inversión (en €) en estas actividades.
7. **Descripción económica de la propuesta.** Volumen de inversión total. Volumen de inversión por fase. Co-financiación pública o privada. Modelo de comercialización futura de la solución (una vez concluya el contrato)

ANEXO 5: SOLUCIONES INFRAESTRCUTURAS Y EQUIPOS DE INCIBE

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Soluciones, infraestructuras y equipos de INCIBE** tiene por objetivo la creación de soluciones que permitan la innovación y mejora de las infraestructuras, los servicios y los equipamientos de INCIBE, y en concreto:

- La creación y desarrollo de un centro demostrador de tecnologías de ciberseguridad desarrolladas por empresas.
- Sistemas de inteligencia de Ciberamenazas
- Sistemas que permitan la prevención, predicción y detección temprana de ciberamenazas y ciberataques.
- Sistemas que permitan evitar que las ciberamenazas produzcan víctimas o, si no llegan a tiempo, que permitan identificar lo antes posible a las víctimas y las ciberamenazas que las han afectado, con el objeto de mitigar los daños.
- Sistemas que permitan a INCIBE conocer y mejorar la ciberseguridad de los ciudadanos y las empresas españolas, así como la generación de conocimiento para el mejor diseño de políticas y toma de decisiones.
- Sistemas de soporte a la respuesta a incidentes de ciberseguridad.
- Cualquier otra infraestructura, sistema o equipamiento que pueda ayudar a INCIBE a desarrollar su mandato o a alcanzar los objetivos de su Plan Estratégico.

La duración del proyecto será de entre 24 y 36 meses.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- Nº de soluciones creadas para INCIBE distinguiendo entre las orientadas a la mejora de servicios y aquellas orientadas a la mejora de equipamientos e infraestructura.
- Características, especificaciones y servicios relacionados con el centro demostrador creado.
- Nº de empresas desarrolladoras que muestran sus tecnologías en el centro demostrador.
- Nº de usuarios (empresas y colectivos de ciudadanos) atendidos en el centro demostrador.

Efectos e impactos.

- La mejora del equipamiento, infraestructuras y servicios públicos de INCIBE.
- La mejora de la ciberseguridad en las empresas españolas (desarrolladoras y usuarias).

- El impulso de soluciones nacionales capaces de ser competitivas a nivel internacional y, por tanto, de la industria española de la ciberseguridad.
- El impulso de la cultura y el conocimiento de la ciberseguridad en las empresas españolas y en la ciudadanía.
- La creación de empleo en el sector de la ciberseguridad.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- Las empresas pueden presentar tantas propuestas como deseen asociadas a las necesidades de INCIBE.
- Todo proyecto deberá dividirse en dos fases:
  - Fase 1: Creación de la Solución.
  - Fase 2: Demostración y validación de la Solución en un entorno real.
- Los proyectos deberán partir de TRL6 o TRL7 y finalizar en TRL 9.
- Las empresas deberán presentar un modelo de gestión de los resultados de los DPI derivados del proyecto, que incluya el modelo de comercialización de la solución más allá de INCIBE como usuario.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiará la creación de soluciones para las diferentes necesidades en equipamientos e infraestructuras de INCIBE. En función del número de propuestas presentadas se determinará el presupuesto de la licitación y la diferenciación por necesidades concretas. La inversión pública estimada se sitúa en 15,4 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

Las empresas que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

1. **Descripción de la solución propuesta:** tecnologías y elementos clave, estado de partida, requerimientos técnicos mínimos de la solución, orientación a las necesidades de INCIBE.
2. **Descripción del valor aportado a INCIBE por la infraestructura o equipamiento**.
3. **Modelo de gestión de los Derechos de Propiedad Intelectual relacionados con el proyecto.** Tipo de resultados, modelo para compartir resultados (royalties, etc.)

4. **Modelo de negocio para la comercialización de la solución**. Mercado estimado, estrategia de comercialización, canales de comercialización, acceso al mercado.
5. **Descripción económica de la propuesta, incluyendo todo el Ciclo de Vida de la infraestructura o equipamiento durante los próximos 10 años.** Volumen de inversión total. Volumen de inversión por fase. Propuesta de Ciclo de Vida.

ANEXO 6: SOLUCIONES FORMACIÓN

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Soluciones Formación** tiene por objetivo la creación de soluciones tecnológicas innovadoras **vinculadas a la formación o al desarrollo de capacidades y de habilidades de las personas** que permitan el desarrollo de perfiles cualificados en el sector de la ciberseguridad.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- Nº de soluciones creadas vinculadas a la formación.
- Nº de soluciones desarrolladas por PYMEs.

Efectos e impactos.

- La mejora en la orientación formativa y de empleo en ciberseguridad en instituciones educativas (institutos, centros de formación profesional, etc.).
- La mejora en la identificación del perfil de necesidades en ciberseguridad en jóvenes y profesionales.
- El desarrollo de perfiles cualificados en el sector de la ciberseguridad.
- La mejora de la ciberseguridad en las empresas españolas (y, especialmente en PYMEs)
- La creación de empleo en el sector de la ciberseguridad.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- Las empresas pueden presentar tantas propuestas como deseen asociadas a la actuación.
- Todo proyecto deberá dividirse en dos fases:
  - Fase 1: Creación de la Solución.
  - Fase 2: Demostración y validación de la Solución en un entorno real.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiará la creación de productos tecnológicos orientados a promover la formación o al desarrollo de capacidades y habilidades de las personas. En función del número de propuestas presentadas se determinará el presupuesto de la licitación. La inversión pública estimada se sitúa en 20 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

Las empresas que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

1. **Descripción de la solución propuesta:** tecnologías y elementos clave, estado de partida, requerimientos técnicos mínimos de la solución, orientación de la tecnología promover la formación y el desarrollo de capacidades y habilidades de las personas en ciberseguridad.
2. **Modelo de negocio para la comercialización de la solución**. Mercado estimado, estrategia de comercialización, canales de comercialización, acceso al mercado.
3. **Validación de la solución:** Descripción del entorno real en que se validará la solución.
4. **Descripción económica de la propuesta.** Volumen de inversión total. Volumen de inversión por fase. Co-financiación pública o privada. Resultados, efectos e impactos esperados.

ANEXO 7: PEQUEÑOS PROYECTOS

1. DESCRIPCIÓN DE LA ACTUACIÓN.

La actuación **Pequeños Proyectos** tiene por objetivo la creación de soluciones tecnológicas altamente innovadoras desarrolladas por PYMEs y emprendedores para aumentar y dinamizar las capacidades en ciberseguridad en cualquier de los ámbitos de actuación (sector público, PYMES o sectores estratégicos), así como la creación de tecnologías de base que puedan servir para la creación posterior de soluciones.

2. RESULTADOS, EFECTOS E IMPACTOS ESPERADOS.

Resultados (Outputs).

- Nº de PYMEs que realicen proyectos.
- Nº de nuevas empresas creadas.
- Nº de socios y capital aportado (en relación al capital total) por el equipo promotor en la creación de nuevas empresas.

Efectos e impactos.

- Creación de un tejido de PYMEs (y nuevas empresas) altamente innovadoras y personal altamente cualificado en el sector de la ciberseguridad.
- El impulso de la cultura y el conocimiento de la ciberseguridad en las PYMEs y empresas de nueva creación.
- La creación de empleo en el sector de la ciberseguridad, especialmente empleo cualificado en PYMEs.

3. REQUERIMIENTOS BÁSICOS.

Se consideran requerimientos básicos de esta actuación:

- El tamaño de los proyectos no podrá superar los 240.000 euros.
- Las empresas pueden presentar tantas propuestas como deseen asociadas a la actuación. En el caso de empresas de nueva creación, el equipo promotor (emprendedor) deberá demostrar su capacidad de gestión:
  - Competencias, formación y experiencia profesional previas, relacionadas con el proyecto.
  - Dedicación técnica y de gestión del equipo promotor al proyecto.
  - Grado de compromiso accionarial del equipo promotor.
  - Vinculación con algún centro de incubación/aceleración de empresas.

4. ORIENTACIÓN PRESUPUESTARIA.

Se financiará la creación de soluciones desarrolladas por PYMEs (y nuevas empresas) que impulsen las capacidades en ciberseguridad en los distintos ámbitos antes mencionados. En función del número de propuestas presentadas se determinará el presupuesto de la licitación, con la posibilidad de asignar una parte del presupuesto a PYMEs y otra a nuevas empresas. La inversión pública estimada se sitúa en 6,1 millones de euros.

5. CONTENIDO DE LA MEMORIA DETALLADA A PRESENTAR.

Las empresas que presenten propuestas en el marco de esta actuación deberán presentar una memoria detallada, de 20 hojas como máximo, con la siguiente estructura:

1. **Descripción de la solución propuesta:** tecnologías y elementos clave, estado de partida, requerimientos técnicos mínimos de la solución.
2. **Modelo de negocio para la comercialización de la solución**. Mercado estimado, estrategia de comercialización, canales de comercialización.
3. **Descripción de las características del equipo promotor (en el caso de empresas de nueva creación**). Formación, competencias, experiencia, compromiso accionarial, técnico y de gestión en la empresa, capital relacional (centros de emprendimiento, incubación/aceleración, relación con fondos de capital, otras fuentes de financiación, etc.)
4. **Descripción económica de la propuesta.** Volumen de inversión total. Resultados, efectos e impactos esperados.

León, 1 de Julio de 2021

DIRECTORA GENERAL

S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A.