Exp. CPP002/22

Documento Regulador de Compra Pública Precomercial

Servicios de I+D+i en materia de ciberseguridad (actuaciones 2, 3, 4, 5 y 7)

MRR C15.I7

ÍNDICE

ÍNDICE DE FIGURAS

No se encuentran elementos de tabla de ilustraciones.

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Este documento está estructurado en 5 apartados principales:

I. **INTRODUCCIÓN**. Pretende contextualizar la Iniciativa Estratégica de Compra de Innovación de INCIBE (en adelante, **IECPI**).
II. **REGULACIÓN DE LA CONTRATACIÓN**. Recoge aspectos claves de cómo se van a regular las actuaciones 2, 3, 4, 5 y 7 de la IECPI.
III. **PROCEDIMIENTO DE ADJUDICACIÓN**. Describe primero aspectos generales del proceso de adjudicación y recorre a continuación cada una de las fases importantes que se seguirán para adjudicar.
IV. **EJECUCIÓN DEL CONTRATO**. Se centra en regular cómo se va a ejecutar cada uno de los contratos que se celebren en el marco del presente documento regulador.
V. **ANEXOS**. Recogen todos los retos propuestos, modelos o plantillas para facilitar al licitador la entrega de documentación, el contenido de la Memoria técnica y los criterios evaluables.

1.1. Competencias y objetivos de INCIBE

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.
- Potenciar la industria española de ciberseguridad.
- Impulsar la I+D+i española en ciberseguridad.
- Identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad.

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 ciberseguridad, y promueve el avance de la cultura de la ciberseguridad a través de la concienciación, la sensibilización y la formación.
- Participa en proyectos complejos de diversa naturaleza con una fuerte componente innovadora y con capacidad para generar inteligencia en ciberseguridad que revierte 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.
- Coordina actuaciones y esfuerzos con el resto de los organismos públicos y privados, nacionales e internacionales, que trabajan en esta materia. A nivel nacional es un actor clave competente en el marco de ciberseguridad nacional recogido en la Estrategia Nacional de Ciberseguridad, destacando su colaboración activa con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) y con las Fuerzas y Cuerpos de Seguridad del Estado en la protección de las infraestructuras y en la lucha contra la ciberdelincuencia respectivamente.

La actividad de INCIBE se enmarca en las políticas públicas de ciberseguridad del Gobierno español. En particular, el nuevo Plan Estratégico 2021-2025 de INCIBE se alinea con la Agenda España Digital 2026, tanto en lo que respecta a sus contenidos, objetivos y metas, como a su plazo

temporal de ejecución; en concreto, en el eje estratégico número 3 Ciberseguridad: "Incrementar las capacidades de ciberseguridad en España, fomentar el desarrollo del ecosistema empresarial en este sector (industria, I+D+i y talento), y potenciar el liderazgo internacional del país en materia de ciberseguridad", donde expresamente a través de INCIBE se establecen medidas específicas:

- Fortalecimiento de la ciberseguridad de los ciudadanos, pymes y profesionales.
- Impulso del ecosistema empresarial del sector ciberseguridad.
- Despliegue y operación de centros de operaciones de ciberseguridad.

Y, de forma específica, la Estrategia Nacional de Ciberseguridad de 2019, cumpliendo el mandato recogido en su Objetivo 4, Línea de Acción 5 "Impulsar programas de apoyo de I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales **y mediante programas de Compra Pública de Innovación**", ha servido de base para formular los objetivos y acciones contemplados en el Plan Estratégico de INCIBE.

1.2. INCIBE en el Plan de Recuperación, Transformación y Resiliencia

INCIBE es el organismo encargado de gestionar las inversiones en ciberseguridad del Plan de Recuperación, Transformación y Resiliencia (Plan España Puede, en adelante **PRTR**) a través del Componente 15[1], Inversión 7: "Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, pymes y profesionales; e Impulso del ecosistema del sector". En este plan, se identifica a INCIBE como la entidad ejecutora de los fondos europeos destinados a este apartado del PRTR y concretamente de ejecutar las inversiones descritas a través de la **Compra Pública de Innovación**.

En concreto, el presente documento se enmarca dentro de la siguiente **JUSTIFICACIÓN**:

- Línea directriz del plan: Transformación digital.
- Componente 15: "Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G".
- Inversión 7: "Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, pymes y profesionales; e Impulso del ecosistema del sector" como una de las actuaciones concretas orientadas a desarrollar las capacidades de ciberseguridad tanto de ciudadanos como empresas y al impulso del ecosistema de ciberseguridad español en el marco de la estrategia de soberanía digital europea.
- Eje 2: "Impulso a la Industria".
- Pilares (1) Apoyo y fomento del emprendimiento; (2) Apoyo por la I+D+i en ciberseguridad como elemento transformador del país; (4) el desarrollo de iniciativas estratégicas de productos mínimos viables (en adelante, **MVP**) con alto impacto; (6) Impulso a la internacionalización; (7) Plataforma y repositorio de retos de la industria y Administraciones Públicas. Además; (8) Nuevas soluciones y prototipado en entornos de usuario final a través de la demanda sofisticada de ciberseguridad e incentivos de compra pre-comercial innovadora; (9) Creación de empleo investigador en empresa privada; (10) Impulso a *start-ups*.
- Financiación con cargo al Mecanismo para la Recuperación y Resiliencia (MRR).

De esta forma, la IECPI se alinea con el impulso de programas específicos que la Comisión Europea y el Gobierno de España desean dar a través de la inversión pública y la innovación, como

[1] Fuente: https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/05052021-Componente15.pdf

instrumentos fundamentales para afrontar los desafíos que plantean la recuperación, la transición ecológica y digital y la creación de una economía más resiliente en la Unión Europea.

OTRAS CONSIDERACIONES:

- Se aplican las particularidades del Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública (en adelante RD36/20) y para la ejecución del PRTR ya que el ámbito subjetivo (artículo 2.1) del RDL 36/20 se extiende a las entidades que integran el Sector Público de acuerdo con lo dispuesto en el artículo 2.1 de la Ley 40/2015, de Régimen Jurídico del Sector Público.
- En los procedimientos vinculados al PRTR se suprime la autorización del Consejo de Ministros prevista en el artículo 324 de la LCSP para los contratos y acuerdos marco de las entidades del Sector Público estatal que tengan la consideración de poderes adjudicadores cuando los mismos superen el umbral de 12 millones de euros o cuando el pago se concierte mediante arrendamiento financiero o arrendamiento con opción de compra y el número de anualidades supere cuatro años.
- Es obligación esencial del contratista colaborar con INCIBE para la consecución de los hitos, objetivos y carga justificativa que sea necesaria.
- No se acuerda la tramitación de urgencia.
- Se deja constancia de que en el expediente obrarán debidamente todas las Declaraciones de Ausencia de Conflicto de Intereses (en adelante, ***DACI***) cumplimentadas y firmadas por todos los intervinientes del Órgano de Contratación en el procedimiento de adjudicación.

En el mismo momento de la formalización del contrato o inmediatamente después, presentarán la oportuna DACI tanto el contratista como, si los hubiere, todos los subcontratistas. Asimismo, tanto contratista como subcontratistas vendrán obligados a incluir en el procedimiento las obligaciones de información detalladas en el art. 8.2 de la Orden HFP/1030/2021, de 29 de septiembre así como la información relativa a los titulares reales del contratista y subcontratista/s en los términos del artículo 10 de la Orden HFP/1031/2021, de 29 de septiembre.

Declaraciones:

1. DECLARACIÓN DE AUSENCIA DE DOBLE FINANCIACIÓN

INCIBE declara expresamente que este contrato no ha percibido ninguna otra ayuda con cargo al presupuesto de la UE.

2. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO

INCIBE se compromete a adoptar cuantas medidas de información, comunicación y visibilidad del proyecto sean requeridas por la normativa comunitaria y en particular por el artículo 9 de la Orden HFP/1030/2021, de 29 de septiembre y por el resto de medidas que resulten de obligado cumplimiento para las actuaciones y proyectos financiados con cargo al Mecanismo de Recuperación y Resiliencia.

3. ADOPCIÓN DE MEDIDAS ADECUADAS Y PROPORCIONADAS DE PREVENCIÓN CONTRA EL FRAUDE

INCIBE en la preparación, tramitación y adjudicación del presente contrato ha adoptado y adoptará medidas adecuadas y proporcionadas de prevención contra el fraude.

4. DECLARACIÓN DE AUSENCIA DE CONFLICTO DE INTERESES

INCIBE declara que, en la preparación, tramitación y adjudicación del presente contrato, se han adoptado y se adoptarán las debidas precauciones que garantizan la prevención de los conflictos de interés, conforme al considerando 104 y al artículo 61 del Reglamento Financiero de la UE y conforme a lo dispuesto a estos efectos en la Instrucción de 23 de diciembre de 2021 de la Junta Consultiva de Contratación Pública del Estado.

En particular, el personal que participa en esta licitación por parte del organismo interesado, es conocedor de que no se consideran admisibles los intentos de influir indebidamente en el presente procedimiento de adjudicación u obtener información confidencial.

Los evaluadores que formen parte del órgano de asistencia realizarán declaración expresa de no estar afectados por las situaciones de conflicto de interés en los términos previstos en el apartado 3 del artículo 61 del Reglamento Financiero de la UE.

5. ACEPTACIÓN DE LOS PRINCIPIOS DE BUENA GESTIÓN FINANCIERA

INCIBE declara expresamente que ha observado en la preparación y tramitación de este contrato y se compromete a observar durante la adjudicación y ejecución del mismo los principios de buena gestión financiera y acepta someterse a las actuaciones de control que sean de aplicación a las ayudas conforme a la normativa comunitaria.

6. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN

INCIBE conoce que debe conservar la información del expediente de contratación por el plazo de disponibilidad que establece la normativa comunitaria (artículo 132 del Reglamento Financiero).

Asimismo conoce que se encuentra sujeta a los controles de la Comisión Europea, la Oficina de Lucha Antifraude, el Tribunal de Cuentas Europeo y la Fiscalía Europea y el derecho de estos órganos al acceso a la información sobre el contrato.

7. PRINCIPIO DO NO SIGNIFICANT HARM

El órgano de contratación declara que respecto a la ejecución del contrato ha tenido en consideración los posibles perjuicios a los objetivos medioambientales del artículo 17 del Reglamento UE nº 2020/852 del Parlamento Europeo y del Consejo de 18 de junio de 2020, relativo al establecimiento de un marco para facilitar las inversiones sostenibles, sin que estos resulten afectados por el presente contrato.

1.3. Contexto actual de ciberseguridad y posicionamiento de España

En marzo de 2021, los ministros de la UE adoptaron el "Proyecto de Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital"[2], que habían presentado la Comisión Europea y el Alto Representante de la UE para Asuntos Exteriores y Política de Seguridad el 16 de diciembre de 2020. En las conclusiones se señala que la **ciberseguridad** es esencial para construir una Europa resiliente, ecológica y digital, y se fija como objetivo clave lograr la autonomía estratégica preservando al mismo tiempo una economía abierta. Para ello es necesario aumentar la capacidad de adoptar decisiones autónomas en el ámbito de la ciberseguridad con el objetivo de reforzar el liderazgo digital y las capacidades estratégicas de la Unión Europea.

Adicionalmente, el "Índice de Ciberseguridad Global (ICG)"[3] publicado el pasado julio de 2021 presentó la mejora de posición de España en el *ranking* de ITU, donde se pasa de ocupar el séptimo puesto en el 2018 al cuarto en 2020 a nivel mundial, y el 2º a nivel de la Unión Europea, solo detrás de Estonia. En el informe de ITU, se presentan los **programas de I+D como una de las medidas impulsoras para desarrollo de capacidades en ciberseguridad.** También se incluye en el mismo informe al Foro Económico Mundial identificando que "aproximadamente un millón de personas se conectan a Internet por primera vez cada día y dos tercios de la población mundial posee un dispositivo móvil". La digitalización aporta beneficios económicos y sociales, pero los riesgos pueden contrarrestar los beneficios. Asegurar el ciberespacio a través de actividades de capacitación en

[2] Fuente: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/es/pdf

[3] Fuente: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

ciberseguridad es clave, ya que contribuye a reducir problemas como la brecha digital y los ciber-riesgos.

En este contexto internacional, se desarrolla la Iniciativa Estratégica de Compra Pública de Innovación (en adelante IECPI).

1.4. IECPI

La IECPI está dotada con un presupuesto global de 224 Millones de euros, con esta dotación pretende realizar un conjunto de siete actuaciones dirigidas a impulsar la I+D+i y la creación de productos y soluciones en el ámbito de la ciberseguridad, a través de la Compra Pública de Innovación.

El presente documento regulador establece las condiciones que regularán la contratación vinculada en concreto a las actuaciones 2, 3, 4, 5 y 7, de acuerdo con el siguiente esquema:

Actuación	Objetivos
2	Soluciones tecnológicas para la ciberseguridad en las pymes.
3	Soluciones tecnológicas de ciberseguridad para sectores estratégicos.
4	Soluciones tecnológicas a retos del Sector Público.
5	Soluciones que permitan la innovación y mejora de las infraestructuras y los equipamientos propios de INCIBE.
7	Pequeños proyectos altamente innovadores en ciberseguridad desarrollados por pymes o por emprendedores.

Tabla 1: Actuaciones y objetivos

Los proyectos se ejecutarán completamente antes del 30 de Junio de 2026. Los proyectos deberán partir desde un *Technology Readiness Level* (en adelante, **TRL**) inferior a 6, llegar al menos a TRL 7 y no superar el TRL 8[4].

Finalmente, los contratistas podrán explotar los resultados desarrollados, pero compartirán los beneficios derivados de los mismos con la entidad contratante, redundando en un importante beneficio para el Sector Público y sector privado español, tal y como se concreta en el presente documento regulador.

1.5. Consulta Preliminar al Mercado

El 1 de julio de 2021, INCIBE publicó en su página web una consulta al mercado con el fin de conocer las propuestas de proyectos concretos en cada una de las siete actuaciones para elaborar un Mapa de Demanda Temprana. Este mapa recoge un listado de necesidades sin solución actual en el mercado en materia de ciberseguridad e identifica las actuaciones, instrumentos y posibles proyectos a licitar mediante Compra Pública de Innovación.

Esta consulta al mercado tenía por objeto:

- Informar al mercado de las actuaciones que se impulsarán a través de la Compra Pública de Innovación.

[4] Según la descripción dada en el presente documento de licitación. Solo podrá abordarse cuestiones sobre operativa y fabricación. La construcción de varias copias una vez ensayado con éxito el prototipo original no constituye I+D. No abarca en ningún caso acciones para el desarrollo comercial como la producción o el suministro a gran escala para determinar la viabilidad comercial o recuperar los gastos de I+D, la integración o la adaptación y los ajustes y la mejoras añadidos a productos o procesos existentes.

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

La consulta inicial recibió 281 propuestas para el total de las actuaciones. A través de las propuestas recibidas, INCIBE pudo conocer en una primera aproximación el eventual interés de los operadores económicos en la participación en las presentes actuaciones, propuestas de posibles proyectos de I+D, así como la capacidad del mercado para lograr los resultados que se esperan de ella, que son:

- Obtención de un número llamativo de productos en TRL 6, 7 y 8 de cara a su futura comercialización.
- Movilización de cofinanciación privada, de manera que la empresa promotora e INCIBE compartan los riesgos de los proyectos I+D.

El informe de la Consulta Preliminar al Mercado, en lo referente a las actuaciones indicadas, se encuentra publicado en la página web de INCIBE y en el perfil del contratante de INCIBE en la Plataforma de Contratación del Sector Público.

2. REGULACIÓN DE LA CONTRATACIÓN

Este apartado regula la contratación vinculada a las actuaciones 2, 3, 4, 5 y 7 de la IECPI.

2.1. Definiciones aplicables al documento regulador

Adjudicatario	Licitador que ha presentado una de las mejores propuestas, cumpliendo todos los requisitos de la licitación y es aceptado por el Órgano de Contratación para ejecutar la prestación de servicios objeto del contrato.
Características técnicas	Se corresponden a aquellos resultados que generen derechos de propiedad y que incluyen todos los elementos (estructurales, tecnológicos o funcionales) de un producto o servicio que contribuyen a dar solución a un problema técnico.
Comprador	Entidad contratante, S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE).
Compromisos posteriores	Todos aquellos compromisos adquiridos por los contratistas y la entidad contratante, en virtud de lo establecido en el contrato, en el presente documento regulador del procedimiento o en la propuesta final de los contratistas, cuya duración supera la de la prestación de servicios, como por ejemplo los derivados del apartado de derechos de propiedad industrial e intelectual.
Conocimientos previos	Cualesquiera patentes, marcas, conocimientos, información y/o experiencia, que hayan sido adquiridos y/o desarrollados por su titular de manera independiente con anterioridad a la adjudicación del contrato. Incluyen, por tanto, todos los derechos de propiedad intelectual prexistentes.
Contratista	Adjudicatario que ya ha perfeccionado el contrato con el Órgano de Contratación y que puede comenzar la prestación de servicios objeto del contrato.
Contrato para el desarrollo precomercial	El contrato de servicios de I+D que se firmarán entre INCIBE y cada adjudicatario, cuyo objeto será la ejecución de un proyecto de I+D por parte del adjudicatario que dé respuesta a algunos de los retos planteados por INCIBE. En adelante, **el contrato**.
Derechos de acceso	Se refiere a los derechos de uso de los resultados y/o de los conocimientos previos bajo los términos y condiciones establecidos en el contrato y en el documento regulador. En especial y de forma no limitante, aquellos derechos de uso de los resultados y/o de los conocimientos previos que resulten imprescindibles para el desarrollo de los servicios de I+D, así como para la obtención y/o explotación de los productos desarrollados.
Derechos de explotación	Se refiere a los derechos de uso, desarrollo, fabricación, venta, importación, exportación, distribución, publicidad, suministro, ofrecimiento en el mercado, uso industrial o comercial de los resultados o mediante cualquier otra forma de explotación de estos prevista en la Ley de Propiedad Intelectual.
Derechos de propiedad	Se refiere a los derechos de propiedad intelectual y/o industrial generados en relación con los productos desarrollados en la prestación de servicios de I+D objeto del contrato.

Documento descriptivo de retos	Anexo 1 al documento regulador que describe, a alto nivel, las necesidades que INCIBE quiere resolver mediante los contratos de desarrollo precomercial.
Efectos técnicos	Se corresponden a aquellos resultados que no generando derechos de propiedad describen y permiten generar determinadas características técnicas sobre un producto o servicio con el fin de solucionar un problema técnico. Un mismo efecto técnico puede ser alcanzado con diferentes características técnicas, no limitándose la solución del problema técnico a una o un conjunto de estas características.
Licitador	Es quien presenta su oferta en el proceso de contratación.
Operador económico	Operador económico, o agrupación de varios operadores económicos, que presenta oferta al procedimiento regulado en el presente documento.
Perfeccionamiento	Se refiere a cualquier modificación y/o nuevo desarrollo que surja a partir de los resultados. De forma más específica, aunque no limitante, se refiere a cualesquiera invenciones, descubrimientos, procesos, usos, protocolos o desarrollos que surjan como resultado del desarrollo del proyecto o los resultados y que constituya una mejora o avance sobre los mismos.
Perfeccionamiento del contrato	Momento del procedimiento en el que el adjudicatario y el Órgano de Contratación redactan y firman el contrato de prestación de servicios del primero al segundo, pudiendo concretar algunos detalles de estos, sin vulnerar en ningún momento lo establecido en el presente documento regulador del procedimiento ni en la propuesta final de la persona adjudicataria.
Persona filial, afiliada o subsidiaria	Se refiere a cualquier entidad legal bajo el control directo o indirecto de las personas contratistas, entendiéndose 'control' como alguno de los siguientes: - Tener directa o indirectamente el 50% o más del valor nominal del capital de la entidad legal en cuestión. - Tener la mayoría de los derechos de voto de los accionistas o asociados de esa entidad. - Tener la propiedad, directa o indirecta, de hecho, o legalmente, de los poderes de toma de decisión en dicha entidad legal. - Tener la facultad de designar o cesar a los administradores sociales. (art. 42 Código de Comercio)
Persona sublicenciataria	Se refiere a cualquier tercero al que hayan sido transmitidos algunos o todos los derechos de las personas contratistas en los términos referidos en este contrato.
Porcentaje de coinversión	Porcentaje del presupuesto del proyecto que es financiado directamente por el licitador y en caso de ser aceptada y mejor valorada la propuesta contratista.
Porcentaje de *royalties*	Porcentaje calculado sobre la base del presupuesto del proyecto que el contratista desembolsará durante los 5 años posteriores a la finalización de éste, a INCIBE, en los términos establecidos en el apartado de Derechos de Propiedad Intelectual e Industrial, como pago de la licencia que INCIBE emitirá a su favor para la explotación de los resultados obtenidos. Durante cada uno de los 5 años posteriores el adjudicatario desembolsará la quinta parte del porcentaje ofertado.

Presupuesto de un proyecto	Importe a valor de mercado, incluyendo todos los impuestos aplicables, que es necesario para la correcta ejecución de un proyecto individual. El presupuesto se dividirá en dos partidas, la inversión que realizará INCIBE para financiar el mismo a través del contrato y la coinversión aportada por el licitador.
Procedimientos de control, seguimiento y evaluación	Conjunto de procedimientos que permitirán a la dirección del proyecto por parte de INCIBE, la valoración y toma de decisiones técnicas, el seguimiento del proyecto y de los compromisos de cada adjudicatario.
Proyecto	Se aplicará la definición de la norma UNE 166000:2006 sobre Terminología y definiciones de las actividades de I+D+i., que servirá a efectos interpretativos en caso de dudas no cubiertas en el presente documento.
Resultado(s)	Se refiere a cualquier efecto y característica técnica generada en el ámbito de un proyecto objeto de la presente licitación que dé lugar a un **producto**, **proceso**, **servicio** o uso que dé respuesta a un problema técnico. También se incluye en esta definición cualquier producto que los incorpore o derive de forma obvia de los mismos, que puedan comercializarse como productos, servicios y/o *know-how* asociado a los mismos. El resultado se espera que sea innovador, o que se trate de mejoras sustancialmente significativas de los productos, procesos o servicios ya existentes. Nótese, y atendiendo al contenido de la UNE 166000:2006, que se podrá entender también como producto a un servicio, ***software***, ***hardware*** o **material** y se considera que la innovación de un producto podrá descansar sobre uno o varios de los anteriores elementos.
Sublicencia	Se refiere a la autorización de uso concedida por los contratistas a terceros, por los que estos adquieren algún derecho de explotación sobre los resultados. Como excepción, los acuerdos referidos exclusivamente a la distribución y comercialización en nombre de los contratistas de los resultados que los contratistas celebren con terceros no entran dentro de esta definición.
Tercero	Se refiere a cualquier persona física o jurídica distinta de las personas contratistas y de la entidad contratante.
Usuarios finales	INCIBE y otros organismos y entidades del Sector Público o privado que puedan beneficiarse en el futuro de los resultados de los proyectos de I+D contratados.
Usuarios finales aportados por el licitador y en su caso, adjudicatario y/o contratista	Organismos y entidades del Sector Público o privado que puedan beneficiarse en el futuro de los resultados de los proyectos de I+D contratados, que el licitador se comprometa a aportar en su oferta y que, en caso de resultar adjudicatario y contratista, evaluarán el resultado del proyecto que desarrolle el propio adjudicatario.
Usuarios finales aportados por INCIBE	INCIBE y otros organismos y entidades del Sector Público o privado que puedan beneficiarse en el futuro de los resultados de los proyectos de I+D contratados, que el propio INCIBE podrá incorporar durante la adjudicación y ejecución de los contratos para que le asesoren en la evaluación de las ofertas y en su caso, proyectos desarrollados.

Valor económico del contrato	Es la suma de todas las aportaciones económicas que tanto INCIBE como el contratista realizarán para cumplir los compromisos adoptados en el presente documento regulador y en la propuesta que resulte adjudicataria que serán llevados al contrato. Se compondrá de la suma de las siguientes partidas: - Inversión INCIBE: La inversión que realizará INCIBE para financiar el proyecto. - Coinversión del adjudicatario: La coinversión que realizará el adjudicatario para financiar el proyecto de I+D. Corresponderá a la aplicación del porcentaje de coinversión al presupuesto del proyecto. - *Royalties*: Suma de los pagos que realizará el adjudicatario a INCIBE, en los 5 años posteriores a la finalización del proyecto, en concepto de licencia. Corresponderá a la aplicación del porcentaje de *royalties* al presupuesto del proyecto.

2.2. Régimen jurídico

2.2.1. Régimen jurídico del contrato

Todo el procedimiento de licitación y adjudicación desarrollado en este documento y el contrato o contratos resultantes se regirán por la legislación española.

La presente licitación y la ejecución de los contratos que resulten de ella estarán también sujetos a las disposiciones del Tratado de la Unión Europea, del Tratado de Funcionamiento de la Unión Europea y a los actos fijados en virtud de estos que resulten de aplicación, así como al Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia.

En lo que resulte aplicable, se estará sujeto a lo mencionado en el apartado *1.2* y en el *2.2*, tanto en lo referente a las **JUSTIFICACIÓN** como a las **OTRAS CONSIDERACIONES** desglosadas en dicho apartado.

Por tanto, el presente procedimiento y la ejecución de los subsiguientes contratos se regirá por la normativa europea y española que regule el funcionamiento del Mecanismo de Recuperación y Resiliencia y la ejecución del Plan de Recuperación, Transformación y Resiliencia, **siendo obligación esencial del contratista colaborar con INCIBE para la consecución de los hitos, objetivos y carga justificativa que sea necesaria**. Especialmente, en lo relativo a la aplicación de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia y la Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.

En el caso de que la financiación propuesta para los proyectos I+D tenga en algún momento origen en otros fondos, los contratistas estarán obligados, adicionalmente, al cumplimiento de la normativa por la que se rijan dichos fondos, velando y asegurando la compatibilidad entre todos los fondos empleados, habiendo analizado todas las posibles incompatibilidades.

El contrato constituye la contratación de servicios de investigación y desarrollo en los que:

1. Los beneficios no pertenecerán exclusivamente al comprador para su utilización en el ejercicio de su propia actividad.
2. El servicio prestado no es remunerado íntegramente por el poder adjudicador.

Ambos extremos se pueden comprobar a lo largo de todo el documento regulador, especialmente el punto 1 en el apartado de 4.8 Derechos de propiedad intelectual e industrial y el punto 2 en los distintos apartados donde se hace referencia a la coinversión por parte del contratista y el pago por royalties.

En consecuencia, la presente contratación está excluida del ámbito de aplicación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (en adelante LCSP), de acuerdo con lo previsto en su artículo 8 así como en el artículo 17 de la Directiva 2014/24/UE del Parlamento europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE.

Quedando excluido del ámbito de aplicación de la LCSP, el presente documento se regirá por el contenido del presente documento, que contiene los pactos y condiciones definitorias de los derechos y obligaciones que asumirán la entidad contratante, los licitadores, y en su momento, la o las empresas adjudicatarias, y en su caso, contratistas.

No obstante, para regular aspectos concretos de la contratación se podrá hacer una remisión expresa a los artículos de la LCSP y su normativa de desarrollo que establezcan condiciones que sean de aplicación, entendiéndose dicha remisión de carácter restrictivo, siendo sólo aplicables aquellos artículos que se hayan referido expresamente con objeto de simplificar los requisitos y facilitar la presentación de las propuestas adecuándolas a las prácticas habituales en la contratación pública.

El procedimiento de contratación deberá desarrollarse, en su caso, respetando los principios de contratación establecidos en el artículo 1 apartado 1 de la LCSP.

La competencia de INCIBE para la formalización de los contratos se rige por lo dispuesto en los estatutos sociales de INCIBE, que concretamente establecen como objeto social: *"[…] la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. La Sociedad podrá desarrollar las actividades integrantes del objeto social, total o parcialmente, de modo indirecto o mediante la titularidad de acciones y/o participaciones en Sociedades con objeto idéntico o análogo*".

El contrato tiene naturaleza privada y, por tanto, aplicarán a su cumplimiento, efectos y extinción las normas aplicables de derecho privado. En caso de discordancia entre el presente documento regulador con cualquiera del resto de documentos contractuales, prevalecerá el presente documento regulador. Las partes quedan sometidas expresamente a lo establecido en este documento, que tiene carácter contractual, por lo que deberá ser firmado, en prueba de conformidad por el o los contratistas, en el mismo acto de formalización del contrato. El desconocimiento del presente documento regulador, del contrato, de sus documentos anexos o de las instrucciones o normas de toda índole aprobadas por la Administración que puedan aplicarse en la ejecución de lo pactado, no eximirá al contratista de la obligación de su cumplimiento. El contrato remitirá a las clausulas jurídicas previstas en el documento regulador recogiendo las condiciones específicas de la propuesta que se contrata.

2.2.2. Seguimiento de las recomendaciones de la Comisión Europea para la Compra Precomercial

2.2.2.1. Marco de Ayudas de Estado a la I+D+i

En el diseño del presente documento regulador se ha seguido escrupulosamente lo indicado en los artículos 32 y 33 de la Comunicación de la Comisión Europea 2014/C 198/01 sobre el Marco sobre ayudas estatales de investigación y desarrollo e innovación, de tal manera que no es necesario que el Estado español se base en una evaluación individual de las condiciones de los contrato entre el comprador público (INCIBE) y las empresas adjudicatarias, ni es necesario notificar una ayuda estatal de I+D+i de conformidad con el artículo 108, apartado 3, del Tratado.

Concretamente, se establece en el presente documento regulador:

1. El precio que se pagará por los servicios refleja plenamente el valor de mercado de los beneficios recibidos por el comprador público y los riesgos asumidos por los licitadores que resulten contratistas.
2. El procedimiento de selección es abierto, transparente y no discriminatorio y está basado en criterios objetivos de selección y adjudicación especificados en el documento regulador antes de que comience el procedimiento de licitación.
3. La descripción de todos los derechos y obligaciones de las partes, incluso con respecto a los derechos de propiedad intelectual e industrial, estando a disposición de todos los licitadores interesados antes del procedimiento de licitación a través del presente documento regulador.
4. Que la contratación no otorgará a ningún licitador trato preferente en el suministro de volúmenes comerciales de los productos o servicios finales a un comprador público en España.
5. Se incluye la obligatoriedad de que todos los proyectos cuenten con usuarios finales para las pruebas y valoraciones de los prototipos. Y la evaluación de los usuarios finales será tenida en cuenta para los cambios de etapa que permitan avanzar en el desarrollo de los proyectos y su valoración final.
6. Se dará amplia difusión a todos los resultados que no generen derechos de propiedad intelectual, por ejemplo, mediante la publicación, la enseñanza o la contribución a organismos de normalización de manera que permita a otras empresas reproducirlos.
7. Que el contratista al que se ceden los resultados que generen derechos de propiedad intelectual concede al comprador público acceso ilimitado a dichos resultados gratuitamente, y está obligado a conceder acceso a terceros mediante licencias no exclusivas, en condiciones de mercado.

2.2.2.2. Otras comunicaciones de la Comisión Europea en materia de compra precomercial

En la elaboración del presente documento regulador, se han seguido las recomendaciones de las siguientes Comunicaciones de la Comisión Europea:

- **SEC(2007) 1668**, "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La contratación precomercial: impulsar la innovación para dar a Europa servicios públicos de alta calidad y sostenibles" **y concretamente** el "*Ejemplo de un posible enfoque para la contratación pública de servicios de I+D aplicando la distribución de riesgos y beneficios en condiciones de mercado, es decir, contratación precomercial* ***{COM(2007) 799 final}***" y el "Dictamen del Comité Económico y Social Europeo sobre la «Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Regiones — La contratación precomercial: impulsar la innovación para dar a Europa servicios públicos de alta calidad y sostenibles» **(2009/C 100/02)**"
- **(2021) 4320 final**, "Comunicación sobre Orientaciones sobre la contratación pública en materia de innovación".

Entre los muchos principios de las citadas comunicaciones, en el presente documento regulador cabe destacar:

1. La compartición y reparto de riesgos y beneficios entre comprador y prestador del servicio.
2. El establecimiento de etapas en la ejecución de los proyectos de I+D y la evaluación de los resultados alcanzados en cada etapa, existiendo la posibilidad de dar por finalizados proyectos de I+D si los resultados de una etapa no son exitosos. También la posibilidad de que sólo los adjudicatarios con resultados más prometedores avancen de unas etapas a otras.

3. La separación de la etapa de I+D del despliegue de volúmenes comerciales de productos finales (que no es objeto del presente documento regulador).
4. Las medidas para promover la participación de pymes, *start-ups* y Organismos de Investigación.
5. El establecimiento de retos que conlleven la mejora de la eficiencia y eficacia de los servicios públicos que presta INCIBE.
6. El diseño de retos que tengan más usuarios potenciales que el propio INCIBE e incluso que el propio Sector Público.
7. El incentivo para conservar en todos los casos, a dos operadores económicos en las últimas etapas de los proyectos de I+D para evitar potenciales situaciones de restricción de operadores futuros en el mercado en fase de comercialización de los resultados.
8. El uso de la Consulta Preliminar al Mercado.
9. La observancia de los principios de transparencia, concurrencia y no discriminación en todo el proceso de contratación.
10. La comprobación por parte del comprador de la naturaleza mayoritaria de I+D de los servicios contratados.
11. La comprobación por parte del comprador de que los servicios se compran a valor de mercado y al mismo tiempo que se obtiene una reducción de precios respecto al coste de desarrollo exclusivo que refleje el valor de mercado de los beneficios recibidos y los riesgos asumidos por el prestador del servicio, mediante las coinversiones y pagos por royalties que realizará el contratista.
12. La inclusión de criterios de adjudicación relacionados con el impacto socioeconómico, no sólo en los servicios públicos, de los resultados y de los propios servicios contratados.
13. La inclusión de rangos de precios en el documento regulador para extraer las mejores ofertas a precios de mercado.
14. Las recomendaciones en materia de gestión de los Derechos de Propiedad Intelectual e Industrial del contrato, en concreto mediante la otorgación al comprador público de derechos suplementarios que eviten la dependencia de determinados proveedores y garanticen el acceso futuro a una cadena de suministro suficientemente competitiva, a través de:
    a. El hecho que el comprador público exige al contratista que conceda (o, en caso de que el contratista no lo haga, a conceder él mismo) licencias a terceros para explotar los resultados para el comprador (es decir, para prestar el servicio innovador o fabricar el producto innovador para el comprador) en unas condiciones justas, transparentes, razonables, proporcionadas y no discriminatorias.
    b. El hecho de que si el contratista utiliza los resultados de forma indebida en perjuicio del interés público o no procede a su explotación comercial antes de 1 de enero de 2028, el comprador puede reservarse el derecho a exigir al contratista, previa consulta de los motivos por los que no ha iniciado la explotación, que le transfiera la titularidad de los resultados (incluidos los Derechos de Propiedad Intelectual e Industrial) derivados del contrato (la denominada 'cláusula de avocación').
    c. El hecho de que si se desea dar a los resultados un uso más amplio que no se limite a los beneficiarios definidos en el contrato o si es importante garantizar la interoperabilidad o interconectividad con otros sistemas del mercado, se pueden contemplar en el contrato el derecho del comprador público o la obligación del contratista a contribuir a la normalización (durante la vigencia del contrato o tras su finalización) o a publicar resúmenes de los resultados (sin perjuicio de una adecuada protección de los Derechos de Propiedad Intelectual e Industrial).
15. Se ha tenido en cuenta en el valor del contrato los costes y las responsabilidades derivados de asegurar y preservar los derechos de la propiedad intelectual (por ejemplo, los costes de registro y mantenimiento o responsabilidades como pleitos y conflictos como titular con los proveedores).
16. El acceso gratuito por parte del comprador público de los Derechos de Propiedad Intelectual e Industrial preexistentes necesarios para la correcta ejecución de los servicios de I+D.

2.2.3. Jurisdicción competente y recursos

Las decisiones, asuntos o discrepancias relativos al presente documento regulador, al procedimiento de adjudicación, y a la ejecución, efectos y extinción del contrato y los proyectos de investigación y desarrollo en él comprendidos, quedarán sujetas al derecho privado español y, en especial al Código Civil español, sin perjuicio de la aplicación de los principios antes indicados para la adjudicación contenidos en la LCSP.

A los efectos de lo indicado en el apartado anterior, los licitadores en el procedimiento por el hecho de su participación y el adjudicatario o los adjudicatarios que formalicen los contratos se someten expresamente a la jurisdicción de los juzgados y tribunales del orden civil de la ciudad de León, sede de INCIBE salvo para los supuestos en que la ley establezca por razón de la materia otro fuero imperativo.

2.3. Objeto del contrato

El objeto del presente contrato es la contratación de servicios de I+D (compra pública precomercial) a varios operadores económicos (o agrupaciones de operadores económicos) en un marco en el que el comprador y el prestador del servicio, compartirán, como se ha indicado anteriormente, riesgos y beneficios, atendiendo entre otras cuestiones, a lo que se regula en el apartado de derechos de propiedad intelectual e industrial.

Cuestiones a tener en cuenta:

- Los servicios de I+D contratados se agruparán en forma de proyectos individuales de I+D que deberán dar respuesta a los retos planteados en el *ANEXO 1. Retos* del presente documento regulador.
- Los proyectos contribuirán a las Actuaciones 2, 3, 4, 5 o 7 en la medida que se ha definido en el *ANEXO 1. Retos*.
- Los proyectos de I+D deberán dar como resultado, una serie de activos que no estén disponibles actualmente en el mercado y que se pretende sean generados por los contratistas, en beneficio de INCIBE y directa o indirectamente, del Sector Público y privado en España y en Europa, según lo que se regula en el apartado de derechos de propiedad intelectual e industrial.
- INCIBE podrá ser propietario de los productos cubiertos por el contrato (por ejemplo, prototipos o productos primeros de prueba desarrollados durante el proyecto), siempre que el valor de esos productos no supere el valor de los servicios de investigación y desarrollo comprendidos en el contrato y sin perjuicio de lo establecido en el apartado de derechos de propiedad intelectual e industrial, especialmente en lo relativo a la explotación de los resultados. Se pretende así acortar el tiempo de llegada al mercado y fomentar la aceptación en los mercados de estas nuevas soluciones.
- Los servicios de I+D contratados se englobarán fundamentalmente entre TRL menores que 6 (como situación de partida) y TRL 7-8 (como situación de llegada) según la definición adjunta en el *ANEXO 10. TRL de la IECPI*. Dichos servicios se desarrollarán en tres etapas[5].
- Asimismo, se involucrará en la validación de los resultados al final de cada etapa, a potenciales usuarios finales de los desarrollos contratados, bien aportados por el adjudicatario o por el propio INCIBE. Dependiendo de quién los aporte, sus funciones podrán ser distintas, como así lo establece en el presente documento regulador.

[5] El proceso de licitación se divide en fases. Para evitar confusiones, durante la ejecución las diferentes fases se denominan etapas.

- 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, para lo que en su caso deberá recurrirse en su día a procedimientos de contratación independientes para la adquisición, en los que los contratistas del presente procedimiento no podrán tener ventaja alguna. **En consecuencia, el contrato no incluirá la producción comercial o venta de los productos terminados, ni actividades por tanto vinculadas al paso del TRL 8 al 9 de las soluciones desarrolladas**. Todo ello sin perjuicio de los derechos de uso o explotación que se reserva INCIBE de acuerdo con lo establecido en el presente documento regulador.
- Será obligatorio que el licitador aporte una carta de compromiso de al menos un usuario final en su oferta, para que dicha oferta sea objeto de valoración.
- El desarrollo de cada uno de los retos será cubierto por un **mínimo de dos contratistas** con ofertas y proyectos independientes entre sí.
- INCIBE podrá ir **reduciendo al final de cada etapa el número de contratistas por reto**, siguiendo el procedimiento establecido en el presente documento regulador, manteniendo siempre al menos dos contratistas por reto, salvo en aquellos casos que tras la finalización de la primera o segunda etapa INCIBE decida que ningún contratista cambie de etapa.
- El resultado de los proyectos será diseñado, desarrollado y probado teniendo en cuenta los requisitos no funcionales (seguridad, mantenibilidad, disponibilidad, rendimiento, interoperabilidad, accesibilidad y usabilidad).

2.4. Presupuesto del contrato

El presupuesto de los proyectos deberá ser tal que la inversión de INCIBE esté comprendida entre un mínimo de 300.000 € + IVA y un máximo de 1.500.000 € + IVA salvo para los retos con presupuesto inferior a 3.000.000 € en cuyo caso la aportación máxima de INCIBE será de la mitad del presupuesto del reto. El detalle de la información se encuentra en ANEXO 6.

El presupuesto máximo de la Etapa 1 del contrato será de 25.000 €+IVA.

El coste de las pruebas realizadas por usuarios finales aportados por el contratista formará parte del presupuesto de la oferta, sin embargo, el coste de las pruebas a realizar por usuarios finales exigidos por INCIBE podrá ser financiado:

a) Mediante una modificación del valor económico del contrato, tal y como se establece en el apartado 4.2.3 Modificaciones del contrato o del proyecto.
b) Por el propio INCIBE en contrato aparte al regulado en el presente documento.

2.5. Otras características de la contratación

2.5.1. El Órgano de Contratación

El Órgano de Contratación de la presente licitación será la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A (INCIBE).

Domicilio: Avenida José Aguado, 41 24005 León.

Teléfono. (+34) 987 877 189

Fax. (+34) 987 261 016

contratacion@incibe.es

Entidad del Sector Público con la condición de Poder Adjudicador que no es Administración Pública.

2.5.2. Presupuesto de la licitación

El presupuesto máximo de la presente contratación es de 137.200.000,00 euros (IVA excluido). El presupuesto máximo con IVA es de 166.012.000 euros.

El presupuesto máximo para cada uno de los retos, y que será la cantidad máxima que INCIBE invierta en cada reto, viene detallado en el *ANEXO6: Presupuesto máximo por reto*.

2.5.3. Plazo de duración

La **duración máxima de los servicios de I+D**, será desde el día siguiente a la formalización del contrato hasta el 30 de junio de 2026. Los proyectos podrán tener una duración menor, de acuerdo con la planificación que se oferte o se determine durante la ejecución del contrato. **No se prevén prórrogas** en cuanto a este plazo, salvo que INCIBE indique lo contrario durante la ejecución de éste.

La duración de los contratos será tal que cubra el plazo para ejecutar todos los compromisos adquiridos por el contratista, incluido el cierre administrativo del proyecto y su carga justificativa necesaria por el uso de fondos PRTR, y especialmente los compromisos asumidos en relación con los derechos de propiedad intelectual e industrial, que se mantendrán hasta el momento de la finalización del plazo legal de duración de esos derechos.

2.5.4. Publicidad y comunicaciones

Todas las decisiones sobre la selección y adjudicación del procedimiento de la presente contratación pública precomercial para el diseño y ejecución de proyectos de I+D, como el anuncio de los actos públicos de la Comisión de Contratación, se publicarán en la página web oficial de INCIBE (www.incibe.es) y en el Perfil del Contratante.

2.6. Comisión de Contratación y el Comité Técnico

2.6.1. Comisión de Contratación

El Órgano de Contratación estará asistido por una Comisión de Contratación de acuerdo con lo establecido en el presente documento regulador.

La Comisión de Contratación estará compuesta por tres miembros de INCIBE con categoría de Subdirector o Gerente de Departamento o persona en quien deleguen, uno de los cuales actuará como Presidente, y un integrante del Departamento Jurídico, que actuará como Secretario.

La composición de la Comisión se publicará en el perfil de contratante del Órgano de Contratación.

Todos los miembros de la Comisión de Contratación tendrán voz y voto, excepción hecha del Secretario, que sólo tendrá voz.

Para la válida constitución de la Comisión de Contratación será imprescindible la asistencia presencial, virtual o híbrida de todos sus miembros. La Comisión de Contratación se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y aprobar y remitir actas tanto de forma presencial, virtual o híbrida, así como por escrito y sin sesión formal.

Las **funciones** de la Comisión de Contratación serán las siguientes:

- En la fase de selección de licitadores, la Comisión de Contratación examinará la documentación administrativa (sobre A) y determinará los licitadores que cumplen los criterios de solvencia.
- Valorará las propuestas presentadas con el apoyo del Comité Técnico clasificándolas en orden decreciente de valoración (Sobres B y C).
- Podrá proponer al Órgano de Contratación que promueva una nueva licitación de similares características en algunos de los retos. La decisión o no de promover la nueva licitación será del Órgano de Contratación así como la determinación de los condiciones.
- Propondrá la admisión o exclusión de las propuestas presentadas, con arreglo a lo indicado en el presente documento.
- Propondrá al Órgano de Contratación la adjudicación o adjudicaciones de los proyectos de I+D que ejecutarán los adjudicatarios, en caso de convertirse en contratistas, según proceda de conformidad con el presente documento regulador:
- Examinará la documentación proporcionada por los licitadores durante las fases de adjudicación y formalización del contrato.
- Las demás funciones previstas en este documento o cualquier otra que le pueda encargar el Órgano de Contratación.

Además, la Comisión de Contratación contará con el apoyo de un Comité Técnico experto, cuyos miembros serán designados por INCIBE.

2.6.2. El Comité Técnico

Las **funciones** del Comité Técnico serán las siguientes:

- Valorar y emitir un informe sobre cada una de las propuestas presentadas por los licitadores, de acuerdo con los criterios de valoración descritos en el presente documento regulador.
- Dar apoyo técnico a la Comisión de Contratación durante todas las fases del procedimiento y responder puntualmente a sus peticiones de asistencia, efectuando las aclaraciones y análisis que se puedan requerir.
- Las demás funciones previstas en este documento o cualquier otra que le pueda encargar la Comisión de Contratación.

3. PROCEDIMIENTO DE ADJUDICACIÓN

El Órgano de Contratación podrá en cualquier momento, particularizar, matizar o detallar lo indicado en este apartado, mediante la oportuna publicación en el Perfil del Contratante.

A partir de la siguiente tabla se puede observar el resumen del procedimiento que se desglosará más adelante:

Fases del procedimiento	Plazo	Limitaciones	Acciones
Fase I: Presentación de ofertas	60 días naturales desde la publicación del documento regulador.	Sin límite de licitadores. Cada licitador puede concurrir máximo a tres retos diferentes. Para un reto, el licitador solo puede presentar 1 oferta.	El licitador entrega los sobres A, B y C.
Fase II: Comprobación de solvencias y capacidad jurídica y de obrar	-	-	INCIBE evalúa sobre A.
Fase III: Evaluación de ofertas	-	-	INCIBE evalúa sobres B y C.
Fase IV: Propuesta de adjudicación	Reto a reto, tras la evaluación de las ofertas.	>=2 adjudicatarios por reto.	INCIBE propone adjudicatarios
Fase V: Adjudicación definitiva	10 días hábiles desde el siguiente a aquél en que hubiera recibido el requerimiento.	>=2 adjudicatarios por reto.	Si toda la información recabada es correcta, el Órgano de Contratación adjudica.
Fase VI: Formalización del contrato	<=15 días naturales desde el siguiente a aquel en que hubiera recibido la notificación de la adjudicación definitiva.	>=2 adjudicatarios por reto.	Se formaliza el contrato.

Tabla 2: Resumen de fases del procedimiento de adjudicación

3.1. Descripción general

Con carácter general, la Comisión de Contratación dejará constancia en actas de las actuaciones que se describen en el presente apartado, que necesariamente deberán publicarse.

La licitación ha sido configurada, en la plataforma de contratación de INCIBE, de tal manera que el licitador deberá presentar sus propuestas de forma separada a cada uno de los retos, indicados en *ANEXO 1. Retos*, que se corresponderán a lotes dentro de la propia plataforma.

La adjudicación de los contratos se realizará a través de un procedimiento abierto.

3.1.1. Límite de retos admitidos por licitador

El Órgano de Contratación limita el **número de retos a los que un licitador puede presentar oferta a tres**. Si algún licitador presentara más de tres ofertas se le consultará al inicio del proceso cuál de los retos realmente presenta y cual retira. Los retirados no serán calificados.

3.1.2. Límite para la adjudicación de cada reto

El número de adjudicatarios por reto será cero o será mayor o igual a 2; por tanto, se hace notar que en caso de que a un determinado reto sólo se presente una oferta válida, el reto será declarado desierto.

El número de adjudicatarios por reto dependerá de la cantidad y calidad de propuestas recibidas y del presupuesto existente para los contratos.

3.1.3. Plazo para presentación de sobres

El plazo máximo para presentar la documentación relativa a los sobres A, B y C será de **sesenta (60) días naturales** a contar desde la publicación del presente documento regulador.

3.1.4. Requisitos de los licitadores

3.1.4.1. Aptitud y capacidad

Podrán presentarse a la presente contratación las personas naturales o jurídicas, españolas o extranjeras, ya sea de forma individual o mediante una agrupación de operadores económicos, que tengan plena capacidad de obrar, no estén incursas en las prohibiciones de contratar señaladas en el presente documento y acrediten las solvencias económica o financiera y técnica o profesional exigidas.

En ningún caso podrán contratar con INCIBE las personas en las que concurra alguna de las circunstancias establecidas en el artículo 71 de la LCSP. Si el licitador incurre en cualquiera de estos criterios de prohibición, será excluido de participar en el presente procedimiento.

Las personas jurídicas sólo podrán ser adjudicatarias si su ámbito de actividad, a tenor de sus estatutos o reglas fundacionales, está directamente relacionado con los fines del presente Documento regulador.

3.1.4.2. Empresas comunitarias

Tendrán capacidad para presentarse a la presente contratación, en todo caso, las empresas no españolas de Estados miembros de la Unión Europea que, con arreglo a la legislación del Estado en que estén establecidas, se encuentren habilitadas para realizar la prestación de que se trate.

Cuando la legislación del Estado en que se encuentren establecidas estas empresas exija una autorización especial, o la pertenencia a una determinada organización, para poder prestar en él el servicio de que se trate, deberán acreditar que cumplen este requisito.

3.1.4.3. Empresas no comunitarias

Las personas jurídicas de Estados no pertenecientes a la Unión Europea deberán justificar mediante informe de la respectiva Misión Diplomática Permanente española, que se acompañará a la documentación que se presente, que el Estado de procedencia de la empresa extranjera admite a su vez la participación de empresas españolas en la contratación con la Administración y con los entes, organismos o entidades del Sector Público en forma sustancialmente análoga.

3.1.4.4. Agrupación de operadores económicos o Unión temporal de empresas

Podrán participar en la presente licitación las agrupaciones de operadores económicos que se constituyan temporalmente al efecto, sin que sea necesaria la formalización de estas en escritura pública hasta que se haya efectuado la adjudicación del Contrato a su favor.

Los empresarios que concurran agrupados en agrupaciones temporales quedarán obligados solidariamente y deberán nombrar un representante o apoderado único de la agrupación con poderes bastantes para ejercitar los derechos y cumplir las obligaciones que del contrato se deriven hasta la extinción de este, sin perjuicio de la existencia de poderes mancomunados que puedan otorgar para cobros y pagos de cuantía significativa.

A efectos de la licitación, los empresarios que deseen concurrir integrados en una agrupación temporal deberán indicar mediante el formato facilitado en el *ANEXO 2. Declaración responsable (sobre A)*, los nombres y circunstancias de los que la constituyan y la participación de cada uno, así como que asumen el compromiso de constituirse formalmente en unión temporal en caso de resultar adjudicatarios del contrato.

La duración de las agrupaciones temporales de operadores económicos será coincidente con la del Contrato hasta su extinción, así como durante el periodo de vigencia de las garantías definitivas presentadas.

No se admitirán cambios en la composición de la agrupación de operadores durante el período de licitación ni de ejecución del contrato, salvo durante la ejecución del contrato en caso de insolvencia de uno de los miembros de la misma o en caso de una operación de reestructuración empresarial que afecte a uno o más de uno de sus miembros, vía fusión, adquisición, transformación o transmisión de empresa o unidad de negocio. Para ello, deberá formalizarse la oportuna cesión del contrato aceptada por todas las partes.

3.1.4.5. Subcontratistas

La subcontratación está permitida en el contrato, no existiendo límite.

Las aportaciones de medios y recursos realizadas por los subcontratistas formarán parte a todos los efectos de los compromisos del licitador.

Los licitadores (individual o conjuntamente) que quieran subcontratar parte de los servicios de investigación y desarrollo deberán detallar en su propuesta técnica, qué partes y proyectos quieren subcontratar a otros contratistas (Universidades, centros de investigación, otras empresas, etc.), entregando para ello el modelo recogido en el ANEXO 3. Modelo de ficha de subcontratación (sobre A), en el que el subcontratista declare:

- que está informado y manifiesta su consentimiento con las disposiciones y requisitos que contiene el presente documento regulador (especialmente las relacionadas con los derechos de propiedad intelectual e industrial);
- que cumple los requisitos de solvencia técnica y económica para la provisión de los servicios subcontratados; y
- que pone sus recursos a disposición del licitador durante toda la duración de su contrato.

A los efectos de la presente licitación, será compatible para las entidades subcontratistas formalizar su compromiso de contratación con diferentes operadores económicos o agrupaciones de operadores económicos.

Si, posteriormente, el contratista necesita cambiar o añadir nuevos subcontratistas (durante la ejecución del contrato), deberá ser autorizado con anterioridad expresamente por INCIBE, debiendo entregar una propuesta junto con el anexo 3. No se admitirá la sustitución de subcontratistas que afecten a las condiciones tenidas en cuenta para el cumplimiento de los criterios de solvencia.

No se admitirán cambios en relación con los subcontratistas si ello genera problemas o conflictos en materia de derechos de propiedad intelectual o industrial.

Aun cuando se produzca una subcontratación de acuerdo con el presente apartado, el contratista seguirá siendo responsable ante la entidad contratante de la ejecución y cumplimiento de todas sus obligaciones, establecidas en el Contrato, siendo responsable asimismo de los daños causados por cualquier negligencia imputable a su subcontratista.

3.1.4.6. Empresas pertenecientes a un mismo grupo empresarial

Se considerarán empresas vinculadas las que se encuentren en alguno de los supuestos previstos en el artículo 42 del Código de Comercio.

La presentación de ofertas diferentes por empresas vinculadas para un mismo reto supondrá la exclusión del presente procedimiento de contratación, a todos los efectos, de las propuestas formuladas.

Cuando empresas pertenecientes a un mismo grupo, entendiéndose por tales las que se encuentren en alguno de los supuestos del artículo 42.1 del Código de Comercio, presenten distintas ofertas para concurrir individualmente o en UTE (Unión Temporal de Empresas) a la adjudicación del contrato para un mismo reto, será causa de exclusión de las ofertas formuladas.

A los efectos de lo dispuesto en este apartado, las empresas del mismo grupo que concurran a un mismo reto deberán presentar declaración sobre los extremos reseñados.

3.1.4.7. Prácticas colusorias

Durante la tramitación del proceso de licitación, tanto el Órgano de Contratación como quienes asistan al mismo velarán por la salvaguarda de la libre competencia. Sin perjuicio de su comunicación a la Comisión Nacional de Mercados y Competencia conforme a lo dispuesto en el artículo 132.3 LCSP, se adoptarán las medidas oportunas para reprimir cualesquiera prácticas colusorias, entendidas como cualquier indicio de acuerdo, decisión o recomendación colectiva, o práctica concertada o conscientemente paralela entre los licitadores, que tenga por objeto, produzca o pueda producir el efecto de impedir, restringir o falsear la competencia en el proceso de contratación.

En particular, serán objeto de análisis específico en el marco de esta licitación los siguientes indicadores de alerta de posible colusión (*red flags*):

- similitudes en el formato o en el texto de las ofertas (por ejemplo, los mismos errores tipográficos o frases en distintas ofertas);
- idénticos metadatos en los documentos;
- subcontratación cruzada (dos licitadores presentan su oferta a título individual y se subcontratan recíprocamente);
- ofertas presentadas por varias empresas, pero firmadas por el mismo representante legal, con idénticos datos de contacto, idéntico domicilio social de ambos licitadores, o cuando exista vinculación entre sus órganos de administración.

Las *red flags* son indicios de colusión, no determinantes en ningún caso de la existencia de ninguna irregularidad, por lo que la eventual exclusión de licitadores se realizará previa audiencia a los mismos, antes de que el Órgano de Contratación tome la decisión definitiva y siguiendo el procedimiento legalmente establecido en la normativa antifraude de INCIBE.

Sin perjuicio de, facultativamente, solicitar un informe previo a la Comisión Nacional de Mercados y Competencia sobre el particular, la decisión de exclusión no precisará necesariamente de pruebas de colusión, siendo posible hacerlo sobre la base de la confirmación de esos indicios, que serán

inmediatamente comunicados a la Comisión Nacional de Mercados y Competencia, a los efectos oportunos. Corresponderá a la propia Comisión, y no al Órgano de Contratación, la calificación definitiva de una conducta como colusoria, y la deducción de las consecuencias que tal circunstancia lleve aparejada conforme a la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

En cualquier caso, la eventual exclusión de un licitador adoptada por el Órgano de Contratación a la vista de los indicios de colusión no tendrá naturaleza sancionadora, sino que se enmarca dentro de sus facultades para velar por el cumplimiento de los principios de igualdad de trato y competencia en el procedimiento de adjudicación, así como para garantizar la integridad, la fiabilidad y la idoneidad del futuro contratista para ejecutar el contrato.

3.1.4.8. Concreción de las condiciones de solvencia

Para acreditar la solvencia necesaria, tanto económica como financiera y técnica o profesional, el empresario podrá basarse en la solvencia y medios de otras entidades, independientemente de la naturaleza jurídica de los vínculos que tenga con ellas, siempre que demuestre que, para la ejecución del contrato, dispone efectivamente de esos medios.

Cuando se trate de empresas pertenecientes a un mismo grupo, entendiéndose por tales las que se encuentren en alguno de los supuestos previstos en el artículo 42 del Código de Comercio, podrán asimismo basarse en la solvencia y medios de las entidades de su grupo empresarial siempre que demuestre que, para la ejecución del contrato, dispone efectivamente de esos medios.

Los licitadores deberán acreditar su solvencia económica y financiera y profesional o técnica en la forma que se determinan a continuación:

3.1.4.8.1. Solvencia económica o financiera

Se establecen como **requisitos mínimos de solvencia**:

- La entidad no está incursa en causa legal de disolución: El patrimonio neto deberá ser igual o superior a la mitad del capital social, en prueba del cual, podrán aportarse las últimas cuentas anuales o extractos de estas. En todo caso, los licitadores que en virtud de disposiciones vigentes vengan obligados a dar publicidad a sus cuentas anuales, deberán presentar las cuentas depositadas en el Registro Mercantil.
- El volumen de negocios antes referido deberá ser por importe igual o superior anual de 50% del precio del contrato en euros en uno de los tres últimos ejercicios. Para su verificación se presentarán las cuentas anuales. En todo caso, los licitadores que en virtud de disposiciones vigentes vengan obligados a dar publicidad a sus cuentas anuales, deberán presentar las cuentas depositadas en el Registro Mercantil. El dato que se verificará es el de importe neto de cifra de negocio de la cuenta de pérdidas y ganancias.
- Una póliza de seguros que ofrezcan un nivel adecuado de cobertura para todos los riesgos en que pueda incurrir el contratista, derivados de la ejecución y cumplimiento del contrato por un importe equivalente al 50% del presupuesto del proyecto.

Para ello se deberá aportar en el sobre A la correspondiente declaración responsable en formato DEUC (ver el *ANEXO 2. DECLARACIÓN RESPONSABLE (SOBRE A)*), sin perjuicio de la documentación posterior que deberá presentarse en caso de resultar el licitador propuesto adjudicatario, tal y como se establece en el presente documento regulador.

A los efectos de contabilización de este criterio, las empresas que formen parte de un grupo empresarial podrán aportar las cifras consolidadas de su grupo de empresas.

3.1.4.8.2. Solvencia técnica y profesional

La solvencia técnica y profesional del licitador deberá acreditarse por el siguiente medio:

El licitador deberá acreditar que ha realizado en los cinco últimos años, al menos, **alguna de las 2 siguientes opciones**:

- Servicios o proyectos de I+D+i en materia de ciberseguridad, tanto con/para entidades públicos como con entidades privadas, en los últimos 5 años.
- Haber generado, fruto de un proyecto de I+D+i propio, un producto de ciberseguridad propio, por cuya comercialización se hayan facturado un mínimo de 200.000,00 €+IVA en los 5 años anteriores a la publicación de esta licitación La comercialización debe haberse efectuado en la Unión Europea o en cualquier país, cuya Misión Diplomática Permanente española acredite, que el Estado de procedencia de la empresa extranjera admite a su vez la participación de empresas españolas en la contratación con la Administración y con los entes, organismos o entidades del Sector Público en forma sustancialmente análoga.

Los servicios o trabajos efectuados se acreditarán mediante:

a) certificados expedidos o visados por el órgano competente, cuando el destinatario sea una entidad del sector público;
b) cuando el destinatario sea un sujeto privado, mediante un certificado expedido por este o, a falta de este certificado, mediante una declaración del empresario acompañado de los documentos obrantes en poder del mismo que acrediten la realización de la prestación

La acreditación se solicitará a los licitadores propuestos adjudicatarios en el sobre A solo se incluirá la De (cuyo modelo se puede ver en el *ANEXO 2. DECLARACIÓN RESPONSABLE (SOBRE A)*), sin perjuicio de la documentación posterior que deberá presentarse en caso de resultar el licitador adjudicatario, tal y como se establece en el presente documento regulador.

3.1.5. Formato y contenido de los sobres A, B y C

La oferta se ha de entregar en tres sobres:

- sobre A: capacidad y solvencias;
- sobre B: documentos relativos a los criterios de juicio de valor;
- sobre C: documentación relativa a los criterios evaluables de forma automática.

3.1.5.1. Contenido del sobre A (capacidad y solvencias)

La documentación para comprobar la **capacidad**[6] **y solvencias** exigidas se incluirá en el **sobre A** que deben presentar los licitadores, cuyos modelos corresponden a los anexos:

- ANEXO 2. Declaración responsable (sobre A), y
- ANEXO 3. Modelo de ficha de subcontratación (sobre A).

Para cada uno de los retos al que se solicite presentar oferta, el licitador deberá por tanto presentar:

a) un único ANEXO 2. Declaración responsable (sobre A) completado correctamente, y
b) tantos ANEXO 3. Modelo de ficha de subcontratación (sobre A) como sean necesarios.

3.1.5.2. Contenido del sobre B (juicio de valor)

[6] Ver apartado Fase V Adjudicación Definitiva

La documentación relativa a los criterios de **juicio de valor** se incluirá en el sobre B y corresponderá con:

- ANEXO 11. Memoria técnica (sobre B);
- ANEXO 4. Modelo de presupuesto de proyectos (sobre B);
- ANEXO 5. Modelo de compromiso con entidad usuaria final de proyecto de I+D (sobre B);
- Información obligatoria según lo establecido en el apartado 4.8 Derechos de propiedad intelectual e industrial.

Para cada uno de los retos al que se solicite presentar oferta, el licitador deberá por tanto presentar:

a) un ANEXO 11. Memoria técnica (sobre B);

b) un ANEXO 4. Modelo de presupuesto de proyectos (sobre B);

c) tantos ejemplares de ANEXO 5. Modelo de compromiso con entidad usuaria final de proyecto de I+D (sobre B).

d) aquella información a la que esté obligada el licitador en materia de derechos de propiedad intelectual e industrial.

- IMPORTANTE:
- Es imprescindible para que la oferta sea evaluada presentar **al menos un**[7] ANEXO 5. Modelo de compromiso con entidad usuaria final de proyecto de I+D (sobre B).
- No se podrá incluir ninguna información en el contenido del sobre B que permita deducir el contenido del sobre C. La inclusión de la citada información podrá implicar la exclusión automática del licitador del procedimiento por parte de la Comisión de Contratación. El licitador podrá formular todas y cuantas solicitudes de aclaración estime oportunas al Órgano de Contratación, hasta tres (3) días hábiles antes del fin del plazo para la presentación de las propuestas (en cualquiera de las fases), sobre qué tipo de información se entiende que implicaría la aplicación de este supuesto.

3.1.5.3. Contenido del sobre C (evaluables de forma automática)

La documentación relativa a los criterios **evaluables de forma automática** se presentará en el SOBRE C y se corresponderá al:

- ANEXO 7. Modelo evaluación automática (sobre C).

Para cada uno de los retos al que se solicite presentar oferta, el licitador deberá por tanto presentar:

a) un ANEXO 7. Modelo evaluación automática (sobre C).

3.1.6. Procedimiento y criterios de evaluación de las propuestas

Los criterios de evaluación de las propuestas se dividen en dos tipos:

a. Criterios sometidos a juicio de valor.
b. Criterios evaluables de forma automática.

Se valorarán primero los contenidos del sobre B aplicando los criterios de juicio de valor.

[7] Se considera pues un requisito mínimo el presentar al menos una carta de compromiso de usuario final. Estas cartas podrán ser de usuarios públicos o privados, ya captados para el codesarrollo y validación tecnológica del proyecto.

Se excluirá a aquellas propuestas que no alcancen un 50% de la puntuación máxima obtenible en el conjunto de los criterios evaluables mediante juicio de valor o que obtengan 0 puntos en alguno de estos criterios.

Tras la publicación de la valoración se abrirá el contenido del sobre C sólo de aquellas ofertas que no se hayan excluido por los motivos anteriormente indicados y se procederá a la valoración de los criterios evaluables de forma automática. Tras dicha evaluación se publicará el informe definitivo de evaluación con la suma de las puntuaciones obtenidas mediante los criterios sometidos a juicio de valor y los evaluables de forma automática.

El Órgano de Contratación podrá requerir, a través de la Comisión de Contratación, cualquier ampliación de información o aclaración que estime necesaria, sobre cualquier contenido de los sobres B y C, siguiendo lo establecido en el presente documento regulador.

Los **criterios de valoración del sobre B** vienen descritos en el ANEXO 12: Criterios evaluables para el sobre B.

La valoración de cada uno de los criterios se realizará de manera competitiva y mediante la comparación de las propuestas de los distintos licitadores en función de lo indicado en los criterios. La valoración será realizada por la Comisión de Contratación, con el apoyo del Comité Técnico.

La Comisión de Contratación, con el apoyo del Comité Técnico, podrá no otorgar el máximo de puntuación en cualquiera de los criterios si entiende que ninguna de las propuestas ha alcanzado el nivel suficiente para ello.

Los **criterios de valoración del sobre C** vienen descritos en el ANEXO 13: Criterios evaluables para el sobre C.

3.2. Fase I: Presentación de ofertas

El plazo para la presentación de ofertas será de sesenta (60) días naturales contados desde la publicación del anuncio en el Perfil del Contratante del presente documento regulador.

Las propuestas deberán ir acompañadas de la documentación administrativa (sobre A) y contenido de la oferta (sobres B y C) que se relacionan en el presente documento regulador.

Los licitadores sólo podrán presentar una única oferta en cada reto. Esta condición es adicional a la del límite de retos que puede ofertar un licitador establecida en el presente documento regulador. Lo podrán hacer de manera individual o en forma de agrupación temporal de operadores económicos (UTE). Asimismo, para un mismo reto, no podrá suscribir ninguna proposición en agrupación con otros si lo ha hecho individualmente ni figurar en más de una agrupación temporal.

Si el Licitador presentara ofertas con otra u otras agrupaciones habiéndolo hecho individualmente o con otra agrupación para un mismo reto, quedarían excluidas todas las ofertas.
La infracción de estas normas dará lugar a la no admisión de todas las proposiciones por él suscritas.

Las proposiciones para tomar parte en la licitación se presentarán únicamente por medios electrónicos a través de los servicios de licitación electrónica de la Plataforma de Contratación del Sector Público y mediante la herramienta de preparación y presentación de ofertas que la Plataforma de Contratación del Sector Público pone a disposición de los licitadores, a través de la cual se garantiza la integridad, no repudio, autenticidad y confidencialidad de las ofertas.

Para la utilización de estos servicios, los licitadores interesados en la presentación de ofertas en este procedimiento deberán registrarse previamente en la Plataforma de Contratación del Sector Público, utilizando para ello las guías de ayuda disponibles, y en concreto, para este trámite, la Guía

de Utilización de la Plataforma de Contratación del Sector Público para Empresas (Guía de Operador Económico), accesible a través de la siguiente página: www.contrataciondelestado.es

Al margen de ello, el empleo de los servicios de licitación electrónica requiere, además de ser usuario registrado en la plataforma, cumplimentar los datos adicionales que constan en la guía de referencia, activando la cuenta de usuario y asociando un correo electrónico al que dirigir las notificaciones y comunicaciones. Como requisitos técnicos, se habrá de disponer de conexión a internet, navegador con una versión 1.8 o superior de máquina virtual Java instalada, y certificado electrónico reconocido por la Administración General del Estado (@firma).

En todo caso, la sola presentación de la oferta implica la aceptación incondicional por el licitador de todas y cada una de las cláusulas de este documento regulador, sin salvedad o reserva alguna, así como la autorización a la Comisión de Contratación y al Órgano de Contratación para consultar los datos recogidos en ROLECE o en las listas oficiales de operadores económicos de un Estado Miembro de la Unión Europea.

De acuerdo con lo previsto en el artículo 23 del Reglamento General de la Ley de Contratos de las Administraciones Públicas (en adelante, RGLCAP), las empresas extranjeras que contraten en España presentarán la documentación traducida de forma oficial al castellano siempre que se les requiera.

La citada herramienta de preparación y presentación de las ofertas asociada a procedimiento estará disponible hasta alcanzar la fecha y hora final de presentación de ofertas que se refleja en la correspondiente fase del procedimiento (o bien las subsanaciones o requerimientos de documentación, si fueran emplazados a ello), sin que sea admisible su presentación transcurrido dicho plazo.

No obstante, en caso de que cualquiera de los documentos de la oferta no pueda visualizarse correctamente, se permitirá que, en un plazo máximo de 24 horas desde que se notifique esta circunstancia, el licitador presente la documentación en formato adecuado, que no podrá sufrir ninguna modificación respecto al original incluido en la oferta. Si el Órgano de Contratación comprueba que el documento ha sufrido modificaciones, la oferta del licitador será excluida del procedimiento (aplicando lo indicado en la Disposición Adicional Decimosexta LCSP en lo referente a la huella electrónica).

En todo caso, y de producirse la situación prevista en el párrafo anterior, no se facilitará a los licitadores interesados en el procedimiento información alguna relativa a los actos celebrados en tanto no se subsane o resuelva dicha circunstancia.

Serán excluidas aquellas solicitudes que se presenten fuera del plazo indicado, sin perjuicio del supuesto de huella electrónica que podrá enviarse en el plazo de 24 horas en los términos recogidos en la citada Disposición Adicional Decimosexta de la LCSP.

Recibida la documentación presentada por los licitadores, el Órgano de Contratación podrá requerir tantas subsanaciones o aclaraciones sobre la documentación presentada como estime oportuno, otorgando un plazo indicado en el propio requerimiento, nunca inferior a tres (3) días hábiles. El plazo será el mismo para todos los licitadores requeridos por el mismo motivo.

3.3. Fase II: Comprobación de solvencias (calificación del sobre A)

La Comisión de Contratación calificará la documentación de las condiciones de capacidad y solvencia de acuerdo con la exigencia inicial de declaración responsable que posteriormente se acreditará si resulta propuesto adjudicatario.

3.4. Fase III: Evaluación de ofertas (valoración de los sobres B y C)

INCIBE valorará las ofertas y actuará del siguiente modo:

- Inicialmente se dará apertura al contenido de los sobres B correspondientes a las ofertas de todos los retos, por parte de la Comisión de Contratación.
- Para cada reto, se elaborará un informe técnico de valoración, que elevará a la Comisión de Contratación, en el que se analicen las ofertas presentadas en relación con los criterios de adjudicación sometidos a juicio de valor y expresen las características y ventajas de cada una de ellas, incluyendo la ponderación de las valoraciones, que serán oportunamente publicadas antes de la apertura del sobre C del reto que se esté evaluando.
- El informe se realizará de tal forma que no recoja información facilitada por los licitadores que éstos hayan designado como confidencial y, en particular, secretos técnicos o comerciales. Si hubiera información identificada como confidencial pero fuera necesaria su publicación se procederá a realizar trámite contradictorio con la empresa y la comisión de contratación decidirá de manera justificada ponderando los principios de confidencialidad y de transparencia e igualdad de trato. En ningún caso, toda la oferta puede ser considerada confidencial.
- La Comisión de Contratación revisará el contenido de las propuestas correspondientes al sobre C y calculará las puntuaciones obtenidas por cada oferta.

La Comisión de Contratación evaluará de forma progresiva si bien no necesariamente consecutiva cada uno de los retos incluidos en el *ANEXO 1. Retos*, pudiendo publicar, el Órgano de Contratación, los resultados de evaluación de cada uno de los retos de manera secuencial, sin tener que esperar, por tanto, a la evaluación del resto de los retos, y sin necesidad de seguir un orden en concreto. De igual modo, INCIBE podrá realizar futuras licitaciones amparadas en los retos definidos actualmente.

3.5. Fase IV: Elaboración de la clasificación de las ofertas y Propuesta de adjudicación

Para cada uno de los retos, la Comisión de Contratación, con el apoyo del Comité Técnico, presentará su informe donde se recoja la valoración de los citados criterios, tanto de juicio de valor, como evaluables mediante fórmula para cada proyecto individual y elevará la propuesta de adjudicación al Órgano de Contratación, propuesta que será notificada a los licitadores a través de la Plataforma de Contratación.

Tal y como ya se ha indicado, deberá proponer, al menos, la adjudicación de un mínimo de dos contratos por reto o, en su defecto, declarar desierto el reto[8]. Del mismo modo, podrá proponer la adjudicación de más contratos, siendo incluso posible proponer la adjudicación a todas las ofertas presentadas.

En cualquier caso, la propuesta de adjudicación recaerá siempre en las propuestas que hayan obtenido una mejor valoración.

La selección de las ofertas para realizar la propuesta de adjudicación se realizará del siguiente modo:

El presupuesto máximo de la licitación (30 retos) asciende a 137.200.000,00 millones de euros. El presupuesto de los proyectos deberá ser tal que la inversión de INCIBE esté comprendida entre el mínimo y el máximo previsto en el ANEXO 6.

Se formalizarán tantos contratos como ofertas se suscriban hasta alcanzar el presupuesto máximo de la licitación. Se formalizarán contratos con las ofertas que cumplan las exigencias mínimas del documento regulado y por orden de clasificación de las ofertas por reto. No se adjudicarán contratos en retos en que no existan dos contratos válidos conforme al documento regulador para evitar la falta de competencia del mercado promovida por INCIBE con la contratación. De existir remanente

[8] Si no hay dos ofertas viables el reto queda desierto para evitar el impacto en la competencia del mercado.

para uno o varios retos (mayor presupuesto máximo para el reto que oferta válidas) una vez adjudicados los contratos que tengan cabida dentro del presupuesto máximo previsto para cada reto se podrá utilizar el remanente para contratar en otros retos en que hayas ofertas válidas pero insuficiencia de presupuesto para cubrirlas. La selección de estos contratistas con remanente se hará del siguiente modo:

1. Se empezará la selección de las ofertas de los retos de mayor a menor presupuesto máximo inicial cuyo presupuesto se haya agotado. Este orden de selección de los retos coincide con el mayor interés de INCIBE en fomentar el desarrollo de la I+D para el tipo de reto y porque los retos de mayor importe se considera tienen un mayor impacto en la ciberseguridad nacional. Si los retos tienen igual presupuesto máximo, se realizará una clasificación de las ofertas de dichos retos y se adjudicará de mayor a menor puntuación de las ofertas. En caso de empate de las ofertas se realizará un sorteo público en al que se convocará a las entidades afectadas.
2. Se seleccionarán las ofertas válidas no adjudicadas en el orden de clasificación obtenido en el reto.
3. Se adjudicarán solo contratos que cumplan los mínimos del documento regulador (deberán atender adecuadamente al requerimiento previo de documentación a la adjudicación).
4. Se adjudicarán contratos hasta agotar presupuesto de remanente esto es hasta alcanzar 137.200.000,00 € IVA excluido que es presupuesto máximo de la licitación, o no alcanzándolo cuando el remanente sea insuficiente para cubrir el siguiente proyecto clasificado.

El procedimiento de adjudicación finalizará en los términos que se han descrito en la cláusula 3.1 Descripción general.

La propuesta de adjudicación, como se ha indicado, se realizará proyecto a proyecto, siendo posible que un licitador reciba propuesta de adjudicación de varios proyectos. Para cada uno de los proyectos para los que haya recibido propuesta de adjudicación, el licitador deberá formalizar un contrato individual.

La Comisión de Contratación podrá requerir a los licitadores que reciban propuesta de adjudicación a su favor, antes de la adjudicación definitiva del contrato, que aclaren determinados aspectos de esta o ratifiquen los compromisos que en ella figuran, siempre que con ello no se modifiquen elementos sustanciales de la propuesta o de la licitación, se falsee la competencia, o se produzca un efecto discriminatorio.

La adjudicación de los contratos se realizará de forma progresiva hasta que se dé una de las siguientes dos circunstancias:

- Que el Órgano de Contratación dé por finalizado el procedimiento de adjudicación, a cuyos efectos realizará la correspondiente publicación en su Perfil del Contratante.
- Que el Órgano de Contratación adjudique todo el presupuesto disponible. Antes de darse esta circunstancia, el Órgano de Contratación podría aumentar la aportación económica máxima prevista, en caso de estimarlo necesario y previa solicitud de las autorizaciones oportunas. En este caso, comunicará esta circunstancia en el Perfil del Contratante.

En cualquier caso, el Órgano de Contratación gestionará el presupuesto disponible para que siempre sea viable, al menos, adjudicar dos contratos por cada uno de los retos, a no ser que no se hayan presentado ofertas suficientes para ello, en cuyo caso podrá convocar nueva licitación para ese reto.

3.6. Fase V: Adjudicación definitiva

El Órgano de Contratación, con carácter previo a la adjudicación definitiva, requerirá a los licitadores que hayan presentado proyectos que hayan sido seleccionados, dentro del plazo de diez (10) días hábiles, a contar desde el siguiente a aquél en que hubiera recibido el requerimiento, presente la siguiente documentación:

- Los documentos que acrediten la personalidad, que serán los siguientes:
  - Será obligatoria la presentación de copia del Documento Nacional de Identidad (o el que, en su caso, lo substituya reglamentariamente), de la persona titular o propietaria de la empresa, así como la documentación acreditativa del alta en el Impuesto de Actividades Económicas.
  - Si la empresa fuese persona jurídica española, Número de Identificación Fiscal y de la escritura o documento de constitución, los estatutos o el acto fundacional, en los que consten las normas por las que se regula su actividad, debidamente inscriptos, en su caso, en el Registro Público que corresponda, según el tipo de persona jurídica de que se trate. Se comprobará que se trata de empresas dedicadas al ámbito de la ciberseguridad, desarrollos de software, consultoría informática, servicios y productos relacionados con las tecnologías de la información y de la comunicación, de telecomunicaciones, I+D y cualquier actividad relacionada con el objeto y el reto al que se presente.
  - La personalidad de los empresarios no españoles de Estados miembros de la Unión Europea o signatarios del Acuerdo sobre Espacio Económico Europeo se acreditará por su inscripción en el registro procedente de acuerdo con la legislación del Estado donde están establecidos. Cuando la legislación del Estado donde están establecidas estas empresas exija una autorización especial o la pertenencia a una determinada organización para poder prestar el servicio de que se trate, deberán acreditar que cumplen este requisito.
  - La capacidad de las empresas extranjeras de Estados no miembros de la Unión Europea se acreditará mediante informe de la Misión Diplomática Permanente de España en el Estado correspondiente o de la oficina consular en cuyo ámbito territorial radique el domicilio de la empresa en el que se haga constar que figura inscripta en el registro local, profesional, comercial o análogo o, en su defecto, que actúan habitualmente en el tráfico local en el ámbito de las actividades a las que se extiende el objeto del contrato.
  - Además, deberán justificar mediante informe de la respectiva Misión Diplomática Permanente Española que el Estado de procedencia de la empresa extranjera admite a su vez la participación de empresas españolas en la contratación con la Administración y su Sector Público. Por ello, no será necesario el informe de reciprocidad en relación con las empresas de Estados signatarios del Acuerdo sobre Contratación Pública de la Organización Mundial del Comercio.
- Los documentos que acreditan la representación, que serán los siguientes:
  - Los que comparezcan y firmen la proposición en nombre de otro deberán presentar copia del DNI o del documento que reglamentariamente lo substituya.
  - Escritura de poder notarial otorgada por el titular o propietario de la empresa.
  - Si el licitador fuese persona jurídica, se aportará copia auténtica o compulsada de la escritura de constitución de la sociedad y modificación, en su caso, inscripta en el Registro Mercantil, o en su caso en el Registro que corresponda.
- Presentación de la documentación hallarse al corriente de las obligaciones tributarias y de Seguridad Social:
  - Certificación positiva de la Tesorería General de la Seguridad Social en la que conste que se encuentra al corriente del cumplimiento de las obligaciones señaladas en el artículo 14 del RGLCAP, expedida a los efectos de la LCSP.

- Certificación positiva de la Agencia Tributaria del Estado en la que conste que no tiene deudas de naturaleza tributaria con el Estado, expedida a los efectos de la LCSP.

- Presentación de la documentación en relación con el Impuesto de Actividades Económicas (IAE).
  - El licitador deberá estar dado de alta en el IAE, en el epígrafe correspondiente al objeto del contrato, siempre que ejerzan actividades sujetas a este impuesto, en relación con las actividades que vengan realizando a la fecha de presentación de las solicitudes de participación, que les faculte para su ejercicio en el ámbito territorial en que las ejercen. La acreditación de este extremo se efectuará mediante la presentación del alta, referida al ejercicio corriente, o del último recibo del IAE, completado con una declaración responsable de no haberse dado de baja en la matrícula del citado Impuesto.
  - En el caso de encontrarse en alguno de los supuestos de exención (respecto del último ejercicio), previstos en el artículo 82.1 del Real decreto legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley reguladora de las Haciendas Locales, esta circunstancia debe acreditarse mediante certificado de la Agencia Tributaria del Estado o cualquier otra documentación justificativa de esta circunstancia.

- Documentación justificativa de la solvencia económica y financiera y de la técnica o profesional y de las solvencias aportadas para ser evaluados mediante los criterios de selección de licitadores, de conformidad con lo señalado en el presente documento regulador.

En caso de agrupación de operadores económicos, cada uno de los empresarios deberá acreditar solvencia económica, financiera, técnica y profesional. A los efectos de la determinación de la solvencia de la agrupación temporal y de la determinación de los umbrales mínimos de solvencia de cada uno de los licitadores se acumularán las características acreditadas por cada uno de los entes integrantes de la agrupación.

- Las empresas de 50 o más trabajadores deberán cumplir el requisito de que al menos el 2 por ciento de sus empleados sean trabajadores con discapacidad, de conformidad con el artículo 42 del Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, en las condiciones que reglamentariamente se determinen; o en el caso de empresas de más de 250 trabajadores, cumplir con la obligación de contar con un plan de igualdad conforme a lo dispuesto en el artículo 45 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad de mujeres y hombres. La acreditación del cumplimiento de la cuota de reserva de puestos de trabajo del 2 por ciento para personas con discapacidad y de la obligación de contar con un plan de igualdad se hará mediante la presentación de la declaración responsable a que se refiere el artículo 140 LCSP. La acreditación se hará mediante la presentación de la declaración responsable a que se refiere el artículo 140 LCSP.

- Declaración jurada de ubicación y subcontratación de servidores, en el caso de que durante la ejecución del proyecto se vayan a tratar datos personales.

- Declaración sobre domicilio fiscal del subcontratista.

- Sí se considerará necesario porque no obre en el expediente acuerdos firmados con las empresas subcontratistas.

- Garantías definitivas conforme lo previsto en el apartado de garantías asociadas al contrato.

- Propuesta de planificación de la ejecución económica del proyecto de I+D, calendarizada por anualidades, indicando la previsión de los hitos de pago correspondientes a la

finalización satisfactoria o con éxito de las etapas del proyecto, según se establece más adelante en el presente documento regulador.

- Propuesta de calendarización de los desembolsos de los *royalties*, que cumplirá las siguientes condiciones:
  - El primer pago se realizará al día siguiente de la finalización del proyecto de I+D correspondiente.
  - El resto de los pagos se realizarán con carácter anual a partir del primero.

El Órgano de Contratación encomendará a la Comisión de Contratación la comprobación de la posesión y de la validez de dicha documentación. En el caso de que la Comisión observase defectos en ella, le concederá al licitador un plazo no superior a tres (3) días hábiles para que los corrija o enmiende.

Si el licitador o licitadores no presentan la documentación requerida, no la enmiendan o lo hiciesen fuera de plazo, la Comisión de Contratación entenderá que se retiró la propuesta y propondrá la adjudicación a la siguiente oferta siguiendo los criterios establecidos para la selección de las ofertas.

Examinada la documentación, el Órgano de Contratación realizará la adjudicación definitiva de los contratos a los licitadores que, habiendo recibido propuesta de adjudicación a su favor, hayan presentado la anterior documentación correctamente y en plazo.

La adjudicación definitiva deberá estar motivada e incluirá el desglose anual de las inversiones previstas por INCIBE en favor de cada uno de los adjudicatarios, con arreglo a lo indicado en este apartado.

La adjudicación definitiva se notificará los adjudicatarios y, simultáneamente, se publicará en el Perfil del Contratante de INCIBE.

El Órgano de Contratación podrá no comunicar determinados datos relativos a la adjudicación cuando considere, justificándolo debidamente en el expediente, que la divulgación de esa información puede obstaculizar la aplicación de una norma, resultar contraria al interés público o perjudicar intereses comerciales legítimos de empresas públicas o privadas o la competencia leal entre ellas, o cuando se trate de contratos declarados secretos o reservados o cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o cuando lo exija la protección de los intereses esenciales de la seguridad del Estado y así se haya declarado de conformidad con lo previsto en el artículo 154.7 de la LCSP.

3.7. Fase VI: Formalización del contrato

No podrá iniciarse la ejecución de los contratos sin su previa formalización.

El contrato se formalizará en documento que se ajuste con exactitud a las condiciones de la licitación, constituyendo dicho documento título suficiente para acceder a cualquier registro público. No obstante, el contratista podrá solicitar que el contrato se eleve a escritura pública, corriendo de su cargo los correspondientes gastos. En ningún caso se podrán incluir en el documento en que se formalice el contrato cláusulas que impliquen alteración de los términos de la propuesta de adjudicación.

El Órgano de Contratación requerirá al adjudicatario para que formalice el contrato en plazo no superior a quince (15) días naturales a contar desde el siguiente a aquel en que hubiera recibido la notificación de la adjudicación definitiva.

Para la formalización del contrato, las empresas adjudicatarias que concurriesen bajo la fórmula de agrupación temporal de empresas tienen que aportar la escritura pública de constitución de la agrupación temporal en la que conste el nombramiento de representante o apoderado único de la unión con poder bastante para ejercer los derechos y cumplir las obligaciones que se deriven del contrato o poderes mancomunados en su caso.

En todos los casos, los adjudicatarios tendrán que aportar los documentos que acrediten la constitución de las garantías indicadas en el presente documento regulador, para que se pueda formalizar el contrato.

La citada documentación será examinada por la Comisión de Contratación.

3.7.1. Contenido del contrato

El contenido del documento en el que se formalice el contrato para el desarrollo precomercial con los adjudicatarios será coherente con el contenido las ofertas adjudicadas. En particular, en cuanto a los servicios de investigación y desarrollo de la propuesta o propuestas seleccionadas el contrato deberá respetar necesariamente los siguientes aspectos respecto a los proyectos ofertados:

- El documento de formalización del contrato remitirá a las estipulaciones del presente Documento Regulador.
- El documento de formalización del contrato deberá incluir las fechas exactas para el comienzo de su ejecución y para su finalización.
- Serán parte del contrato:
  - el presente documento regulador firmado por el adjudicatario;
  - el contenido de los sobres B y C;
  - la planificación aprobada de la ejecución económica de los desembolsos de los *royalties*;
  - la calendarización aprobada de pagos de la inversión de INCIBE.

En la fase de formalización del contrato se firmarán la Declaración de Ausencia de Conflicto de Intereses (DACI) firmado por el contratista y el/los subcontratistas.

3.7.1.1. Garantías asociadas al contrato

Para responder del cumplimiento del contrato de I+D y de los compromisos recogidos en el mismo, el adjudicatario deberá constituir las garantías definitivas indicadas a continuación:

1. Garantía por el 5% del importe de la inversión de INCIBE.
2. Garantía por el 20% del importe comprometido en concepto de *royalties*.

La garantía podrá constituirse mediante depósito, seguro de caución o aval.

Cuando se trate de pequeña o mediana empresa, definida según lo establecido en el Reglamento (CE) nº 651/2014, de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayuda compatibles con el mercado común en aplicación de los artículos 107 y 108 del Tratado y no estén controladas directa o indirectamente por otra empresa que no cumpla tales requisitos se podrá solicitar que la constitución de la garantía se realice mediante retención en el precio. En cuyo caso, la retención corresponderá con los % indicados anteriormente y se realizará del siguiente modo:

a) Siempre que sea posible se retendrá el total de la garantía en la primera factura.

b) Si no fuese posible se retendrá de facturaciones sucesivas hasta completar el 5% de garantía.

La retención se hará sobre bases imponibles. Las facturas recogerán el concepto de “Retención garantía 5% o 20%”.

En caso de que se hagan efectivas sobre la garantía las penalidades o indemnizaciones exigibles al adjudicatario, éste deberá reponer o ampliar aquélla, en la cuantía que corresponda, en el plazo de quince días desde la ejecución, incurriendo en caso contrario en causa de resolución.

La garantía responderá de los siguientes conceptos:

a. De las penalidades impuestas al contratista.

b. De la correcta ejecución de las prestaciones contempladas en el contrato, de los gastos originados a INCIBE por la demora del contratista en el cumplimiento de sus obligaciones, y de los daños y perjuicios ocasionados a la misma con motivo de la ejecución del contrato o por su incumplimiento, cuando no proceda su resolución.

c. De la incautación que puede decretarse en los casos de resolución del contrato, de acuerdo con lo que en él o en esta Ley esté establecido.

La primera garantía del 5% podrán ser restituida al contratista tras los 12 meses siguientes a la finalización satisfactoria del proyecto de I+D, mientras que la segunda garantía del 20% será restituida a los 5 años de la finalización de este.

La primera de las garantías responderá de los siguientes conceptos:

- De las penalidades impuestas al contratista.
- De la correcta ejecución de las prestaciones contempladas en el contrato, de los gastos originados a INCIBE por la demora del contratista en el cumplimiento de sus obligaciones, y de los daños y perjuicios ocasionados a la misma con motivo de la ejecución del contrato o por su incumplimiento, cuando no proceda su resolución.
- De la incautación que puede decretarse en los casos de resolución del contrato.

Los supuestos y la forma de determinar la penalización se recogen principalmente en el apartado 4.13 del presente documento.

Cuando INCIBE deba decidir entre la imposición de penalidades y la resolución del contrato, la decisión debe satisfacer de la mejor forma posible el interés general que perseguía la ejecución del contrato, conforme a los principios de objetividad, eficacia y eficiencia (artículos 103.1 y 31.2 CE). Para ello se valorarán los hechos concretos que rodean al contrato y la necesidad de motivar la solución que toma.

Esta decisión tendrá algunos límites tales como:

- La imposición de penalidades –diarias–, no posibilitarán resolver el contrato hasta que estas penalidades alcancen un múltiplo del 5% del contrato.
- Derá preceptiva la resolución contractual cuando se produzca un retraso injustificado sobre el plan de trabajos establecido en el documento regulador «por un plazo superior a un tercio del plazo de duración inicial del contrato, incluidas las posibles prórrogas»; decisión que dependerá de las concretas circunstancias que concurran en el supuesto de hecho y, en particular, de si efectivamente se ejecutaría el contrato en un menor plazo, con igual calidad, con la resolución del contrato Las penalidades consideradas en conjunto no podrán superar el 50% del precio del contrato, IVA excluido.

El órgano competente de INCIBE será:

- El Equipo de Seguimiento y Control (ESC) si el importe de cada una de las penalizaciones no supere los 20.000,00 € y que en el global de las penalizaciones no se superen los 25.000,00 € y siempre que hay acuerdo con el contratista. Dicho acuerdo sobre la imposición de penalizaciones se recogerá en acta firmada por el contratista y el Equipo de Seguimiento

y Control (ESC) de INCIBE con el visto bueno de su superior jerárquico con categoría de subdirector o gerente.

- Para el resto de supuestos, el Consejo de Administración salvo que con ocasión de la aprobación de la clasificación de las ofertas, acuerda delegar en el/la directora/a general este/a las “incidencias del contrato”.
- En estos casos, se debe elevar propuesta de imposición de penalizaciones elaborada por el Equipo de Seguimiento y Control (ESC). Se realizará trámite contradictorio con el contratista. Se requiere acuerdo de imposición de penalizaciones que firmará el órgano de contratación en que se reflejará la voluntad de este. En caso, de ser necesario se reflejará lo procedente en relación a la incautación y restablecimiento dela garantía.
  Cuando no haya acuerdo con el contratista, en todo caso, se elevará propuesta de penalizaciones y se seguirá procedimiento contradictorio que finalizará con acuerdo del Órgano de Contratación (Consejo de Administración o Director/a General por delegación).

4. EJECUCIÓN DEL CONTRATO

Durante la ejecución de los contratos derivados de la aplicación del presente documento regulador, INCIBE podrá matizar y completar lo descrito en este apartado, con los contratistas, en cualquier momento de la vida de estos.

4.1. Planificación inicial y reunión de lanzamiento

En el primer mes del comienzo del contrato se celebrará una reunión de lanzamiento que tendrá al menos los siguientes objetivos:

- Presentación del equipo de trabajo por parte del contratista y del equipo de seguimiento, según se establece a continuación, de INCIBE. El contratista propondrá un coordinador general del proyecto I+D que será el primer interlocutor de INCIBE. Deberá tener un perfil y experiencia profesional adecuados. INCIBE se reserva el derecho de rechazar la propuesta, de forma motivada y solicitar un nuevo interlocutor.
- Acordar la gestión documental del proyecto, que seguirá las directrices comunicadas por INCIBE en la reunión de lanzamiento, especialmente garantizando el intercambio seguro de documentación, que deberán observarse durante toda la ejecución del contrato.
- Establecer un calendario inicial de las reuniones de seguimiento del proyecto, entre INCIBE y el contratista.
- Establecer los contenidos mínimos obligatorios de reporte general a INCIBE del avance del proyecto, por parte del contratista, que deberán de cumplir siempre los plazos que indique previamente INCIBE.

Durante la reunión de lanzamiento, el contratista deberá presentar firmados los siguientes documentos:

- Documento sobre la seguridad de la cadena de suministro.
- Documento de Requisitos Específicos de Acceso.
- Normativa de Buenas Prácticas para Entidades.
- Otros documentos que se estimen necesarios.

4.2. Gestión, seguimiento y control de la ejecución del contrato

4.2.1. Órganos de gestión, seguimiento y control

Se establecen los siguientes órganos de gestión, seguimiento y control para la ejecución del objeto de la presente contratación, con el consiguiente grado de jerarquización:

- El Órgano de Contratación.
- El Equipo de Seguimiento y Control (en adelante, ESC).

Los dos órganos podrán estar apoyados en cualquier momento por cualquier asistencia técnica, asesor externo independiente o representantes de los usuarios finales (aportados por el adjudicatario o por INCIBE) que estime el Órgano de Contratación en cualquier momento de la duración del contrato. La participación de estos apoyos externos será comunicada por el Órgano de Contratación u órgano en el que delegue, con la debida antelación al contratista.

4.2.1.1. El Órgano de Contratación

El Órgano de Contratación será el Consejo de Administración de INCIBE sin perjuicio de las delegaciones específicas que pueda realizar en el Director General.

Serán competencia del Órgano de Contratación, entre otras:

- La aprobación de la certificación del cumplimiento de las fases, en los términos establecidos más adelante, para proveer al pago.
- La autorización de sustitución de los subcontratistas.
- En el supuesto de que en algún contrato estén trabajando varias empresas, la autorización de sustitución de una de las empresas.
- La autorización de cambios propuestos en el contrato.
- La designación de los componentes del ESC.
- Cualquiera otra competencia que se deduzca del contrato y que no estuviera asignada expresamente a otro órgano.

4.2.1.2. El Equipo de Seguimiento y Control (ESC)

El ESC, que podrá estar formado por una o más personas de INCIBE, desempeñará funciones similares al responsable del contrato en el ámbito de aplicación de la LCSP.

No podrá formar parte del ESC personal que tenga relación profesional o conflicto de intereses con el contratista.

El ESC podrá consultar tanto a representantes de los distintos departamentos de INCIBE como a expertos externos cuyo conocimiento sea relevante para el seguimiento y control del contrato, o representantes de los usuarios finales (tanto aportados por el adjudicatario como los que pueda aportar INCIBE).

Dentro del ESC se designará a la persona que será responsable del contacto con el contratista.

A nivel general, el ESC está autorizado para:

- Solicitar documentación o información al contratista, particularmente con el fin de demostrar que estos siguen cumpliendo con los correspondientes requisitos de capacidad, que no incurren en ninguna de las causas de prohibición de contratar con la Administración previstas en el artículo 71 de la LCSP y que disponen de solvencia técnica y financiera durante todo el desarrollo precomercial.
- Visitar las instalaciones del contratista o subcontratistas, previo aviso por su parte, y preguntar o requerir información de todo tipo a los empleados o subcontratistas del contratista sobre el desarrollo de los distintos proyectos.
- Programar reuniones con el contratista para discutir el desarrollo de los proyectos, ya sea en el lugar donde se está llevando a cabo los proyectos o donde decida el ESC. Estas reuniones no modificarán en ningún momento las obligaciones contractuales del contratista.
- Llevar a cabo cualquier acción para controlar el desarrollo general del proyecto de I+D y el cumplimiento específico de todos los objetivos en cualquier Etapa de los proyectos.

4.2.2. Supervisión y control de la ejecución del contrato

Durante cada etapa, la ejecución del contrato podrá ser supervisado periódicamente y revisado con respecto a los resultados esperados (resultados por etapas y resultados de salida) por el ESC designado por el Órgano de Contratación, apoyándose en todo momento por entidades externas si así lo estima necesario.

Habrá reuniones periódicas de seguimiento entre el adjudicatario y dicho equipo, con una frecuencia semestral. Dicha frecuencia podrá ser modificada en todo momento por el ESC. Asimismo, el ESC podrá solicitar, con una antelación mínima de 24 horas, cuantas reuniones de seguimiento al contratista como estime oportunas.

Durante la ejecución del contrato se establecerá, por parte del ESC, la forma en que se llevarán a cabo las reuniones (presenciales, virtuales o híbridas) y su alcance. A los contratistas se les podrá pedir discutir los resultados alcanzados en el período anterior y presentar su plan de trabajo actualizado; el ESC podrá visitar las instalaciones del contratista para supervisar periódicamente los progresos; el contratista podrá visitar las instalaciones del usuario final aportado por el adjudicatario o por INCIBE (en particular, al el inicio de una etapa si se considera que facilita la posibilidad de conocer de primera mano el entorno operativo y garantizar que las soluciones sean diseñadas para que se adecuen a él). El contratista deberá cubrir sus propios costes, y por lo tanto prever el personal y los presupuestos de viaje en su propuesta.

4.2.3. Modificaciones del contrato o del proyecto

Si en cualquier momento una de las partes considera que una disposición del contrato ha de ser modificada o solicita una actualización o cambio en el proyecto de I+D, la otra parte habrá de ser informada inmediatamente por escrito, facilitando todos los detalles de la propuesta de modificación y su justificación.

Tras la recepción de la solicitud, la parte receptora podrá:

- Acordar variar el contrato siempre que dicha modificación no sea discriminatoria y no suponga un cambio sustancial del contrato, del ámbito del proyecto o del ámbito de los resultados tal como permite la jurisprudencia del Tribunal de Justicia de la Unión Europea o de la normativa imperativa tales como los principios recogidos en la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE, y en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Rechazar la solicitud y exigir la continuación del proyecto de I+D de conformidad con el contrato inicial.

Todas las modificaciones o actualizaciones que solicite el contratista se realizarán **a través del procedimiento de gestión de cambios** que se recoge a continuación y siempre que INCIBE tenga disponibilidad presupuestaria y esté conforme con la modificación que se propone.

Entre las modificaciones posibles, existirá la posibilidad de que se solicite, por cualquiera de las partes, el **aumento del valor económico del contrato en un máximo de un 20%** sobre el valor adjudicado. Dicha solicitud deberá estar motivada única y exclusivamente en un aumento del alcance del proyecto, de la funcionalidad o ambición del prototipo que se va a desarrollar durante el proyecto, o de las pruebas que se efectuarán sobre el mismo.

4.2.3.1. Procedimiento de Gestión de Cambios

Los contratistas podrán en cualquier momento solicitar y el Órgano de Contratación, u órgano en el que delegue, podrá en cualquier momento recomendar un cambio en el proyecto de I+D, de acuerdo con lo establecido en el siguiente proceso de gestión de cambios.

Si el contratista quisiera solicitar un cambio o el Órgano de Contratación recomendarlo, el representante de la parte correspondiente deberá enviar a la otra parte un breve escrito de acuerdo con el formato recogido en el *ANEXO 8. MODELO DE DOCUMENTO DE PROPUESTA DE CAMBIOS (DPC) Y RESPUESTA (R-DPC)* y *ANEXO 9. MODELO DE NOTA DE CAMBIOS EN EL CONTRATO (NCC)*, describiendo, al menos:

- El título del cambio propuesto y su número de referencia.

- Identificación del representante de la parte que realiza la propuesta y la fecha en que se realiza.
- Las razones justificativas del cambio que se solicita.
- Los detalles y alcance completos del cambio que se propone, distribuidos en los tres conceptos siguientes:
  - Impacto técnico: elementos eliminados, elementos introducidos, nuevos objetivos.
  - Impacto económico-financiero: sobre los costes del proyecto.
- Una planificación y calendario de ejecución razonable para dicho cambio, así como una propuesta de fechas para la toma de decisiones.

En el caso de cambios propuestos por el contratista, los detalles sobre cómo afecta el cambio propuesto a otros aspectos del contrato, como:

- Las cláusulas y pactos del contrato, incluida su propuesta final.
- Los contratos de subcontratación.
- Las obligaciones del contratista.
- La inversión de INCIBE y la coinversión del contratista.
- Los pagos y certificaciones.
- La planificación del proyecto.
- Los resultados esperados del proyecto.
- Los objetivos y especificaciones del proyecto.
- Los derechos sobre la propiedad industrial e intelectual.
- Y, en general, cualquier otro aspecto que se pueda ver afectado por el cambio.

Una vez enviado por correo electrónico del DPC, la parte que reciba la propuesta deberá responder al DPC por escrito de acuerdo con el modelo recogido en el *ANEXO 8. MODELO DE DOCUMENTO DE PROPUESTA DE CAMBIOS (DPC) Y RESPUESTA (R-DPC)*, y, en su caso, mantener las reuniones que sean necesarias para analizar el cambio propuesto. Con carácter general, el plazo máximo de respuesta será de dos (2) meses, a no ser que se establezca algo distinto por parte del Órgano de Contratación.

A la vista del DPC o del R-DPC enviado por el ESC al contratista, éste podrá proponer al órgano de contratación decidir entre:

- Aceptar los cambios tal y como estén descritos en el DPC o en el R-DPC, en cuyo caso las partes documentarán el cambio en el formato recogido en el anexo 9: Modelo de nota de cambios en el contrato (NCC), que será firmada por los representantes de las partes e incorporada como Adenda al contrato;
- Solicitar cambios en el DPC o el R-DPC al ESC, que éste deberá atender diligentemente;
- Rechazar el DCP o el R-DCP, en cuyo caso el contrato no será variado.

Cada NCC será numerada secuencialmente con un número denominado ‘Variación Número’.

Las partes deberán firmar la NCC, siendo efectivo desde la fecha de aceptación del cambio por ambas partes.

Los cambios que sean resultado de la aplicación de lo contenido en 4.2.2 Supervisión y control de la ejecución del contrato se documentarán igualmente mediante una NCC, de acuerdo con lo establecido en los puntos anteriores.

El ESC podrá documentar el proceso de decisión sobre los cambios técnicos mediante la documentación *ad hoc* que establezca a tal efecto, no siendo preceptivas ni las DCP ni las R-DCP en dichos casos.

En ningún caso se podrán autorizar cambios que impliquen un aumento del valor económico del contrato si INCIBE no dispone previamente del crédito necesario para afrontar dicho aumento.

En caso de aceptarse el aumento del valor económico del contrato, se aplicará el mismo el porcentaje de coinversión y de inversión en *royalties* ofertado por el contratista.

Previamente a la aceptación de un cambio vinculado a un aumento presupuestario, el contratista deberá justificar que el nuevo importe responde a valores de mercado, como requisito imprescindible para su aceptación, por parte del ESC.

4.3. Etapas de desarrollo precomercial objeto del contrato

4.3.1. Planteamiento general

Durante la ejecución de los proyectos de I+D [9] tendrán las siguientes etapas:

- Etapa 1: proyecto de ingeniería de detalle.
- Etapa 2: elaboración y validación de un prototipo.
- Etapa 3: verificación y demostración del prototipo en un entorno operacional.

4.3.1.1. Etapa 1: Proyecto de Ingeniería de detalle

En esta etapa el contratista deberá:

- Presentar un **proyecto de ingeniería** cuyo contenido deberá respetar lo indicado[10] en el ANEXO 14. CONTENIDO DEL PROYECTO DE INGENIERÍA.
- Adicionalmente, a la finalización de esta etapa el contratista entregará un **informe emitido por una entidad de validación acreditada por la Entidad Nacional de Acreditación (ENAC) o entidad equivalente** de cualquier Estado Miembro de la Unión Europea, sobre la naturaleza de las actividades (Investigación, Desarrollo, Innovación o actividades de mercado) del proyecto planteado. El objetivo de este informe será acreditar que la calificación global del proyecto sea I+D, supervisando los TRL de partida y llegada establecidos por el licitador en su propuesta y en el proyecto de ingeniería de detalle.
- Un **informe de evaluación** emitido por el o los usuarios finales aportados por el adjudicatario contratista y por INCIBE, en su caso.
- Este informe se hará con el modelo indicado en el *ANEXO 16: Informe de evaluación (usuario final - Etapa 1)*.
- Entregará el **informe final de etapa**, que evidencie de una manera clara y concreta las tareas realizadas, resultados e impactos obtenidos así como el grado de avance o progreso en el ciclo de vida previsto del proyecto. Igualmente incidentes acontecidos, su resolución, y el trabajo previsto en las subsiguientes etapas.
- Este informe deberá de respetar la plantilla y nivel de detalle que INCIBE le facilite al comienzo de la etapa.

[10] INCIBE se reserva el derecho a completar o modificar el contenido propuesto en dicho anexo.

4.3.1.2. Etapa 2: Elaboración y validación de un prototipo

En esta etapa el contratista deberá:

- **Desarrollar y entregar un prototipo** que haya alcanzado al menos el TRL 6 de acuerdo con las definiciones establecidas en el *ANEXO 10: TRL de la IECPI*.
- En función del TRL de partida, esta etapa podrá tener mayor o menor duración, la cual vendrá detallada, delimitada y justificada en el proyecto de Ingeniería presentado y acordado en la etapa anterior.
- Dicho prototipo será testeado y validado en un entorno simulado relevante, de acuerdo con el plan específico de validación de la etapa 2, incluido en el proyecto de ingeniería de detalle finalmente aprobado por INCIBE.
- Un **informe o informes de evaluación** emitidos por el o los usuarios finales aportados por el adjudicatario contratista y por INCIBE, en su caso.
- Este informe se hará con el modelo indicado en el ANEXO 17: Informe DE EVALUACIÓN (USUARIO FINAL - ETAPA 2).
- En el supuesto que el contratista finalice con esta etapa el contrato, entregará un **informe favorable de una auditoría externa contable**, en los términos que se describen en el apartado *4.6 Auditoría externa de las cuentas justificativas*.
- Actualización del **Plan específico de transferencia de resultados** que se ha incluido en el proyecto de ingeniería (ver descripción del plan en el *ANEXO 14. CONTENIDO DEL PROYECTO DE INGENIERÍA*).
- Actualización del **Plan para la dirección del proyecto** (ver descripción del plan en el ANEXO 14. CONTENIDO DEL PROYECTO DE INGENIERÍA).
- Entregará el **informe final de etapa**, que evidencie de una manera clara y concreta las tareas realizadas, resultados e impactos obtenidos así como el grado de avance o progreso en el ciclo de vida previsto del proyecto. Igualmente incidentes acontecidos, su resolución, y el trabajo previsto en las subsiguientes etapas.
- Este informe deberá de respetar la plantilla y nivel de detalle que INCIBE le facilite al comienzo de la etapa.

4.3.1.3. Etapa 3: Demostración del prototipo en un entorno operacional

Igualmente, se espera en esta etapa la participación activa de los usuarios finales aportados por el adjudicatario contratista y por INCIBE, en su caso, por lo que se deberá aportar un informe de evaluación emitido por cada uno de ellos.

En esta etapa el contratista deberá:

- **Desarrollar y entregar un prototipo** En esta etapa el contratista evolucionará el prototipo validado en la etapa 2, hasta alcanzar un TRL entre 7 y 8. Dicho prototipo será testeado en un entorno operacional, de acuerdo con el plan específico de validación de la etapa 3, incluido en el proyecto de ingeniería de detalle finalmente aprobado por INCIBE.
- Un **informe o informes de evaluación** emitidos por el o los usuarios finales aportados por el adjudicatario contratista y por INCIBE, en su caso.
- Este informe se hará con el modelo indicado en el ANEXO 18: Informe DE EVALUACIÓN (USUARIO FINAL - ETAPA 3).
- En el supuesto que el contratista finalice con esta etapa el contrato, entregará un **informe favorable de una auditoría externa contable**, en los términos que se describen en el apartado *4.6 Auditoría externa de las cuentas justificativas*.

- Actualización del **Plan específico de transferencia de resultados** que se ha incluido en el proyecto de ingeniería (ver descripción del plan en el *ANEXO 14. CONTENIDO DEL PROYECTO DE INGENIERÍA*).
- Actualización del **Plan para la dirección del proyecto** (ver descripción del plan en el ANEXO 14. CONTENIDO DEL PROYECTO DE INGENIERÍA).
- Entregará el **informe final de etapa**, que evidencie de una manera clara y concreta las tareas realizadas, resultados e impactos obtenidos así como el grado de avance o progreso en el ciclo de vida previsto del proyecto. Igualmente incidentes acontecidos, su resolución, y el trabajo previsto en las subsiguientes etapas.
- Este informe deberá de respetar la plantilla y nivel de detalle que INCIBE le facilite al comienzo de la etapa.

4.4. Cambios de etapa

4.4.1. Planteamiento general de los cambios de etapa

A la finalización de cada etapa, el ESC evaluará los resultados y documentación aportados por el contratista, aplicando los criterios de cambios de etapa que se incluyen más abajo en este apartado y elaborando un informe de cambio de etapa que elevará al Órgano de Contratación.

El resultado alcanzado por el contratista, a la finalización de cualquiera de las etapas, deberá corresponderse a alguna de las siguientes categorías:

- **Finalización no satisfactoria**: el contratista no ha ejecutado los servicios contratados previstos o los ha ejecutado de manera deficiente (con independencia del resultado obtenido).
- En este caso, no se abonará al contratista el precio ofertado para la citada etapa e implicará la resolución inmediata del contrato por parte del Órgano de Contratación.
- **Finalización sin cambio de etapa**: el contratista ha ejecutado los servicios contratados correctamente, pero, en aplicación de los criterios de cambios de etapa, no avanzará a la siguiente etapa.
- En este caso, se abonará al contratista en función de lo establecido en el apartado relativo al pago de la inversión de INCIBE e implicará la resolución inmediata del contrato por parte del Órgano de Contratación.
- **Finalización con cambio de etapa ("Finalización satisfactoria"** en el caso de la etapa 3**):** el contratista ha ejecutado los servicios contratados correctamente y, en aplicación de los criterios de cambios de etapa, avanzará a la siguiente etapa.
- En este caso, se abonará al contratista en función de lo establecido en el apartado relativo al Pago de la Inversión de INCIBE.

Por ejecución **de manera correcta**, se entenderá, entre otras cosas:

- La documentación entregada al final de cada etapa estará lo suficientemente sea detallada, completa y auto explicativa para ser entendida por evaluadores no licitadores ni familiarizados con el proyecto.
- Los informes de final de etapa muestran una idea clara y concreta de las tareas realizadas, resultados e impactos obtenidos así como el grado de avance o progreso en el ciclo de vida previsto del proyecto. Igualmente incidentes acontecidos, su resolución, y el trabajo previsto en las subsiguientes etapas.

- En el caso de una validación / demostración (para los TRL 6 y siguientes), se entenderá que:
  - La validación / demostración puede ser entendida y verificada por alguien que esté familiarizado con el tema, pero no un experto (por ejemplo, alguien con conocimiento operativo, pero no técnico).
  - La demostración muestra cómo funciona la innovación, la forma en que se puede utilizar, el valor diferencial que aporta y otras cuestiones que se estimen relevantes para el proyecto.

Antes de la finalización de una etapa, el ESC podrá requerir al adjudicatario la reorientación de los trabajos, la realización de nuevas tareas técnicas o la preparación de nueva documentación.

La finalización de la etapa 1 o 2, en las categorías "no satisfactoria" o "sin cambio de etapa" implicarán la resolución inmediata del contrato por parte del Órgano de Contratación.

4.4.2. Criterios de cambio etapa 1 a 2

Se seguirá el siguiente procedimiento para valorar este cambio de etapa:

1) En primer lugar, el ESC examinará el informe emitido por una entidad de validación acreditada por la Entidad Nacional de Acreditación (ENAC) o entidad equivalente.
   En el caso en que la conclusión obtenida tras el examen de este informe, sea que la calificación global del contrato no sea I+D, el Órgano de Contratación, a propuesta del ESC, podrá determinar la calificación de la finalización de la etapa 1 como "no satisfactoria", sin necesidad de evaluar el proyecto de ingeniería de detalle entregado, sin perjuicio del pago previsto en el apartado relativo al *4.7 Pago de la inversión de INCIBE*, relativo al pago del informe de la empresa certificadora acreditada por ENAC o entidad equivalente.
2) A continuación examinará:
   a. Los **informes** de evaluación emitidos por el o los **usuarios finales** aportados por el **contratista**.
   b. Los **informes** de evaluación emitidos por el o los **usuarios finales** aportados por **INCIBE**, en su caso.
   c. El proyecto de ingeniería.
   d. El **informe final de etapa**, que en esta etapa no se incluirá como criterio valorable, pero ha de estar aprobado por INCIBE.

El cambio de etapa 1 a etapa 2 se determinará en base a los siguientes criterios:

Criterio 1. Valoración de usuarios finales

IMPORTANTE: Se incluirá en principio la media aritmética de las valoraciones de **todos los usuarios** finales que hayan entregado su valoración firmada y completada correctamente. Pero en el caso de que haya usuarios finales aportados por INCIBE, y la puntuación otorgada por éstos, difiera en más de un 25% de la media aritmética de las puntuaciones del resto de usuarios finales, **sólo se utilizará para la valoración de este criterio la valoración del usuario final aportado por INCIBE**.

Puntuación: **de 0,00 a 20,00** puntos, que se valorará en base a la siguiente fórmula:

- $P_{UF}(n) = [(V_{UF1} + V_{UF2} + \ldots + V_{UFn}) / TotalUF] \times 0{,}20$

Siendo:

- $P_{UF}(n)$, la puntuación alcanzada para este criterio del licitador n.
- $V_{UF1}, V_{UF2}, V_{UFn}$, cada una de las valoraciones parciales de los usuarios finales.

- TotalUF, el total de usuarios finales que han entregado correctamente su valoración.

Criterio 2. Valoración del proyecto de ingeniería

Se incluirá el resultado de la valoración del proyecto de ingeniería.

Puntuación: **de 0,00 a 80,00** puntos, que se valorará en base a la siguiente fórmula:

- $P_{PI}(n) = (V_{PI}) \times 0{,}80$

Siendo:

- $P_{PI}(n)$, la puntuación alcanzada para este criterio del licitador n.
- V_{PI}, la valoración final que ha tenido el proyecto de ingeniería, según lo establecido en el ANEXO 15: Criterios para evaluar el proyecto de ingeniería.

El ESC establecerá en su informe, en base a las puntuaciones obtenidas por cada contratista y a lo establecido en la presente cláusula, la calificación final de la etapa, que podrá ser una de las siguientes opciones:

- **No satisfactoria**, ante cualquiera de los siguientes supuestos:
  - En el caso en que la conclusión obtenida tras el examen del informe de la entidad acreditada por ENAC o entidad equivalente, sea que la calificación global del contrato no sea I+D, el Órgano de Contratación, a propuesta del ESC, podrá determinar la calificación de la finalización de la etapa 1 como “no satisfactoria”, sin necesidad de evaluar el proyecto de ingeniería de detalle entregado, sin perjuicio del pago previsto en el apartado *4.7 Pago de la inversión de INCIBE*, relativo al pago del informe de la empresa certificadora acreditada por ENAC o entidad equivalente.
  - Si la puntación parcial obtenida en el *Criterio 1. Valoración de usuarios finales* fuera inferior a 5 puntos (sobre la puntuación máxima obtenible para este criterio que es de 20 puntos)**.**
  - Si la puntuación final alcanzada es inferior al 20 puntos (sobre de la puntuación máxima obtenible total que es de 100 puntos).
  - La etapa en general, no se ha ejecutado de **manera correcta**, según se indica en el apartado 4.4.1 Planteamiento general de los cambios de etapa.
- **Finalización sin cambio de etapa:** para aquellas propuestas que hayan alcanzado una puntuación entre 20 y 60 puntos, ambos incluidos (sobre de la puntuación máxima obtenible total que es de 100 puntos).
- **Finalización con cambio de etapa**: en el resto de casos, el ESC establecerá esta clasificación, incluyendo aquellas propuestas que hayan alcanzado una puntuación superior a 60 puntos (sobre de la puntuación máxima obtenible total que es de 100 puntos).

El Órgano de Contratación, de acuerdo con el informe elevado por el ESC, notificará a todos los contratistas las puntuaciones y calificaciones alcanzadas, y adoptará las decisiones oportunas.

4.4.3. Criterios de cambio de etapa 2 a 3

Los criterios para valorar los resultados la documentación aportada y sobre todo los resultados alcanzados en las pruebas realizadas al prototipo a la finalización de la etapa 2, serán los siguientes:

Criterio 1. Valoración de usuarios finales

IMPORTANTE: Se incluirá en principio la media aritmética de las valoraciones de **todos los usuarios** finales que hayan entregado su valoración firmada y completada correctamente. Pero en el caso de que haya usuarios finales aportados por INCIBE, y la puntuación otorgada por éstos, difiera en más de un 25% de la media aritmética de las puntuaciones del resto de usuarios finales, **sólo se utilizará para la valoración de este criterio la valoración del usuario final aportado por INCIBE**.

Puntuación: **de 0 a 35,00** puntos, que se valorará en base a la siguiente fórmula:

- $P_{UF}(n) = [(V_{UF1} + V_{UF2} + \ldots + V_{UFn}) / TotalUF] \times 0{,}35$

Siendo:

- $P_{UF}(n)$, la puntuación alcanzada para este criterio del licitador n.
- $V_{UF1}, V_{UF2}, V_{UFn}$, cada una de las valoraciones parciales de los usuarios finales.
- TotalUF, el total de usuarios finales que han entregado correctamente su valoración.

Criterio 2. Nivel de cumplimiento del proyecto de ingeniería

Puntuación: **de 0,00 a 25,00** puntos, que se valorará en base al grado de avance del proyecto medido en cobertura de alcance, plazos, costes y recursos empleados observados a partir del análisis de los siguientes documentos entregados en esta etapa:

- Plan específico de transferencia de resultados, correctamente actualizado.
- Plan para la dirección del proyecto, correctamente actualizado.
- Informe final de etapa.

Criterio 3. Interés y valor de los productos resultados del proyecto

Puntuación: **de 0,00 a 40,00** puntos, que se valorará en base a lo siguiente:

- Grado de cumplimiento de los **objetivos específicos del proyecto** reflejados en el proyecto de ingeniería para esta etapa 2.
- Plan específico de validación de la etapa 2 reflejado en el proyecto de ingeniería.

El ESC establecerá en su informe, en base a las puntuaciones obtenidas por cada por cada contratista y a lo establecido en la presente cláusula, la calificación final de la etapa, que podrá ser una de las siguientes opciones:

- **No satisfactoria**, ante cualquiera de los siguientes supuestos:
  - Si la puntación parcial obtenida en el *Criterio 1. Valoración de usuarios finales* fuera inferior a 10 puntos (sobre la puntuación máxima obtenible para este criterio que es de 35 puntos)**.**
  - Si la puntuación final alcanzada es inferior al 20 puntos (sobre de la puntuación máxima obtenible total que es de 100 puntos).
  - La etapa en general, no se ha ejecutado de **manera correcta**, según se indica en el apartado 4.4.1 Planteamiento general de los cambios de etapa.
- **Finalización sin cambio de etapa:** para aquellas propuestas que hayan alcanzado una puntuación entre 20 y 60 puntos, ambos incluidos (sobre de la puntuación máxima obtenible total que es de 100 puntos).

- **Finalización con cambio de etapa**: en el resto de casos, el ESC establecerá esta clasificación, incluyendo aquellas propuestas que hayan alcanzado una puntuación superior a 60 puntos (sobre de la puntuación máxima obtenible total que es de 100 puntos).

El Órgano de Contratación, de acuerdo con el informe elevado por el ESC, notificará al contratista las puntuaciones y calificaciones alcanzadas, y adoptará las decisiones oportunas.

4.4.4. Criterios de evaluación de resultados de la etapa 3

Los criterios para valorar los resultados la documentación aportada y sobre todo los resultados alcanzados en las pruebas realizadas al prototipo a la finalización de la etapa 3, serán los siguientes:

Criterio 1. Valoración de usuarios finales

IMPORTANTE: Se incluirá en principio la media aritmética de las valoraciones de **todos los usuarios** finales que hayan entregado su valoración firmada y completada correctamente. Pero en el caso de que haya usuarios finales aportados por INCIBE, y la puntuación otorgada por éstos, difiera en más de un 25% de la media aritmética de las puntuaciones del resto de usuarios finales, **sólo se utilizará para la valoración de este criterio la valoración del usuario final aportado por INCIBE**.

Se incluirá la media aritmética de las valoraciones de todos los usuarios finales que hayan entregado su valoración firmada y completada correctamente.

Puntuación: **de 0 a 35,00** puntos, que se valorará en base a la siguiente fórmula:

- $P_{UF}(n) = [(V_{UF1} + V_{UF2} + \ldots + V_{UFn}) / TotalUF] \times 0{,}35$

Siendo:

- $P_{UF}(n)$, la puntuación alcanzada para este criterio del licitador n.
- $V_{UF1}, V_{UF2}, V_{UFn}$, cada una de las valoraciones parciales de los usuarios finales.
- TotalUF, el total de usuarios finales que han entregado correctamente su valoración.

Criterio 2. Nivel de cumplimiento del proyecto de ingeniería

Puntuación: **de 0,00 a 25,00** puntos, que se valorará en base al grado de avance del proyecto medido en cobertura de alcance, plazos, costes y recursos empleados observados a partir del análisis de los siguientes documentos entregados en esta etapa:

- Plan específico de transferencia de resultados, correctamente actualizado.
- Plan para la dirección del proyecto, correctamente actualizado.
- Informe final de etapa.

Criterio 3. Interés y valor de los productos resultados del proyecto

Puntuación: **de 0,00 a 40,00** puntos, que se valorará en base a lo siguiente:

- Grado de cumplimiento de los **objetivos específicos del** proyecto reflejados en el proyecto de ingeniería para esta etapa 3.
- Plan específico de validación de la etapa 3 reflejado en el proyecto de ingeniería.
- La etapa en general, se ha ejecutado de **manera correcta**, según se indica en el apartado 4.4.1 Planteamiento general de los cambios de etapa.

El ESC establecerá en su informe, en base a las puntuaciones obtenidas por cada contratista y a lo establecido en la presente cláusula, la calificación final de la etapa, que podrá ser una de las siguientes opciones:

- **No satisfactoria**, ante cualquiera de los siguientes supuestos:
  - Si la puntación parcial obtenida en el *Criterio 1. Valoración de usuarios finales* fuera inferior a 10 puntos (sobre la puntuación máxima obtenible para este criterio que es de 35 puntos)**.**
  - Si la puntuación final alcanzada es inferior al 40 puntos (sobre de la puntuación máxima obtenible total que es de 100 puntos).
  - La etapa en general, no se ha ejecutado de **manera correcta**, según se indica en el apartado 4.4.1 Planteamiento general de los cambios de etapa.
- **Finalización con cambio de etapa**: en el resto de casos, el ESC establecerá esta clasificación, que en este caso al no existir más etapas previstas, significa **finalización satisfactoria**.

El Órgano de Contratación, de acuerdo con el informe elevado por el ESC, notificará al contratista las puntuaciones y calificaciones alcanzadas, y adoptará las decisiones oportunas.

4.5. Cláusula de adaptación al progreso técnico y conocimientos científicos

El contratista deberá ejecutar el contrato de conformidad con lo que, en cada momento, y según el progreso de la ciencia, disponga la normativa técnica, medioambiental y de seguridad que resulte de aplicación.

Esta cláusula de progreso será aplicable en todo lo relativo a los servicios de desarrollo e investigación y en general, a cualquier actividad complementaria al servicio o íntimamente ligada al mismo que esté sometida a cambios en cuanto a las exigencias de la tecnología o los medios empleados para llevarla a cabo.

En este caso, el contratista no tendrá derecho a exigir indemnización alguna, por parte de INCIBE, derivada de las cargas económicas inherentes a los trabajos para poner en práctica las citadas adaptaciones técnicas.

Pero en cualquier caso, el adjudicatario podrá informar al ESC a través del 4.2.3.1 Procedimiento de Gestión de Cambios acerca de la modificación sustancial producida y justificar el desequilibrio económico que tal progreso técnico le provoca, con el objeto de que INCIBE pueda evaluar si corresponde la modificación económica del contrato con las condiciones y dentro de los límites establecidos en el presente documento.

4.6. Auditoría externa de las cuentas justificativas

Este apartado es de aplicación a las etapas 2 y 3. Previo al **último pago previsto** por parte de INCIBE durante el contrato que puede producirse bien en la etapa 2 o bien en la etapa 3, y una vez notificado por INCIBE la resolución definitiva del estado de terminación de la etapa, se exige al contratista que presente los resultados favorables de una auditoría externa competente e independiente para la revisión de las cuentas justificativas del proyecto con el propósito de certificar que las justificaciones a presentar a INCIBE son sinceras, fidedignas y están acreditadas por los correspondientes documentos justificativos, siguiendo la normativa de aplicación de este contrato y sus cargas justificativas.

El alcance de esta **única auditoría final** se circunscribe exclusivamente a la gestión económica de todos los costes del contratista acontecidos durante el contrato. El auditor que verifique la cuenta justificativa deberá estar inscrito en el Registro Oficial de Auditores de Cuentas[11] (ROAC) ya sea individualmente o como socio ejerciente de una firma auditora. Deberá contar con los conocimientos técnicos necesarios para realizar el trabajo de una manera adecuada, con la máxima calidad y garantía.

El auditor deberá realizar la auditoría sobre la cuenta justificativa del contrato, una vez terminadas las actividades técnicas del mismo, y se hayan contabilizado todos los costes reales del mismo.

Como resultado de la auditoría, se deberán generar los siguientes documentos en idioma español:

- los términos de referencia que incluyan las características para la realización de la auditoría en virtud de las consideraciones de este contrato relativas al régimen jurídico y cargas justificativas. Debe incluir al menos el objeto del compromiso, responsabilidades, normativa aplicable de auditoría y código ético profesional, metodología o proceso a seguir para la verificación de costes elegibles, resultados e informes a generar.
- un informe independiente del auditor de conclusiones fácticas sobre los costes declarados en virtud de las consideraciones de este contrato relativas al régimen jurídico y cargas justificativas.
- El Informe de conclusiones debe incluir membrete del auditor, y estar debidamente fechado, sellado y firmado por el auditor. Debe incluir justificación del alcance efectivo de los trabajos realizados así como los hallazgos de la auditoría especificando de forma clara las conclusiones, las cuales deberán estar soportadas en documentos y papeles de trabajo que contengan la evidencia pertinente a fin de lograr una base de juicio razonable en la que apoyar los comentarios. Se relacionarán todos los gastos del proyecto considerados como costes elegibles según la normativa aplicable para este contrato.

El contenido de estos documentos deberá seguir los modelos disponibles que pueda facilitar INCIBE, o en su defecto los comúnmente utilizados para proyectos de I+D+i similares y en caso de no existir modelos de referencia se podrán utilizar los modelos de términos de referencia[12] e informe independiente de auditoría generalmente aceptados para proyectos europeos.

Los costes de esta auditoría incurridos por parte el adjudicatario se consideran costes elegibles del contrato.

4.7. Pago de la inversión de INCIBE

Los pagos de la inversión de INCIBE a los contratistas se producirán a la finalización de cada etapa, si dicha etapa ha finalizado de forma satisfactoria o con cambio de etapa, una vez:

- Se haya notificado al contratista la resolución definitiva del estado de terminación de la etapa.
- El contratista aporte la documentación necesaria para realizar el pago previsto en el contrato.
- Para los contratos que superen la etapa 1 y en el caso de ser el último pago previsto del contrato (bien en etapa 2 o 3) la presentación de los documentos resultado indicados en la sección *4.6 Auditoría externa de las cuentas justificativas*.

y si se cumplen el resto de las condiciones indicadas en el presente apartado.

[11] https://www.icac.gob.es/servicios-roac

[12] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/temp-form/report/cfs_en.docx

El Órgano de Contratación comprobará, a través del ESC y a la finalización de cada etapa, si los medios y recursos aportados por el adjudicatario han sido empleados y justificados, siendo su consumo proporcional al contenido de la etapa según el presupuesto que figura en la oferta del contratista y en el propio contrato. Comprobará también si el trabajo se ha llevado a cabo de conformidad con las disposiciones del contrato (incluyendo en particular, la verificación de si el adjudicatario ha protegido y gestionado debidamente los derechos de propiedad intelectual generados en la etapa respectiva).

Si fruto de esa comprobación, se establece que el gasto real ejecutado por el contratista es inferior al previsto, se minorará de forma proporcional el importe a abonar por INCIBE. Dicha minoración será trasladada al contratista a efectos que adapte su facturación.

Se resumen a continuación en la siguiente tabla las posibles situaciones que se puedan dar en cuanto a la planificación de pagos del contrato asociados a la finalización de cada etapa y la forma en que se regularán los citados pagos:

GASTO A VALOR DE MERCADO EJECUTADO EN LA ETAPA	PAGOS EFECTUADOS A INCIBE EN CONCEPTO DE *ROYALTIES* HASTA LA FECHA DE FINAL DE LA ETAPA	PAGO DE INCIBE CORRESPONDIENTE A SU INVERSIÓN EN EL PROYECTO DE I+D
Igual o superior a lo planificado	Igual a lo planificado	Según lo planificado
Inferior a lo planificado	Igual a lo planificado	Proporcional al gasto real
Cualquier situación	Inferior a lo planificado	No se efectúa el pago hasta que el pago en concepto de *royalties* alcance lo planificado

Tabla 3: Planificación de pagos del contrato asociados a la finalización de cada etapa

Las planificaciones de gasto a valor de mercado, pago por royalties o pagos de la inversión de INCIBE se pueden ver afectadas atendiendo al procedimiento de gestión de cambios. Tendrá validez en el momento de cada pago, la última planificación aprobada.

En ningún caso, el retraso podrá ser tal que el proyecto exceda el plazo máximo de ejecución de los proyectos, superando la fecha del 30 de junio de 2026. Si el retraso del proyecto es tal que se excede esa fecha, INCIBE no estará obligado a abonar los pagos correspondientes a ejecución posterior al 30 de junio de 2026, renunciando el contratista a cualquier reclamación en este sentido. Dada esta circunstancia, INCIBE y el contratista podrán establecer, de mutuo acuerdo, la resolución del contrato, liberando al contratista de las obligaciones que estuviesen pendientes por su lado.

Finalmente, si a la finalización de la Etapa 1, el Órgano de Contratación determina que no es satisfactoria, INCIBE abonará al contratista un único pago de 3.000 €+IVA por los servicios prestados en la citada etapa, sin posibilidad de que el contratista pueda reclamar ningún importe adicional.

El pago de la etapa 2 cuando se haya finalizado con “cambio de etapa” se realizará mediante “pago a cuenta” a expensas que la Auditoría externa (indicada en el apartado 4.6. Auditoría externa de cuenta justificativa), a realizar en la siguiente etapa, establezca la elegibilidad de los costes justificados por el contratista en la etapa 2.

Cuando el importe del coste de contrataciones y subcontrataciones asociadas al proyecto supere los 15.000 €, el beneficiario deberá presentar al menos 3 ofertas de diferentes proveedores para garantizar que el servicio o suministro se obtiene a precio de mercado. Quedan exceptuadas de este requisito contrataciones iniciadas con anterioridad a la publicación de la convocatoria

4.8. Derechos de propiedad intelectual e industrial

Los derechos de propiedad intelectual e industrial (DPII) a los que hace referencia este apartado incluyen:

i. patentes, patentes de diseños, inventos, modelos de utilidad, diseños, derechos de autor y derechos relacionados, derechos sobre bases de datos, marcas registradas, nombres comerciales, denominaciones sociales y el derecho de registrarlas;
ii. derechos sobre nombres de dominios;
iii. conocimientos técnicos;
iv. solicitudes y renovaciones de cualquiera de los derechos anteriores;
v. cualquier otro derecho que tenga un efecto similar en cualquier país del mundo;
vi. licencias o derechos contractuales sobre cualquiera de los derechos anteriores.

Los contratistas tendrán en cuenta todos los costes derivados del presente apartado en el presupuesto de sus propuestas.

4.8.1. Conocimientos previos

Los licitadores deberán presentar en sus propuestas, **dentro del sobre B**, la siguiente información en relación con los conocimientos previos:

- Declaración responsable de tecnologías y/o conocimientos a aportar.
- Declaración responsable de las licencias de terceros y sus condicionantes y limitaciones.
- Declaración responsable de la adquisición a los propietarios de cualquier conocimiento previo poseído por terceros la licencia necesaria o que se ha realizado la variación necesaria de cualquier licencia preexistente que se requiera para que la entidad contratante pueda utilizar los conocimientos previos para todos los usos previstos en este apartado, en la medida en que se suministran con o forman parte del contrato.
- Declaración de la extensión de las licencias de terceros necesarias al Órgano de Contratación, de forma gratuita y en las condiciones establecidas en la presente cláusula.

Durante la ejecución del contrato, cuando exista una variación respecto a la documentación previa presentada, los contratistas deberá notificar al Órgano de Contratación por escrito, con información completa y detallada la existencia de cualquier otro conocimiento previo que sea de titularidad propia o de terceros y que, de cualquier manera, pueda afectar al desarrollo del proyecto, a los derechos de acceso, y/o explotación correspondientes al Órgano de Contratación.

Estas notificaciones deben ser facilitadas por los contratistas con las necesarias autorizaciones y sin coste para la entidad contratante. Las contratistas deberán confirmar que adquirieron de los propietarios de cualquier conocimiento previo poseído por terceros la licencia necesaria o que se ha realizado la variación necesaria de cualquier licencia preexistente que se requiera para que la entidad contratante pueda utilizar los conocimientos previos en la medida en que se suministran con o forman parte del contrato.

La licencia o licencias referidas con anterioridad a favor de la entidad contratante se entenderán otorgadas a favor de dicha entidad o bien de cualquier otra entidad que en un futuro deba realizar los objetivos y funciones que se tengan asignadas éstas. En todo caso, los contratistas deberán responder ante la entidad contratante y mantenerlo indemne frente a cualquier reclamación de terceros en relación con una infracción debida al uso de los conocimientos previos.

En caso necesario, la entidad contratante será confirmada como usuario legítimo de los conocimientos previos correspondientes. Cuando sea necesario, se deberán sustituir las soluciones por soluciones o productos equivalentes que no infrinjan DPI de terceros.

Cada parte mantendrá la titularidad de los conocimientos previos.

Durante el periodo de vigencia del presente contrato, y siempre cuando sea estrictamente necesario para el desarrollo de las actividades del proyecto relativo al contrato, así como para el cumplimiento

de los compromisos posteriores, las partes se concederán los derechos de acceso pertinentes a dichos conocimientos previos. En ningún caso, estos derechos de acceso en relación con los conocimientos previos supondrán una cesión de su titularidad ni otorgará derecho alguno sobre los mismos a la otra parte.

4.8.2. Resultados generados

El contratista deberá informar a la entidad contratante de los resultados de su proyecto que resulten adecuados para la explotación, sean patentables o no, en el plazo máximo de un (1) mes desde su obtención. Tanto los contratistas como la entidad contratante se abstendrán de realizar cualquier publicación que pueda perjudicar a los registros de estos.

4.8.2.1. Titularidad

La titularidad de los derechos de propiedad nacidos bajo el ámbito del presente contrato pertenecerá al contratista, a no ser que se aplique la cláusula *call-back* regulada en el presente apartado, en cuyo caso la titularidad pasará a ser de la entidad contratante.

Se requerirá el consentimiento de INCIBE para la transmisión de la titularidad de los derechos de propiedad para garantizar que esta transmisión resulta coherente con lo regulado en el presente documento. Para ello, el contratista estará obligado a comunicar sus intenciones con al menos tres (3) meses de antelación INCIBE.

En concreto, en el supuesto de que la identidad del receptor de la titularidad fuera importante (contrato *intuitu personae*) o de que existieran problemas de seguridad o de autonomía estratégica, INCIBE podría no otorgar el citado consentimiento al contratista de transferir la titularidad de los derechos de propiedad o de conceder licencias exclusivas sobre ella a terceros (por ejemplo, a terceros no pertenecientes a la Unión).

Se reconocerán los derechos personales y morales que la Ley 2/2019[13], de 1 de marzo, otorga al personal investigador, tanto aquellos que formen parte del consorcio de personas físicas o jurídicas que presten servicios por parte de los contratistas, como de aquellos que participen en el proyecto por parte de la entidad contratante en la obtención de un resultado, sea o no susceptible de protección por propiedad intelectual o industrial, y en especial el de ser reconocidos como autores o inventores de los resultados.

4.8.2.2. Solicitud, gestión y mantenimiento de los derechos de propiedad

Mientras el contratista sea el titular de los derechos de propiedad nacidos bajo el presente contrato deberá cumplir lo indicado a continuación.

Los contratistas deberán velar por que los resultados del proyecto se identifiquen, registren y distingan claramente de los resultados de otras actividades de investigación y desarrollo que no estén cubiertas por el proyecto, y para que antes de cualquier publicación sobre el proyecto, las invenciones patentables que resulten del mismo estén identificadas debidamente teniendo en cuenta su patentabilidad y, cuando sea razonable hacerlo, se presenten las solicitudes pertinentes de patentes. Todas estas solicitudes de patente deberán ejecutarse con diligencia y procesarse teniendo en cuenta todas las circunstancias del caso.

[13] (Ley 2/2019, de 1 de marzo) por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017

Los contratistas serán por tanto responsables de la preparación, solicitud, gestión y mantenimiento de los derechos de propiedad nuevos generados en relación con los resultados, y correrá con todos los gastos relacionados.

Los contratistas informarán al Órgano de Contratación, **al menos anualmente y por escrito**, del estado de todos estos derechos de propiedad. Las partes decidirán de común acuerdo los territorios en los que se solicitará la protección, siendo obligatorio para las personas contratistas la protección al menos en Europa, Estados Unidos y Canadá.

Las partes cooperarán razonablemente en la gestión de los derechos de propiedad y en preparar la respuesta a cualquier comunicación, u otro tipo de acción, procedente de cualquier oficina u órgano competente, siendo, en cualquier caso, dichas actuaciones responsabilidad del contratista. Si los contratistas tienen la intención de dejar expirar o abandonar cualquier derecho de propiedad (incluyendo, pero no limitándose a la entrada en fases nacionales en cualquier país), los contratistas notificarán al Órgano de Contratación sobre dicha intención al menos sesenta (60) días antes de la fecha en la que tales derechos de propiedad expiren o sean abandonados (incluyendo, pero no limitándose al pago de anualidades y entradas en fases nacionales), y el Órgano de Contratación tendrá derecho, pero no la obligación, de asumir la responsabilidad sobre la preparación, solicitud, gestión y mantenimiento de tal derecho de propiedad.

En todo momento, se permitirá a la entidad contratante la supervisión del funcionamiento y eficacia de los procedimientos de los adjudicatarios para la gestión de los DPI cuando aquél lo considere razonablemente necesario. La entidad podrá solicitar protección adicional para los resultados si entiende que las medidas adoptadas por el contratista no son suficientes.

4.8.2.3. Defensa frente a la demanda por infracción de los derechos de un tercero

En el caso de los contratistas o cualquier persona filial, afiliada, subsidiaria o sublicenciataria sea demandada por un tercero o advertido por escrito de una posible demanda, investigación o procedimiento judicial de naturaleza similar, en base a la infracción de un derecho de propiedad intelectual o industrial de ese tercero debido a la explotación de cualquier derecho de propiedad resultado del contrato, los contratistas deberán notificarlo inmediatamente al Órgano de Contratación, proporcionándole toda la información que posea al respecto.

Todos los gastos asociados, especialmente los de los litigios, serán asumidos por los contratistas. Los contratistas tendrán la obligación de actuar en primer lugar para defender los derechos de explotación de los productos desarrollados. Si esa defensa implica la defensa de un producto desarrollado, las partes colaborarán para intentar que no resulte en litigio judicial. Si finalmente se produjera éste, el abogado que represente los intereses de las personas contratistas, filial, afiliada, subsidiaria o sublicenciataria demandada deberá elegirse de conformidad con el Órgano de Contratación.

En cualquier caso, la entidad contratante colaborará con las personas contratistas en cualquier demanda, juicio, investigación o procedimiento de naturaleza similar en la que la entidad contratante esté implicada en base a la infracción de un derecho de propiedad intelectual o industrial de ese tercero debido a la explotación de cualquier resultado y/o producto desarrollado por este contrato. Los contratistas correrán con todos los posibles costes adicionales generados a la entidad contratante por dicha colaboración, tales como los costes de viajes, dietas, formalización y registro de documentos, trabajos realizados por terceros y similares.

Cualquier cantidad recibida por los contratistas en concepto de compensación por daños y perjuicios u otras compensaciones económicas, será asignada a cubrir todos los gastos incurridos por los contratistas a tal efecto, en especial los de cualquier juicio, acción o procedimiento legal en los que pudiera haberse incurrido directamente o a través de terceros para la obtención de dichas compensaciones.

4.8.2.4. Defensa frente a infractores de los derechos de propiedad

En el caso de infracción de cualquiera de los derechos de propiedad generados bajo el presente contrato por un tercero, la parte que tenga conocimiento de ello lo notificará a la otra, proporcionándole toda la evidencia de dicha infracción de la que disponga.

Las partes cooperarán y harán los esfuerzos razonables para detener tal infracción sin llegar a litigio judicial. Si se requiere litigio, los contratistas tendrán la obligación de promover y desarrollar toda demanda, acción o procedimiento legal necesario, que se entienda razonable. Todos los gastos asociados, especialmente los de los litigios, serán asumidos por los contratistas.

El abogado que represente los intereses de los contratistas deberá elegirse de conformidad con el Órgano de Contratación, quien tendrá además el derecho a ser representado de forma independiente por un consejero o asesor legal y cuyo coste correrá a cargo de la entidad contratante.

Los contratistas notificarán al Órgano de Contratación la decisión de iniciar cualquier acción legal para defender cualquier derecho de propiedad en un período de sesenta (60) días después de haber conocido la infracción. Si dicha acción legal comprende la defensa de cualquier derecho de propiedad, las personas contratistas notificarán el Órgano de Contratación su decisión con al menos noventa (90) días de antelación a la fecha límite para iniciar esa defensa.

Los contratistas no aceptarán ni se comprometerán a aceptar ninguna solución, incluida cualquiera que se pueda alcanzar durante cualquier juicio, acción o procedimiento legal, relativa a la infracción por terceros de cualquier derecho de propiedad, sin el consentimiento previo y por escrito del Órgano de Contratación.

La entidad contratante colaborará con los contratistas en cualquier juicio, demanda, reclamación, investigación o procedimiento legal de naturaleza similar en el que los contratistas estén o vayan a estar implicados debido a infracción de cualquier derecho de propiedad por un tercero. Los contratistas correrán con todos los costes adicionales generados a la entidad contratante en relación con dicha colaboración, tales como los costes de viajes, dietas, formalización y registro de documentos, trabajos realizados por terceros y similares.

Cualquier cantidad recibida por los contratistas en concepto de compensación por daños y perjuicios u otras compensaciones económicas, obtenidas en base a la infracción por terceros de cualquier derecho de propiedad, será asignada a cubrir los gastos incurridos por las personas contratistas, en especial los de cualquier juicio, acción o procedimiento legal en los que pudiera haberse incurrido directamente o a través de terceros para la obtención de dichas compensaciones.

Si los contratistas rehúsan una acción contra la infracción por terceros de cualquier derecho de propiedad, la entidad contratante tendrá derecho de emprender cualquier pleito, acción o procedimiento legal por su cuenta para la defensa de cualquier derecho de propiedad frente a una infracción por un tercero.

4.8.2.5. Explotación

Los contratistas ostentarán con total plenitud y en exclusiva el ejercicio de los derechos de explotación de cualquier forma y modalidad de cualquier producto desarrollado bajo el contrato.

Los contratistas tendrán derecho a conceder sublicencias (exclusivas o no exclusivas) de los productos desarrollados, previa autorización por parte del Órgano de Contratación, bajo las siguientes condiciones:

1. La concesión estará supeditada a condiciones de mercado y siempre que existan necesidades justificadas de explotación, por ejemplo, por la necesidad de expansión a nuevos mercados. Este hecho no limita la capacidad de los contratistas para llegar a acuerdos de comercialización y distribución de los productos desarrollados con terceros. Para establecer el valor de mercado de las sublicencias el contratista propondrá al Órgano

de Contratación tres expertos independientes de reconocido prestigio para efectuar dicha valoración. El experto será seleccionado por el Órgano de Contratación y el coste de su valoración, será asumido por el contratista. Se permitirá una actualización anual del valor de la sublicencia atendiendo al último IPC anual publicado en España desde la fecha de la sublicencia.

Si el valor propuesto por el experto no fuese a juicio de INCIBE razonable, el Órgano de Contratación de INCIBE podrá solicitar un segundo informe a un experto de reconocido prestigio. En el caso de que la diferencia entre la valoración el primer y el segundo informe fuese superior al 15%, el Órgano de Contratación establecerá cuál de los dos valores será el utilizado o, en su caso, el valor medio de ambos.

Con el objeto de asegurar el acceso a otros operadores en la cadena de valor en situaciones en las que el mercado demande la necesidad de poder disponer de una lista suficiente de potenciales proveedores, INCIBE podrá requerir al contratista que se sublicencie de forma no exclusiva a cualquier tercero de los productos desarrollados al valor arriba indicado.

2. Antes de celebrar el contrato de sublicencia, los contratistas deben notificar al Órgano de Contratación su intención de celebrar dicho acuerdo y los términos en los que se va a otorgar la sublicencia, para recabar su autorización.
3. Los contratistas serán responsables del cumplimiento del contrato de sublicencia por parte de las personas sublicenciatarias y de la conducta de las personas sublicenciatarias, como si hubiera sido un incumplimiento del propio contratista en virtud del presente contrato. En su caso, los contratistas deberán indemnizar a la entidad contratante contra cualquier pérdida, daños, costes, reclamaciones o los gastos que se irroguen o se hayan sufrido por la entidad contratante.
4. En ningún caso, las personas sublicenciatarias podrán conceder sublicencias a terceros sin que previamente tengan conocimiento de dicha intención tanto los contratistas como el Órgano de Contratación y sin que éste último otorgue la correspondiente autorización para su concesión. En este sentido, los contratistas incluirán una cláusula en los acuerdos formalizados con las personas sublicenciatarias estableciendo la limitación anterior.
5. En concreto, en el supuesto de que la identidad del receptor de la sublicencia fuera importante (contrato *intuitu personae*) o de que existieran problemas de seguridad o de autonomía estratégica, INCIBE podría no otorgar el citado consentimiento al contratista.
6. Las personas sublicenciatarias de las personas sublicenciatarias deberán ser tratados como las personas sublicenciatarias de los contratistas a los efectos del presente contrato, tanto si se conceden los derechos directa o indirectamente por las personas contratistas y así sucesivamente.
7. Los contratistas deberán notificar al Órgano de Contratación de cualquier perfeccionamiento desarrollado por las personas sublicenciatarias como consecuencia del desarrollo de los derechos de explotación.
8. Las sublicencias son accesorias a la relación de los contratistas con la entidad contratante y se extinguirán cuando dicha relación se termine, en cualquier caso.

Sin perjuicio de lo dispuesto en párrafos anteriores, las partes acuerdan mediante este proceso de contratación la concesión a favor de la entidad contratante (INCIBE) de una licencia de uso gratuita, ilimitada e indefinida con fines propios de sus competencias o para el cumplimiento de encargos que pueda recibir por parte del Sector Público estatal, y en especial de investigación y de docencia, de las características técnicas para todos aquellos centros, servicios y establecimientos dependientes de INCIBE. Para ello, los contratistas se asegurarán de entregar toda la información y recursos técnicos y/o tecnológicos para poder usar de manera efectiva la referida licencia de uso.

La licencia referida anteriormente en favor de INCIBE se entenderá otorgada en favor de dichas entidades o bien de cualquier otra entidad que en un futuro deba realizar los objetivos y funciones que tengan asignadas éstas. Si la entidad contratante es objeto de una fusión, escisión o cualquier

otra medida de reestructuración, la licencia será transferida automáticamente –sin que se requiera consentimiento de los contratistas– a la nueva (cuando proceda) entidad legal.

Esta licencia en favor de entidad contratante deberá incluir, en la medida en la que esté relacionada con un *software*, el derecho de acceso inmediato, de desarrollo, de modificación, de transformación y de adaptación del código fuente actualizado, incluye por tanto el derecho de acceso, entre otros, al código fuente y los ejecutables.

Asimismo, INCIBE se reserva el derecho de conceder licencia de uso gratuita a favor de otras entidades del Sector Público con competencias en ciberseguridad en cualquier momento y, adicionalmente en situaciones de emergencia o claro interés público, a cualquier entidad del Sector Público en España, sin que esta concesión pueda entenderse por parte del contratista como un intento de INCIBE de desarrollar una actividad comercial que entre en competencia con la explotación de los resultados por parte del contratista.

De hecho, la licencia otorgada por el contratista a favor de la entidad contratante no permitirá el uso de los derechos con fines comerciales ni el derecho a ponerlo a disposición de usuarios en supuesto distintos a los aquí indicado. Asimismo no permite a la entidad contratante que facilite el *software* con una licencia de código abierto.

Finalmente, INCIBE se reserva el derecho de publicar el contenido de las soluciones innovadoras que se hayan desarrollado con éxito fruto del proyecto de I+D, indicando en todo momento, el contratista que posee los derechos de explotación de dichos resultados.

Adicionalmente, los contratistas se comprometen a:

- Difundir los efectos técnicos, por ejemplo, mediante la publicación, la enseñanza, o la contribución a organismos de normalización o regulación de manera que permita a terceros reproducirlos. En particular, las personas contratistas deberán realizar todos los esfuerzos necesarios para promover la difusión de los efectos técnicos del proyecto y, por consiguiente, tendrán la obligación de trabajar con otras autoridades públicas, entidades de calidad o con las organizaciones de desarrollo de estándares (SDO, del inglés *Standard Development Organizations*) que muestren interés en hacer cualquier uso de las soluciones o experiencias vividas durante este procedimiento competitivo, garantizando la difusión de los mismos, así como una posibilidad de explotación a escala, al menos europea, o la ampliación de los conocimientos en procedimientos de compra precomercial.
- Conceder los derechos de acceso a terceros, por ejemplo, mediante licencias no exclusivas, en condiciones de mercado, equitativas y razonables que permitan el acceso de estos a futuros contratos de centros, servicios y establecimientos de INCIBE. El establecimiento del valor de mercado de estas licencias será el mismo indicado en los anteriores párrafos.

La entidad contratante recibirá una contraprestación por los ingresos que se deriven de la explotación de cualquier producto desarrollado. Dicha contraprestación consistirá en el pago de *royalties* durante los 5 años posteriores a la finalización del proyecto de I+D cuyos resultados sean explotados. Dicha contraprestación equivaldrá a la aplicación del porcentaje de *royalties* ofertado por el contratista en su propuesta final, aplicado sobre el presupuesto del proyecto de I+D y se abonará anualmente, celebrándose el primer pago al día siguiente de la finalización del proyecto.

En el caso de producirse perfeccionamiento, el contratista deberá ofrecer a la entidad contratante un precio de licencia en las mejores condiciones comerciales previstas, y estará obligado a ofertarlo a la entidad contratante en procesos de licitación de esta en los que el perfeccionamiento tenga un encaje razonable.

Los contratistas aceptan que los derechos de explotación concedidos por la entidad contratante en el presente contrato no le otorgan derecho alguno para proveer cualquiera de los productos desarrollados de manera gratuita, a precio fuera mercado o a cambio de retribuciones no autorizadas, entre las que se encuentran aquellas:

- Que tienen como efecto el reducir o evitar las obligaciones de pago a la entidad contratante en virtud de este contrato.
- Que resultan, a través de cualquier actividad, en una retribución (dineraria o no), beneficio monetario o de cualquier otra índole para los contratistas, cualquier tercero asociado a este, las personas filial, afiliada o subsidiaria, o empresa perteneciente al grupo empresarial al que pertenezcan las personas contratistas, sin que se produzca la compensación debida a la entidad contratante a la luz de las condiciones del mercado en cada momento.

Nada de lo estipulado en párrafos anteriores impide que los contratistas puedan llegar a acuerdos de codesarrollo con terceros, que se traduzcan en la recepción de un beneficio monetario o no monetario o de un beneficio para dichas partes, si esos acuerdos se alcanzan en una transacción en condiciones de libre competencia y no tiene el efecto de evitar o reducir la obligación de pagar a la entidad contratante una contraprestación bajo este contrato.

4.8.2.6. Retrasos e impagos

Los retrasos en el cumplimiento de las obligaciones de pago del contratista otorgan derecho la entidad contratante a percibir intereses moratorios que serán del 2% anual más el Euribor a tres meses en el momento de emisión de la correspondiente factura por la entidad contratante correspondiente a los *royalties*. El interés moratorio será calculado sobre el balance pendiente de pago desde el comienzo del retraso.

4.8.2.7. Mantenimiento de registro y derecho de control del Órgano de Contratación

Los contratistas deben guardar fiel registro (junto con la documentación que lo respalde) en su lugar habitual de negocio de los productos licenciados fabricados, usados, vendidos y sublicenciados bajo este contrato.

Dicho registro debe ser mantenido al menos durante los diez (10) años siguientes a la finalización del proyecto, y deberán poder ser consultables durante el horario normal de oficina para su examen por un auditor independiente o personal designado por el Órgano de Contratación. El coste de dicha auditoría correrá a cargo de la entidad contratante.

Los contratistas deberán garantizar que la entidad contratante mantiene los mismos derechos establecidos en la presente cláusula para con las personas sublicenciatarias, filiales, afiliadas y subsidiarias, y obligación de guardar los mismos registros, salvo acuerdo en contra entre las partes.

4.8.2.8. Obligaciones de explotación

Los contratistas se obligan a realizar esfuerzos objetivos y razonables para explotar de manera adecuada, suficiente y diligente los productos desarrollados según el plan de explotación de los productos desarrollados presentados en su propuesta, sujetos a criterio de adjudicación según lo establecido en el presente documento regulador.

Se considerará que los contratistas no han realizado los esfuerzos objetivos y razonables para explotar los productos desarrollados si excede en dos (2) años los tiempos planteados en el plan de explotación comercial del resultado del servicio de I+D con terceros de su propuesta por causas distintas a las de fuerza mayor, estando en este caso sujeto las personas contratistas a la penalización correspondiente descrita en el presente documento regulador.

Adicionalmente, los contratistas tendrán la obligación, durante los cinco (5) años posteriores a la adjudicación del contrato, de ofertar los resultados derivados del contrato a licitaciones de entidades europeas, donde sea razonablemente viable concurrir en condiciones de mercado.

4.8.2.9. Publicación

Cualquier publicación relacionada con los resultados requerirá de la aprobación de las partes. En todos los casos, las partes deben pedir autorización por escrito, que debe ser respondida en un plazo máximo de treinta (30) días naturales. En caso de no obtener respuesta de cualquiera de las anteriores solicitudes de permiso, se entenderá que el permiso ha sido concedido.

Ninguna de las partes tendrá el derecho de publicar o permitir la publicación de aquellos datos que incluyan conocimientos previos, así como información confidencial que se haya tenido acceso en el transcurso del desarrollo de actividades del objeto del contrato, a no ser que cuente con su autorización por escrito.

Previo a la publicación de resultados, deberán identificarse aquellos que pueden ser susceptibles de ser protegidos por propiedad intelectual y/o industrial, y proceder a su registro y protección en aquellos casos que sea viable.

4.8.2.10. Apoyo en la explotación de los resultados por parte de la entidad contratante

La entidad contratante se compromete a colaborar de manera razonable en la explotación de los resultados a los contratistas, incluyendo la posibilidad de que él mismo organice visitas o demostraciones de potenciales clientes en las instalaciones de la entidad contratante donde se estén utilizando los resultados.

4.8.2.11. Cláusula de avocación / *call-back provision*

INCIBE podrá adquirir sin coste alguno, los DPI cuando el adjudicatario o adjudicatarios no tengan éxito en su explotación por sí mismo en un plazo de 5 años.

Adicionalmente, el contratista deberá proceder a la devolución de los DPI, o *call-back provision*, para que sean transferidos a INCIBE aquellos que no puedan ser explotados por los propios contratistas en un plazo máximo de dos (2) años desde la finalización del proyecto que los ha generado, o para garantizar que los DPI no sean utilizados en detrimento del interés público representado por la Iniciativa Estratégica de Compra Pública Innovadora, por contradecir lo establecido en este documento regulador.

A este respecto, INCIBE podrá pedir información al contratista para confirmar la efectiva y adecuada explotación de los DPI por parte de éste.

En el caso de que el contratista decida renunciar a estos derechos, se lo deberá notificar a INCIBE como mínimo seis (6) meses antes de que expire el título de la propiedad del correspondiente DPI. En este caso, el contratista transferirá los DPI en cuestión, a quien sea designado por el propio INCIBE.

4.8.2.12. Régimen de penalizaciones

En caso de que las personas contratistas incumplan alguna de las condiciones establecidas en la presente cláusula, podrán aplicársele las penalizaciones que se establecen en el presente documento regulador.

4.9. Confidencialidad

4.9.1. Obligaciones de INCIBE

Sin perjuicio de la información que debe facilitarse a los licitadores en relación con las decisiones que tome INCIBE respecto a la valoración de las respectivas propuestas y la adjudicación del contrato, la entidad contratante estará sujeta, en principio, a las siguientes obligaciones de confidencialidad.

Por lo que respecta a toda la información confidencial procedente del adjudicatario, INCIBE se compromete a guardar el secreto, mantenerla en la más estricta confidencialidad y no proporcionar información confidencial alguna a terceros, excepto:

- Si el adjudicatario expresa su conformidad por escrito.
- Si esta información está destinada a empleados, representantes, evaluadores o personas de la entidad contratante o cualquier otra entidad que participe activa o directamente en el proyecto.
- Si la normativa así lo establece.

No obstante lo que se dispone anteriormente, los licitadores y el adjudicatario autorizan específica y expresamente a la entidad contratante a publicar y revelar las mejores prácticas en relación con el procedimiento de contratación precomercial extraídas de la participación como observador y evaluador del proyecto.

Además, mediante la presentación de sus propuestas, los licitadores otorgan de forma excepcional a INCIBE permiso para compartir el acceso a los resultados del procedimiento con otras autoridades y poderes adjudicadores, tras la terminación de este, a fin de educarlas para futuras licitaciones. INCIBE dará a los licitadores interesados aviso previo de la información que tiene intención de compartir con otras autoridades o poderes adjudicadores antes de su divulgación. Si los licitadores consideran que la información que se compartirá incluye información confidencial, se lo deben notificar a INCIBE. INCIBE no puede revelar la información confidencial sin el consentimiento previo del licitador o licitadores a los que se refiere dicha información.

De la misma forma, INCIBE promoverá el interés por los resultados del proyecto entre otras autoridades y poderes adjudicadores para fomentar su éxito comercial.

4.9.2. Obligaciones del contratista

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar ni utilizar con fin distinto al que figura en este documento regulador, ni tampoco ceder a otros ni siquiera a efectos de conservación, sin el previo consentimiento por escrito de INCIBE. Se considerará información confidencial cualquier información a la que el contratista acceda en virtud del contrato o como consecuencia de su ejecución, que con tal carácter se indique.

El adjudicatario ratifica que se debe a los principios de buena fe, sigilo, profesionalidad y confidencialidad y se compromete a no divulgar, transmitir, revelar, comunicar, filtrar o, en general, dar conocimiento directa o indirectamente a otra persona empresa o institución de cualquier información confidencial de uso interno de INCIBE, o de sus clientes o de sus empresas colaboradoras a las que haya tenido acceso para la realización de los trabajos objeto del contrato.

El contratista informará a su personal, colaboradores, suministradores y subcontratistas de las obligaciones de confidencialidad establecidas en este documento regulador, así como de las obligaciones relativas al tratamiento automatizado de datos de carácter personal. El contratista pondrá todos los medios a su alcance para que su personal y colaboradores cumplan tales obligaciones. Cuando el contratista desee utilizar los resultados parciales o finales, en parte o en su totalidad, para su publicación como artículos, conferencias, o similares, deberá solicitar su conformidad a INCIBE mediante petición dirigida al responsable de ésta.

Se excluye de la categoría de información confidencial toda aquella que haya de ser revelada de acuerdo con las leyes o por una resolución judicial o acto de autoridad competente.

El contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato a la que se le hubiese dado el referido carácter en el presente documento o en el contrato, o que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá durante un plazo indefinido desde el conocimiento de esa información.

El contratista responderá por cualquier daño directo que pudiera resultar del incumplimiento de las obligaciones de confidencialidad previstas en el presente contrato.

A la finalización del contrato el contratista devolverá a INCIBE toda la información recibida, incluidas todas aquellas copias o reproducciones que de la misma se hubieran realizado. Asimismo, finalizado el objeto del contrato deberá eliminar o borrar toda aquella información que hubiera sido almacenada en soporte no susceptible de devolución.

4.10. Obligaciones de información y seguimiento para la evaluación

Con el fin de contribuir activamente a los fines y objetivos de la Iniciativa Estratégica de Compra Pública de Innovación, los adjudicatarios, así como sus subcontratistas, estarán obligados a colaborar activamente con INCIBE mediante la provisión de la información necesaria para la evaluación y seguimiento del impacto de sus proyectos de I+D.

La información deberá ser facilitada en el tiempo y forma que sea solicitada por el ESC. En este sentido, los adjudicatarios, en el caso que formalicen cualquier operación con terceros en relación con los resultados de su Proyecto de I+D que incluya algún acuerdo de confidencialidad, no podrán restringir en dicho acuerdo su deber de información para con el ESC. No obstante, el contratista informará a INCIBE del acuerdo de confidencialidad formalizado con el tercero e INCIBE se comprometerá a no hacer pública la información suministrada bajo esta circunstancia.

El ESC establecerá el informe modelo de seguimiento y evaluación incluyendo indicadores de los distintos resultados, efectos e impactos, así como las herramientas e instrumentos necesarios para la gestión de esta información, que sería trasladado al contratista en la reunión de lanzamiento del contrato.

El contratista presentará al ESC este informe con la periodicidad que el propio ESC establezca, informando de los resultados alcanzados en los proyectos en el marco de su proyecto y, de manera expresa, de los productos y servicios en situación de ser comercializados.

A estos efectos, el contratista presentará con la periodicidad acordada, del estado del proyecto en el que se incluirán, como anexos, al menos, los siguientes componentes:

- Informe de empleo.
- Informe de subcontratación.
- Informe de resultados obtenidos.

El contenido que deberá incluir el contratista en este informe, así como su formato, será determinado por INCIBE y podrá ser modificado a lo largo de la ejecución del contrato, con el objetivo de garantizar correctamente las labores de monitorización, seguimiento y evaluación.

El contratista se compromete a incluir los compromisos de información previstos en la presente cláusula en todos los contratos con sus subcontratistas, de manera que estos conozcan y se obliguen igualmente con los compromisos. En todo caso, el contratista será siempre responsable del cumplimiento de los compromisos por parte de sus subcontratistas.

El contratista y sus subcontratistas se comprometen a participar en cualquier actividad de difusión, divulgación o comunicación de los resultados, efectos e impactos de su Proyecto de I+D o de la Iniciativa Estratégica de Compra Pública de Innovación siempre que les sea solicitado por INCIBE.

4.11. Protección de datos

Tanto INCIBE como los licitadores o en su caso, contratistas, quedan obligados por las disposiciones de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que se adapta en base al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); y a completar sus disposiciones, y normativa de desarrollo.

Todos los datos obtenidos en el marco de la ejecución del presente contrato serán propiedad exclusiva de INCIBE y deberán ser tratados por el adjudicatario con la máxima confidencialidad. No se podrán utilizar estos datos por parte del adjudicatario salvo que así se autorice por INCIBE mediante escrito en el que se determinarán las condiciones a las que se deberá ajustar dicho uso.

4.12. Transparencia, publicidad y buen gobierno

El adjudicatario o adjudicatarios se comprometerán a colaborar para dotar a la Iniciativa Estratégica de Compra Pública de Innovación de un sistema de gestión de la transparencia y de buen gobierno que cumpla con los requisitos de las mejores prácticas internacionales en esta materia.

El contratista deberá comprometerse a ejecutar el contrato conforme a los manuales, normas y otras reglas de gobernanza que, en su caso, le exija INCIBE.

INCIBE podrá incluir en su página web un apartado concreto dedicado a la transparencia de la Iniciativa. En este caso, el contratista estará obligado a aportar toda la documentación e información que le sea solicitada y que se hará pública en dicho apartado.

En concreto, y sin carácter exhaustivo:

- Información relativa a la formalización del contrato.
- Información sobre los contratos del contratista con los subcontratistas.
- Información sobre todos los procesos de contratación de personal vinculados a cada proyecto de I+D.
- Información sobre los procesos de contratación de obras, bienes y servicios vinculados a cada proyecto de I+D.

La publicación de documentación que incluya contenido confidencial por su carácter técnico o comercial será realizada de acuerdo con el contratista y sustituyendo dicho contenido por páginas en blanco con la referencia ‘contenido técnico de carácter confidencial’ o ‘contenido comercial de carácter confidencial’.

4.13. Penalidades por incumplimiento del contrato y daños y perjuicios

4.13.1. Penalidades generales

Se establecen los siguientes incumplimientos, que se calificarán como:

1. Incumplimiento **MUY GRAVE** las siguientes actuaciones:

a. La falsedad de cualquier información incluida en los informes.

b. La comisión de 2 o más faltas graves.

2. Incumplimiento **GRAVE** las siguientes actuaciones:

a. La no presentación en plazo de los informes de seguimiento establecidos de acuerdo con lo indicado en el presente documento regulador.

b. El incumplimiento de la obligación de facilitar al ESC del contrato toda aquella documentación prevista en el documento regulador.

c. La no comunicación de cualquier circunstancia que pueda impedir conseguir los plazos y objetivos establecidos en cualquiera de los proyectos.

d. Los incumplimientos repetidos de las normas de seguridad en materia de prevención de riesgos laborales.

e. Que se cometan 2 o más faltas leves.

3. Incumplimiento **LEVE** las siguientes actuaciones:

a. El incumplimiento de cualquier obligación incluida en las condiciones de contratación no calificada como GRAVE o MUY GRAVE.

Por el incumplimiento de lo establecido en las condiciones de contratación, y con el siguiente desglose en función de la gravedad del incumplimiento, las penalidades serán:

- Falta LEVE: penalización del 0,5 por ciento del importe máximo del precio del contrato que debe abonar INCIBE en cada de las etapas (IVA excluido) por cada incumplimiento.
- Falta GRAVE: penalización desde el 1,5 por ciento del importe máximo del precio del contrato que debe abonar INCIBE en cada de las etapas (IVA excluido) por cada incumplimiento.
- Falta MUY GRAVE: penalización desde el 3 por ciento del importe máximo del precio del contrato que debe abonar INCIBE en cada de las etapas (IVA excluido) por cada incumplimiento.

En ningún caso, las penalidades podrán exceder, individual o acumuladamente, del 10 por ciento del importe del contrato.

4.13.2. Penalidades por infracción de las condiciones de subcontratación

La infracción de las condiciones de subcontratación ocasionará la imposición de una penalidad hasta del 6 por ciento del importe subcontratado, IVA excluido.

4.13.3. Penalidades por incumplimiento de pagos a subcontratistas

El incumplimiento del régimen de pagos a subcontratistas ocasionará la imposición de una penalidad del 6 por ciento del importe adeudado a aquellos (IVA excluido).

4.13.4. Penalidades por incumplimiento de la cláusula de derechos de propiedad industrial e intelectual

En el caso en que las personas contratistas no hayan realizado los esfuerzos objetivos y razonables para explotar los productos desarrollados con un exceso de plazo de dos (2) años respecto a los tiempos planteados en el plan de explotación comercial de su propuesta final por causas distintas a las de fuerza mayor, deberá abonar a la entidad contratante, en concepto de penalidades, el 2 por ciento (2%) máximo del precio del contrato que debe abonar INCIBE (IVA excluido).

En el caso de que las personas contratistas no envíen al Órgano de Contratación los informes financieros a los que se refiere el apartado sobre derechos de propiedad industrial e intelectual o no abone el importe correspondiente a los *royalties* a la entidad contratante, pasado más de un año de la obligación para efectuar dicho abono, los contratistas tendrán que satisfacer, por cada anualidad no satisfecha, en concepto de penalidad, un importe adicional equivalente a la deuda contraída por este concepto, del 20 por ciento (20%) de la citada deuda.

En el cálculo de la deuda, se tendrán en cuenta los intereses regulados en el apartado de Derechos de propiedad intelectual e industria de este documento regulador.

En el caso de que los contratistas incumplan cualquiera de sus obligaciones en lo relativo a sufragar los costes de cualquiera de las obligaciones de protección, extensión, defensa frente a terceros, etc. de los derechos de propiedad industrial e intelectual detalladas en el presente documento regulador del procedimiento deberá satisfacer, en concepto de penalidad, una cantidad equivalente al valor de mercado de dichas gestiones más un diez por ciento (10%) del máximo del precio del contrato que debe abonar INCIBE.

En el caso de que los contratistas infrinjan cualquiera de los derechos de acceso a los que la entidad contratante tiene derecho según lo regulado en el presente documento regulador del procedimiento, los contratistas deberá satisfacer a la entidad contratante, en concepto de penalidad, una cantidad equivalente al cincuenta por ciento (50%) del presupuesto del proyecto asociado a esos resultados, sin perjuicio de las posibles reclamaciones adicionales por daños y perjuicios que la entidad contratante pudiese ejercer contra ellos.

4.13.5. Daños y perjuicios

Será obligación de las personas contratistas indemnizar todos los daños y perjuicios que se causen a terceros como consecuencia de las operaciones que requiera la ejecución del contrato.

4.14. Causas generales de resolución

INCIBE puede notificar por escrito en cualquier momento la resolución del contrato y no quedará sujeta a responsabilidades por ningún daño, pérdida o coste que se pueda producir como resultado o a causa de esta resolución si:

a) El contratista no supera los cambios de etapa según se establece en el presente documento regulador.
b) El adjudicatario se declara en situación de insolvencia en cualquier procedimiento o concurso.

La declaración de insolvencia en cualquier procedimiento y, en caso de concurso, la apertura de la fase de liquidación, darán siempre lugar a la resolución del contrato.

En caso de declaración de concurso y mientras no se haya producido la apertura de la fase de liquidación, la entidad contratante podrá continuar con el futuro contrato, si los contratistas prestasen las garantías suficientes a juicio de aquélla para su ejecución.

c) El contratista incumple de forma grave, y por causa a él imputable, y es requerido por INCIBE para que lo cumpla si:
   - El incumplimiento imputado se puede subsanar y el contratista no lo hace en un periodo de treinta (30) días desde la recepción de la notificación por escrito en la que se especifica el incumplimiento y se solicita la subsanación de este.
   - El incumplimiento no se puede subsanar.
d) Los trabajos realizados por el contratista y relacionados con el proyecto no cumplen los requisitos aplicables en el contrato.
e) Se dan las causas establecidas para la resolución en el contrato.

INCIBE podrá instar inmediatamente la resolución del contrato si el contratista no estuviese dispuesto o no pudiesen continuar el contrato por cualquier razón o si se constata mediante los informes del ESC que el contratista incumple reiteradamente la consecución de un nivel de calidad aceptable en la ejecución de los trabajos relacionados con el proyecto. Si se da este caso, la entidad contratante no estará obligada a realizar ningún otro pago al contratista.

La resolución del contrato por cualquier motivo no implicará:

1. Liberar al contratista de sus obligaciones y deberes en materia de confidencialidad y protección de datos, colaboración o información, a los que viene obligado tanto él como sus agentes, directores, empleados o antiguos empleados, de conformidad con el contrato y cualquier legislación aplicable en materia de información confidencial.
2. Perjuicio o afectación de los derechos, acciones o recursos que se hayan generado antes de la resolución.

La resolución del contrato por causa imputable al contratista determinará la exigencia de los daños y perjuicios sufridos.

Las partes podrán resolver el contrato por mutuo acuerdo.

La resolución por mutuo acuerdo sólo podrá tener lugar cuando no concurra ninguna causa de resolución que sea imputable al contratista, y siempre que razones de interés público hagan innecesaria o inconveniente la permanencia del contrato. Cuando la resolución se produzca por mutuo acuerdo, los derechos de las partes se acomodarán a lo válidamente estipulado por ellas.

4.14.1. Responsabilidades del contratista

El contratista/s garantizarán y manifestarán que:

- Tendrán plena capacidad y autoridad y todas las licencias, permisos y consentimientos necesarios para formalizar y ejecutar el futuro contrato;
- El futuro contrato será ejecutado por un representante debidamente autorizado;
- No habrá acciones, demandas o procedimientos pendientes ante un tribunal u órgano administrativo que puedan afectar la capacidad del contratista de cumplir y llevar a cabo sus obligaciones en virtud del futuro contrato;
- El proyecto de I+D será llevado a cabo por personal con la adecuada experiencia, calificaciones y formación;
- Cumplirán con sus obligaciones en virtud del futuro contrato con la capacidad, precaución y diligencia debida incluyendo, a título enunciativo, pero no limitativo, la buena práctica del sector y (sin limitar la generalidad de los términos anteriores) de acuerdo con sus procedimientos internos establecidos;
- El contratista, sus empleados, directivos, administradores y agentes responderán ante la entidad contratante contra cualquier responsabilidad, reclamación, acción, demanda o procedimiento de cualquier tipo con respecto a:
    - Cualquier daño lesión a personas, que resulten o se produzcan durante, o estén relacionados con, el cumplimiento de los servicios, excepto en la medida en que dichos daños o lesiones estén motivados por un acto o negligencia de la entidad contratante.

El contratista/s será/n responsable/s de la calidad técnica de los trabajos que desarrollen y de las prestaciones y servicios realizados, así como de las consecuencias que se deduzcan para INCIBE o para terceros de las omisiones, errores, métodos inadecuados o conclusiones incorrectas en la ejecución del contrato.

Cuando tales daños y perjuicios hayan sido ocasionados como consecuencia inmediata y directa de una orden de la entidad contratante, será esta responsable dentro de los límites señalados en el ordenamiento jurídico.

En ningún caso INCIBE será responsable de los daños, pérdidas o daños indirectos o emergentes.

El contratista contratará y mantendrán con empresas aseguradoras pólizas de seguros que ofrezcan un nivel adecuado de cobertura para todos los riesgos en que pueda incurrir el contratista, derivados de la ejecución y cumplimiento del contrato por un importe equivalente al 50% del presupuesto del proyecto.

El contratista mantendrá un seguro de responsabilidad de empleador respecto del personal asignado al proyecto de acuerdo con los requisitos legales aplicables en cada momento.

El contratista entregará al ESC, previa petición, copias de todas las pólizas de seguro referidas a este proyecto u otra acreditación que confirme la existencia y el alcance de la cobertura otorgada por dichas pólizas, junto con recibos u otras acreditaciones de pago de las últimas primas debidas en virtud de estas pólizas.

Los términos de cualquier seguro o el importe de la cobertura, no exonera al contratista/s de sus responsabilidades en virtud del contrato. Será responsabilidad de los contratistas determinar la cantidad de la cobertura del seguro que sea adecuada para que pueda cubrir cualquier responsabilidad referida en esta cláusula.

4.15. Terminación de los contratos

Los contratos terminarán de forma normal por cumplimiento al completarse la última etapa prevista para cada proyecto de investigación y desarrollo, una vez finalizada, analizadas y remuneradas las correspondientes pruebas efectuadas por los contratistas y toda la vigencia de todos los aspectos regulados en el apartado de *4.8 Derechos de propiedad intelectual e industrial*.

4.16. Responsabilidades

El contratista responderá ante INCIBE, sus empleados, directivos, administradores y agentes de cualquier responsabilidad, reclamación, acción, demanda o procedimiento de cualquier tipo por lo que respecta a cualquier daño a la propiedad, incluida cualquier vulneración de los derechos de propiedad intelectual de terceros y cualquier lesión a personas que resulten o se produzcan en relación con, el cumplimiento del contrato, excepto en la medida que dichos daños o lesiones sean causa de un acto o negligencia de la entidad contratante.

4.17. Medidas anticorrupción

Los licitadores, o en su caso, contratistas deberán aplicar las medidas necesarias para asegurarse de que, en todo momento durante el procedimiento de adjudicación y durante la ejecución del contrato, sus empleados y directivos cumplen toda la normativa local e internacional en materia de prevención de la corrupción y, especialmente, el Código Penal español.

Así mismo, deberán dar estricto cumplimiento al procedimiento para la prevención y lucha contra el fraude, la corrupción vinculada a la gestión de fondos europeos aprobado por la INCIBE y que se pondrá a disponibilidad de los contratistas debidamente.

INCIBE, entidad del Sector Público español, tiene naturaleza jurídico-privada (sociedad mercantil) y forma específica de Sociedad Anónima, teniendo por objeto social la gestión, asesoramiento, promoción y difusión de proyectos tecnológicos en el marco de la Sociedad de la Información. INCIBE se define como medio propio y servicio técnico de la Administración General del Estado y de sus Organismos Públicos estando obligada a realizar los trabajos que le encomienden la

Administración General del Estado y sus Organismos Públicos en las materias objeto de sus funciones. INCIBE tiene entre sus objetivos reforzar, dentro del ámbito de sus competencias, su actuación para la prevención del fraude, la corrupción y los conflictos de intereses y, en dicha medida, se compromete a mantener un alto nivel de calidad jurídica, ética y moral, y a adoptar los principios de integridad, imparcialidad y honestidad, de manera que su actividad sea percibida por todos los agentes que se relacionan con INCIBE como opuesta al fraude y a la corrupción en cualquiera de sus formas.

El Plan antifraude de INCIBE junto con unos procedimientos adecuados de evaluación del riesgo de fraude y la puesta en marcha de medidas efectivas y proporcionadas al respecto, a través de un plan de acción (cuando el riesgo neto tras el control sea «importante» o «grave»), son elementos fundamentales de la estrategia de INCIBE contra el fraude, la corrupción y los conflictos de intereses, y tiene varios objetivos:

- Evitar que en nombre o por cuenta de INCIBE, y en su provecho, sean cometidos delitos por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma. Igualmente, evitar que puedan ser cometidos delitos, en el ejercicio de las actividades sociales y por cuenta y en beneficio directo o indirecto de INCIBE, por quienes, estando sometidos a la autoridad de los representantes legales y administradores de hecho o de derecho, pudieran llevar a cabo tales hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.
- Establecer los mecanismos para que, en caso de que, pese a esta función preventiva, las personas mencionadas cometiesen delitos, poner éstos de forma inmediata en conocimiento de la autoridad competente, cumpliendo así INCIBE con el deber de denuncia que establece la legislación vigente.
- Manifestar de manera clara y eficaz el compromiso institucional de INCIBE con el establecimiento de mecanismos de lucha contra el fraude, la corrupción y el conflicto de interés.
- Implementar sistemas de gestión del cumplimiento eficaces que ayuden a alcanzar los objetivos perseguidos por los fondos europeos, dando así cumplimiento a las obligaciones que el artículo 22 del Reglamento (UE) 241/2021 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, impone a España en relación con la protección de los intereses financieros de la Unión como beneficiario de los fondos MRR, toda entidad, decisora o ejecutora, que participe en la ejecución de las medidas del PRTR deberá disponer de un “Plan de medidas antifraude” que le permita garantizar y declarar que, en su respectivo ámbito de actuación, los fondos correspondientes se han utilizado de conformidad con las normas aplicables, en particular, en lo que se refiere a la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses.
- Mejorar la gestión de los recursos públicos.
- Fomentar y destacar la integridad de la actuación de la entidad como un aspecto especialmente indispensable.

4.18. Idioma

Toda la documentación que los operadores económicos aporten a INCIBE, en cualquier momento del procedimiento, deberá estar redactada en español, salvo que INCIBE autorice expresamente el uso de otro idioma.

4.19. Moneda

Todas las indicaciones monetarias de las propuestas deberán estar expresadas en euros, sin incluir el IVA.

4.20. Cómputo de plazos señalados por días

A efectos de los cálculos de plazos señalados por días, se considerará que los días son naturales (salvo que el documento regulador señale expresamente días hábiles). No obstante, si el plazo finaliza en día inhábil, se considerará prorrogado hasta el día hábil siguiente, de conformidad con la normativa de aplicación.

4.21. Principio “no causar un daño significativo”

Los contratistas, así como sus subcontratistas, estarán obligados en todo momento al cumplimiento del principio de “no causar un perjuicio significativo” a alguno de los objetivos medioambientales durante la ejecución del proyecto, de conformidad con el artículo 5 del citado Reglamento (UE) 2021/241, en relación con el artículo 17 del Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo, de 18 de junio de 2020, relativo al establecimiento de un marco para facilitar las inversiones sostenibles y por el que se modifica el Reglamento (UE) 2019/2088.

En particular, vendrán obligados a la realización de las evaluaciones y a la presentación de la documentación justificativa que INCIBE pueda reclamarles para justificar el cumplimiento de este principio.

4.22. Imagen corporativa, imagen de los fondos, protocolo de negocios y publicaciones

4.22.1. Imagen corporativa

El Órgano de Contratación informará a los contratistas acerca de sus obligaciones de comunicación y utilización de la imagen de INCIBE en los equipos, materiales e instalaciones empleados en el futuro contrato.

Los contratistas se comprometen a cumplir dichas obligaciones.

4.22.2. Logotipos y marcas

El contratista recibirá del Órgano de Contratación unas instrucciones de comunicación relacionadas con el uso de los logotipos de la Unión Europea, de *Next Generation EU*, del Plan de Recuperación, Transformación y Resiliencia y cuales quiera otros que resulten aplicables al proyecto.

El contratista se compromete a seguir dichas instrucciones en cualquier actividad de comunicación, divulgación o difusión del proyecto, reconociendo que conoce la transcendencia del uso correcto de dichos logotipos y del cumplimiento de las obligaciones impuestas por la Unión Europea al respecto.

En todo caso, el contratista no podrá hacer uso del nombre, logotipo o cualquier signo distintivo o material que le haya facilitado INCIBE para el cumplimiento de las obligaciones derivadas del presente contrato fuera de las circunstancias y fines de éste ni una vez terminada la vigencia de este.

4.22.3. Visitas de clientes

El contratista dispondrá en sus instalaciones del equipamiento necesario para la atención a clientes públicos y privados que puedan estar interesados en conocer el proyecto y sus desarrollos.

4.22.4. Publicaciones

Sin perjuicio de lo establecido en la cláusula relativa a los derechos de propiedad intelectual e industrial, durante el plazo de duración del contrato y durante un período de cinco (5) años después de su finalización, cualquier publicación y/o comunicación escrita u oral o cualquier otro tipo de divulgación en cualquier medio o forma relativa a los servicios o los resultados (en adelante, publicación) por parte del contratista deberá ser notificado a la entidad contratante.

El contratista debe entregar una copia de cualquier proyecto de publicación a la entidad contratante:

- Para una publicación escrita, en el mismo momento de la presentación al editor para su publicación o, como mínimo, veinte y ocho (28) días naturales antes de la fecha pretendida de la publicación, la que sea anterior;
- Para una comunicación oral o cualquier otro tipo de divulgación, tres (3) días hábiles antes de la fecha estimada de la presentación en el organizador de una reunión científica u otro tipo de acto.

El contratista, a petición de la entidad contratante, ha de eliminar cualquier información confidencial antes de la divulgación que pretenda.

Con sujeción a las disposiciones en materia de confidencialidad, INCIBE podrá en cualquier momento divulgar, publicar o compartir libremente con el público los resultados y cualquier lección aprendida del proyecto de I+D, previa notificación por escrito al contratista de la intención de publicar o compartir con el público, siempre que no ponga en riesgo la protección de cualquiera de los derechos de propiedad intelectual del proyecto.

Cualquier publicación que resulte del trabajo que se realice en virtud del contrato debe reconocer el apoyo financiero de la entidad contratante e incluir la cláusula de exoneración de responsabilidad que la misma exija o, a falta de instrucciones de esta, un aviso del como el siguiente:

“La presente publicación ha sido resultado de los servicios y trabajos realizados con cofinanciación del S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE). El contrato se ha financiado con fondos del Plan de Recuperación, Transformación y Resiliencia procedentes del Mecanismo de Recuperación y Resiliencia de la Unión Europea. Las opiniones expresadas en esta publicación son de los autores y no necesariamente las de la entidad de cofinanciación”.

4.22.5. Actividades de comunicación y difusión obligatorias

El contratista estará obligado a participar en todas las actividades de comunicación y difusión diseñadas por INCIBE.

Ninguna de las actuaciones de comunicación podrá poner en riesgo la protección de los resultados de los proyectos según se establece en el apartado relativo a los derechos de propiedad intelectual e industrial.

Con carácter general, los contenidos y formatos de las actividades de comunicación en las que participe el contratista serán coordinadas con la persona o el departamento de INCIBE que indique el Órgano de Contratación.

ANEXO 1. RETOS

RETO 01: LUCHA CONTRA LOS *INSIDERS*

MOTIVACIÓN

La protección del ecosistema empresarial está contemplada en la Estrategia Nacional de Ciberseguridad de 2019. Con el objetivo de proteger a las organizaciones se plantea el presente reto que pretende dar solución a una de las amenazas que más preocupa a las organizaciones: las amenazas internas o *insiders* constituidas por el propio personal de la organización o terceros contratistas quienes están en una situación privilegiada con acceso directo/interno a sistemas de información para realizar ataques que evaden la clásica seguridad perimetral o se aprovechan de su posición en la empresa. Según el informe[14] de ENISA que ofrece una visión general de este tipo de amenazas, el 88% de las organizaciones encuestadas reconoce los *insiders* como un motivo de alarma.

Los hallazgos de este informe dejan de manifiesto la necesidad de encontrar soluciones innovadoras[15] para mitigar esta amenaza que sean incluidas en la estrategia de seguridad y protección de datos de las organizaciones.

Igualmente la ENISA identifica en 2020 la amenaza de los insider como el riesgo 9 dentro de los 15 más importantes y con una tendencia en crecimiento.

OBJETO

Descripción del reto

SOLUCIONES INNOVADORAS PARA DETECTAR Y PROTEGER A LAS ORGANIZACIONES Y SUS DATOS Y RECURSOS FRENTE A LOS *INSIDERS O AMENAZAS INTERNAS*

Problema a resolver

Un ***insider***, también conocido como **amenaza interna, es un riesgo que se origina dentro de cualquier organización.** Podríamos definir a un *insider* como cualquier persona que trabaja o ha trabajado pero no se le ha restringido el acceso, en una organización y cumple los siguientes requisitos:

- Tener o haber tenido acceso, de manera autorizada, a la red, a los sistemas o a los datos de una empresa.
- Haber excedido o usado, intencionalmente, ese acceso de manera que haya afectado, negativamente, a la confidencialidad, integridad o disponibilidad de la información, los sistemas o los recursos de la organización.

Las motivaciones pueden ser muy variadas y aunque la principal de ellas es la económica, también hay otras como: el espionaje industrial, la venganza o el desconocimiento por parte del empleado.

Las amenazas internas se pueden clasificar según sus razones y objetivos:

[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-insider-threat

[15] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

a) los agentes internos descuidados que manejan mal los datos, incumplen las políticas de uso e instalan aplicaciones no autorizadas;
b) los agentes internos que roban información en nombre de externos;
c) los agentes internos descontentos que buscan perjudicar a la organización;
d) los agentes internos malintencionados que utilizan los privilegios existentes para robar información para obtener un beneficio personal;
e) los agentes internos irresponsables que comprometen la seguridad mediante inteligencia, uso indebido o acceso malicioso a un activo o su utilización desde dentro de la organización.

Por agentes internos se engloba a trabajadores de la propia entidad, personal de terceras entidades como contratistas y proveedores de negocio, de servicios, de suministro, de mantenimiento con acceso interno físico o a través de accesos lógicos privilegiados (como *extranets*) diferenciados de los accesos externos extra perimetrales.

Dada la naturaleza de estas amenazas, su detección es bastante compleja ya que es frecuente en las empresas no considerar un ataque originado desde el interior de sus sistemas. Por tanto, se plantea como un reto la detección y protección de las organizaciones ante este tipo de ataques proponiendo soluciones innovadoras de gestión y evaluación de amenazas internas.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- **Monitorización de la actividad interna.** Lo cual incluye acceso y uso de los servicios de los sistemas de información, en especial sus activos y red de comunicación. Existen múltiples herramientas de detección pero la innovación y mejora de ellas (por ejemplo con utilización de métodos de Inteligencia Artificial) ayudará sin duda a disuadir a los *insiders* y asegurando la integridad de los datos confidenciales.
- Detección temprana de posibles *insiders*, es decir personas de este tipo de perfil o de alto riesgo, por ejemplo, a través de *People Analytics*, u**n método de investigación basado en datos cuyo objetivo es estudiar a las personas que forman parte de la organización**.

Detección y prevención de amenazas internas no intencionadas. Según los expertos en ciberseguridad el *phishing* (38%) es la mayor vulnerabilidad en el caso de las amenazas internas no intencionadas. En una posición inferior posición de la lista se encuentran el *spear phishing* (21%), la debilidad o reutilización de contraseñas (16%), las cuentas en desuso (10%) y la navegación por sitios sospechosos (7%).

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- Establecer y mantener un entorno seguro dentro de las organizaciones para evitar que se produzcan actos de sabotaje, robo o filtración de información y otros actos hostiles.
- Disuadir y prevenir las posibles amenazas internas instituyendo políticas, controles de seguridad procedimientos y programas para proteger a la organización
- Detectar comportamientos amenazantes o preocupantes e identificar a las personas que corren el riesgo de convertirse en *insiders*.
- Evaluación y seguimiento (acorde a cumplimiento normativo) de amenazas internas reales o potenciales así como efectividad de las medidas implantadas.
- Detectar y paralizar las posibles amenazas internas antes de que se conviertan en ataque, espionaje, sabotaje o robo

- Análisis del impacto generado por el ataque interno.

ALCANCE

- Para cumplir con un TRL7-8 se espera una prueba en **entorno operativo** de al menos una organización donde la solución muestre sus capacidades para la detección e identificación de *insiders*.
- El **volumen y tipología de datos** han de ser similares a los de un entorno real.
- La **duración** de la prueba de concepto será suficiente para abarcar las tipologías de operaciones habituales.
- Listado de usuarios finales:
  - Al menos una organización: sector estratégico o PYME.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 02: CRIPTOGRAFÍA AVANZADA RESISTENTES A ATAQUES CUÁNTICOS

MOTIVACIÓN

La **computación cuántica** supone un cambio de paradigma con respecto a la computación clásica, y ofrece una serie de oportunidades y retos desde la perspectiva de **ciberseguridad** que hace falta resolver. Las capacidades de este nuevo paradigma de computación presentan una amenaza frente a las técnicas y métodos actuales de cifrado, que serán totalmente vulnerables en los próximos años.

Los expertos estiman en un 20% la probabilidad de romper los mecanismos actuales en los próximos 10 años y un 90% en los próximos 20.

A diferencia de la criptografía clásica, donde la información está protegida basándose en la complejidad computacional de problemas matemáticos, en criptografía cuántica se basa en la capa física y puede, en principio, proporcionar seguridad teórica de la comunicación de la información. En este sentido, la irrupción de la distribución de claves cuánticas (QKD) como una forma de comunicación de información basada en las leyes de mecánica cuántica (en particular el principio de incertidumbre de Heisenberg y el teorema de no-clonación) hace virtualmente imposible las escuchas no detectadas. La promesa de una seguridad a largo plazo imposible de hackear, incluso en presencia de computadoras cuánticas universales de pleno uso está provocando un interés creciente en la seguridad cuántica, desde varias perspectivas.

Tras lograr un progreso significativo en los fundamentos técnicos de QKD, el siguiente paso es llevarlo a sistemas comerciales. Es importante apoyar el desarrollo de infraestructuras de comunicación dirigidas a la era de la computación cuántica y la comunicación post-cuántica. Esto requiere una inversión importante en temas como QKD, que probablemente sea la aplicación más realista de la comunicación cuántica en un futuro próximo, pero también alternativas de seguridad computacional como criptografía post-cuántica, un campo en el que Europa ha estado invirtiendo poco por ahora en comparación con Estados Unidos o China.

Además, los sistemas industriales tienen una vida útil de +30 años, por lo que los productos entregados a día de hoy se enfrentarán a esta amenaza en los próximos años. Se necesitan suites criptográficas post-cuánticas en el ámbito IT y también en OT para proteger las redes de comunicaciones y operaciones contra amenazas tanto cuánticas como clásicas.

Los intentos de construir una infraestructura paneuropea comenzaron con la "Infraestructura de comunicación cuántica" (QCI): una iniciativa respaldada por la Comisión Europea y actualmente firmada por 24 estados miembros de la UE que tiene como objetivo construir una infraestructura de comunicación cuántica paneuropea basada tanto en fibra como en satélite.

En España el proyecto Quantum Spain con la participación de 25 centros, ubicados en 14 Comunidades Autónomas cuenta con una inversión inicial de 22 millones de euros en 2021 y se prevé que alcance los 60 millones de euros de inversión a través de la participación en diferentes iniciativas europeas. Persigue desarrollar un computador cuántico de altas prestaciones que se pondrá a disposición de la comunidad investigadora para el desarrollo de la Inteligencia Artificial; se creará un servicio de acceso remoto en la nube al procesador; y se desarrollarán librerías de algoritmos cuánticos útiles (Quantum Machine Learning), aplicables a problemas reales (química cuántica, finanzas, optimización de procesos de la cadena productiva, criptografía y cualquier otro problema en diversos ámbitos), para usuarios finales tanto de empresas como de entidades públicas. Bajo el modelo de colaboración público-privada para crear un verdadero ecosistema cuántico en España diseñado de forma descentralizada para llegar a todo el territorio nacional.

Al mismo tiempo, todavía no hay una superposición completa entre las comunidades de QKD y de la seguridad clásica de las TIC, y los esfuerzos deben ser dedicados a la integración de las comunidades así como de las tecnologías correspondientes. China ya ha gastado casi mil millones

de dólares en investigación cuántica con progreso significativo en el establecimiento de enlaces QKD de largo alcance. Para evitar la dependencia global en aplicaciones altamente sensibles, es necesario desarrollar tecnología europea independiente.

Es importante señalar que los esfuerzos en el desarrollo de capacidades de comunicación cuántica aún se han visto obstaculizados por la falta de coordinación entre las iniciativas que abordan los segmentos espacial y terrestre. Además, si bien la seguridad incondicional y perpetua parecen ser las promesas de la tecnología de comunicación cuántica, cabe señalar que el desafío ha sido fomentado hasta la fecha por los físicos, mientras que los profesionales de la seguridad esencialmente se mantienen al margen de las iniciativas líderes en el campo. La posible consecuencia es que los experimentos QKD de última generación no abordan una serie de escenarios de ataque básicos, como los ataques de denegación de servicio (DoS) y los ataques de canal lateral en los nodos repetidores.

La Comisión Europea ha lanzado la iniciativa: Quantum Flagship. En materia de comunicación cuántica, es importante destacar las iniciativas punteras de los gobiernos de Austria y Alemania, así como algunos estudios teóricos realizados por la ESA y la Comisión Europea, incluido el proyecto lanzado a principios de 2020 por la CE para la definición de “Overarching System Architectures of the European Infraestructure” de comunicación cuántica.

En particular, la Comisión Europea también ha lanzado el proyecto OpenQKD, un proyecto piloto para la infraestructura QCI con el objetivo de demostrar una amplia gama de casos de uso de QKD en toda Europa. Recientemente, CEN CENELEC ha lanzado un Focus Group sobre Quantum Technology para garantizar el soporte de estándares para el despliegue de Quantum Technology en la industria.

Se espera en un futuro próximo consolidar el Backbone europeo para QKD (llegando a todos los Estados Miembros) conectando las principales infraestructuras críticas y fuertemente integrado con entornos de seguridad clásicos. Innovaciones en el área de adaptación de la ciberseguridad clásica para el advenimiento cuántico se centrará en el análisis de las tecnologías cuánticas y su impacto en los mecanismos de seguridad clásicos, así como en cómo los mecanismos clásicos (incluida la criptografía) pueden ayudar en la informática cuántica y la seguridad de las comunicaciones.

Se espera que el mercado global de criptografía cuántica crezca de 285 millones de dólares en 2018 a 950 millones de dólares para 2024, a una tasa de crecimiento anual del 15 % durante el período de pronóstico. Se prevé un mercado de criptografía cuántica muy favorecedor debido a la creciente irrupción de ciberataques en la era de la digitalización, el aumento de la inversión y financiación en ciberseguridad y la creciente demanda de seguridad de próxima generación.

En conclusión: se precisa crear nuevas suite criptográficas o robustecer la existentes con capacidades de cifrado asimétrico y simétrico resistente a los ataques de computación cuántica, siguiendo los estándares internacionales así como ser testadas y validadas en entornos de laboratorio IT y/o OT con el objetivo de definir vías de acción para acelerar su comercialización.

OBJETO

Descripción del reto

DESARROLLO DE SISTEMAS CRIPTOGRÁFICOS AVANZADOS RESISTENTES A ATAQUES CUÁNTICOS.

Problema a resolver

Creación de soluciones innovadoras con alto potencial de escalado y comercialización que provean de las capacidades criptográficas (cifrado de documentación, comunicación segura, etc.) robustas de forma ágil para necesidades genéricas IT en especial para PYMEs, como en entornos OT de sectores estratégicos.

Las soluciones deben incluir **algoritmos resistentes a ataques cuánticos**, aumentando la complejidad de los actuales o implementando nuevos métodos (criptografía post-cuántica). Igualmente pueden proveer de la capacidad de **generación y distribución de claves de cifrado aleatorias usando computación cuántica** de forma segura preservando su integridad (criptografía cuántica). Con **generación** haciendo uso de las infraestructuras cuánticas públicas disponibles desplegadas en la actualidad, integraciones con estas o despliegue de nuevas, y con **distribución** a través de redes de telecomunicaciones convencionales.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Desarrollo de una suite criptográfica resistente a ataques cuánticos y su validación a través de pilotos en entornos IT y/o OT.
- Desarrollo y despliegue de centros de distribución de claves basada en tecnología QKD (Quantum Key Distribution) para servicio de provisión de claves simétricas haciendo uso de las infraestructuras cuánticas públicas vigentes. Las claves se generan con dispositivos cuánticos que garantizan aleatoriedad y se distribuyen con métodos de cifrado post-cuánticos por múltiples canales convencionales como 5G o fibra óptica.
- Servicio criptográfico post-cuántico en la nube que permita el intercambio de claves, cifrado de documentos, comunicaciones cifradas extremo a extremo, almacenamiento de información cifrada con capacidades homomórficas y trazabilidad de operaciones y documentos.
- Soluciones innovadoras que permitan cifrado en reposo y en tránsito para el uso seguro de las capacidades de las nubes públicas.

Funcionalidades

Incluimos un listado de funcionalidades o de objetivos clave y deseables.

- Funcionalidades obligatorias.
  - Servicios criptográficos robustos basados en estándares y el estado del arte científico y normativo como el NIST Post-Quantum Cryptography Standardization Project
  - Facilidad, simplicidad y transparencia en su uso
  - Demostradores IT y/o OT testados con la participación de varios usuarios finales
- Funcionalidades deseables
  - Trazabilidad de operaciones y documentos
  - Capacidades homomórficas para operar con los datos cifrados
  - Validación por agencias regulatorias y certificadoras.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Entornos operativos IT y/o OT donde la solución muestre sus capacidades criptográficas para comunicaciones seguras, cifrado de documentos o intercambio seguro de claves.
- Prueba con tipología de datos y volumen de carga similares a los de un entorno real.
- Duración de la experimentación suficiente para abarcar las tipologías de operaciones habituales.

- Pruebas de eficiencia y rendimiento para la realización de las operaciones criptográficas
- Listado de usuarios finales:
  - Se propone disponer de pymes no tecnológicas para la prueba en entornos IT, así como operadores estratégicos para la prueba en infraestructuras OT cuasi-reales.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 03: SOLUCIONES PARA LA SEGURIDAD DE DATOS Y PREVENIR SU USO MALICIOSO

MOTIVACIÓN

La sociedad actual se basa en datos, donde es cada vez más importante detectar, recopilar, procesar y actuar sobre los datos. Por ejemplo, la mayoría, si no todas, nuestras infraestructuras críticas (energía, transporte, salud, etc.) dependen de un número cada vez mayor de sensores para brindar los servicios que esperamos.

Actualmente estamos experimentando un enorme aumento en la importancia de los datos electrónicos en la toma de decisiones. Los datos ahora no solo son la base de muchas aplicaciones autónomas, incluidos sistemas de entretenimiento, vehículos autónomos, robots industriales, recomendaciones financieras y sistemas de publicidad, pero también son la base de importantes procesos democráticos, incluidas las elecciones públicas.

Desafortunadamente, los datos creados con un propósito específico pueden convertirse en un motor de ciberataques. Por ejemplo, inyectar o usar datos corruptos en los sistemas de control de infraestructuras críticas puede interrumpir significativamente las operaciones básicas.

Existen ejemplos significativos en los que los datos y sistemas corruptos comprometen infraestructuras críticas, con un coste económico mínimo significativo (es decir, el cierre de fábricas de producción durante días) y un riesgo potencial para la vida humana (por ejemplo, el cierre de un hospital).

Desde el punto de vista del ciudadano, se puede pensar que siempre existe la opción de "excluirse" de forma voluntaria y directa de todos los procesos de recopilación de datos, esto se está volviendo cada vez más difícil. Tomemos, por ejemplo, los medidores inteligentes conectados de consumo eléctrico que están reemplazando lentamente a los contadores tradicionales en los servicios públicos. Los medidores inteligentes generan datos, usan datos y son un requisito para la gestión adecuada de la producción y distribución de energía. Por lo tanto, independientemente de los aspectos de privacidad, nos enfrentaremos al hecho de que se crearán y utilizarán datos (de uso, de consumo, etc.) que afectan de forma indirecta al ciudadano y del que no puede excluirse. Este desafío debe ser enfrentado por varios actores, entre ellos:

- Los gobiernos y los reguladores deben especificar la creación adecuada y el alcance de los datos necesarios para operar los servicios esenciales, y habilitar la auditoría, la verificación, y potencialmente la certificación.
- Los operadores de servicios necesitan
  - (i) implementar sistemas seguros de tratamiento automático de datos, de conformidad con las normas,
  - (ii) detectar brechas de seguridad relacionadas con los datos, tanto entrantes (intentos de atacar la infraestructura) y salientes (integridad de la información);
- Las organizaciones que brindan servicios basados en IA deben verificar la integridad de los datos de fuentes confiables para detectar datos envenenados de fuentes no confiables / no controlados.
- Los usuarios finales deben comprender cómo se recopilan y utilizan sus datos; necesitan ser notificados e informados sobe la recopilación de sus datos en servicios digitales con la posibilidad de poder excluirse selectivamente en los que sea posible.
- Todos deben estar atentos a la creación, propagación, y el uso de datos corruptos (o simplemente falsos). Tales datos pueden incluir noticias falsas, estadísticas corruptas e incluso falsificaciones profundas (deepfakes): medios sintéticos que son prácticamente imposibles para la mayoría de los humanos para diferenciarse de los reales.

OBJETO

Descripción del reto

SOLUCIONES PARA LA SEGURIDAD DE DATOS Y PREVENIR SU USO MALICIOSO.

Problema a resolver

Creación de soluciones innovadoras con alto potencial de escalado y comercialización que provean de las capacidades automatizadas para

- Reconocimiento y filtrado automatizados de datos falsos/envenenados (en particular, datos de entrenamiento para modelos de IA)
- Probar los sistemas basados en datos para detectar sesgos y resultados erróneos
- Mecanismos para verificar la procedencia/trazabilidad e integridad de los datos
- proporcionar a las organizaciones y ciudadanos tecnologías para identificar datos falsos (incluidas noticias falsas),
- empoderar a los ciudadanos con herramientas de gestión de datos que estén orientadas a sus propios perfiles, con el fin de asegurar y, en última instancia, controlar la difusión de datos privados o sensibles. Para ello hay que proporcionar las herramientas apropiadas que alentarán a compartir y permitirá excluirse cuando lo desee.
- proteger los procesos de toma de decisiones de las actividades de desinformación y contrainformación es una tarea vital para cualquier país y a nivel de la UE.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Soluciones innovadoras para asegurar integridad y trazabilidad de la información. Por ejemplo, a nivel documental dentro de una organización, o de forma automática en servicios como la medición del consumo eléctrico.
- Soluciones de marcas de agua persistentes en documento digital y físico.
- Soluciones esteganográficas avanzadas que permitan, en diferentes modalidades de uso, la protección de una comunicación o información y, sobre todo, de la propia existencia de esta, con algoritmos robustos y auditables aplicables tanto a contenido multimedia, como ocultación en lenguaje natural.
- Servicios de detección de noticias falsas, contenidos multimedia falsos, desinformación y de verificación de confiabilidad de fuentes y datos.
- Soluciones para el filtrado de datos erróneos o manipulados.
- Soluciones para la detección de posibles sesgos y resultados erróneos en tratamientos automáticos de información basados en IA.
- Tecnologías PET (Privacy-enhancing technologies): diseño de herramientas novedosas para proporcionar a los usuarios la funcionalidad que requieren sin exponer más información de la necesaria, y sin perder el control sobre sus datos.
- Soluciones novedosas para la detección de fugas de datos.
- Soluciones innovadoras diferenciales con respecto a las existentes en mercado, que permitan a las pymes identificar sus repositorios de datos, gestionar su seguridad en reposo

y en tránsito, así como proteger y recuperar ante contingencias conforme al marco normativo.

Funcionalidades

Incluimos un listado de funcionalidades o de objetivos clave y deseables.

- Funcionalidades obligatorias.
  - Servicios para asegurar integridad y trazabilidad de la información.
  - Servicios para la detección de datos erróneos / fraudulentos
  - Servicios para la detección de sesgos y resultados erróneos.
  - Conformidad con los estándares y regulaciones en la materia.
- Funcionalidades deseables
  - Trazabilidad de operaciones y decisiones
  - Validación por agencias regulatorias y certificadoras.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Entornos operativos IT donde la solución muestre su eficacia.
- Prueba con tipología de datos y volumen de carga similares a los de un entorno real.
- Duración de la experimentación suficiente para abarcar las tipologías de operaciones habituales.
- Pruebas de eficiencia y rendimiento para la realización de las operaciones
- Se propone disponer de entidades empresariales no tecnológicas para la prueba en entornos IT
- Debido a la transversalidad de la solución puede aplicarse a pymes, Gobierno, operadores esenciales, prestadores de servicio, ciudanía, etc.
- Listado de usuarios finales:
  - Al menos una organización representativa del mercado al que se dirige.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 04: SISTEMAS INNOVADORES PARA LA EVALUACIÓN, CUMPLIMIENTO NORMATIVO Y CERTIFICACIÓN

MOTIVACIÓN

Cada entidad u organización que desarrolla una actividad empresarial debe ser conocedora del **marco normativo** que le es de aplicación, para que de esa forma pueda asegurar que está cumpliendo con la legalidad vigente.

Dicho marco normativo puede completarse con políticas, normas, recomendaciones, estándares o buenas prácticas, y pueden tener carácter sectorial por actividad, o por ubicación geográfica de la actividad (a nivel Europeo, nacional, regional, provincial o local).

Igualmente, las normativas pueden aplicar tanto a la operación de la **actividad** (procesos) como a los **bienes y servicios** (productos) que genera.

En definitiva, es un ejercicio particular y específico de cada entidad conocer su marco regulatorio que incluya las normas tanto el de obligado cumplimiento, como aquellas de referencia a las que la entidad decide adherirse para regular su actividad o sus productos.

El control y gestión del cumplimiento efectivo del marco normativo requiere de un esfuerzo constante de cada entidad, con implicación de políticas, personas y procesos. En general se suelen incorporar sistemas de gestión integrados que incluyen estos componentes, y que de una forma homogénea permiten aplicar un ciclo de mejora continua e incremental para dar cumplimiento al marco normativo.

Existen soluciones que dan respuesta a determinadas normativas más comunes con mayor o menor grado de automatización. En algunos casos más sencillos el propio organismo regulador puede proporcionar listas de comprobación para facilitar una trazabilidad completa de lo que exige la norma. En otros casos con mayor grado de sofisticación las soluciones de mercado integran en paneles de control, un seguimiento continuo de indicadores de cumplimiento en base a medidas que extraen sondas de medición de forma continua.

En el caso de la **ciberseguridad**, asegurar el cumplimiento normativo pasa por una **evaluación** continua y exhaustiva de las garantías de seguridad y privacidad de sistemas y procesos, **certificando** que productos y servicios cumplen con el nivel exigido. Medir la ciberseguridad es por tanto crucial para comparar y evaluar diferentes sistemas y dispositivos, garantizar su nivel de cumplimiento así como para encontrar soluciones contra posibles fallos encontrados.

La aplicación de la ciberseguridad en el mundo empresarial ha seguido un enfoque basado en riesgos, para desplegar medidas de seguridad de forma proporcional al impacto en los procesos de negocio. La evaluación de riesgos sigue siendo subjetiva, ya que las métricas utilizadas para medir el nivel de seguridad pueden verse afectadas por el juicio de expertos y dependen de la comprensión de los vectores de amenazas potenciales y el impacto. Así mismo, algunas de las variables implicadas, como la probabilidad, son difíciles de medir. En este sentido, la evaluación de seguridad proporciona una manera objetiva y empírica de evaluar un sistema lo que resta subjetividad. Sin embargo, el proceso de valoración todavía se realiza manualmente y la integración entre la valoración de seguridad y la evaluación de riesgos sigue siendo un tema abierto. Además, existe la necesidad de enfoques de evaluación de riesgos capaces de agregar el riesgo en sistemas complejos y heterogéneos, reutilizando la mayor cantidad de información posible de la evaluación a bajo nivel tecnológico de componentes. Adicionalmente, la heterogeneidad existente en los mecanismos de evaluación y certificación hace que esta situación sea aún más difícil. Cada esquema utiliza diferentes criterios y métricas que pueden dar lugar a diferentes interpretaciones según el experto evaluador. Métricas y criterios bien definidos para medir la seguridad así como un alto grado de automatización también permitirán pasar de un análisis cualitativo a uno cuantitativo, lo que facilitará la comprensión de los impactos de los posibles ataques, una mejor predicción de la eficacia de las contramedidas de seguridad para fortalecer los servicios y productos.

La complejidad de la evaluación de la ciberseguridad aumenta cuando la protección de datos puede verse afectada, por ejemplo, en la evaluación y certificación de servicios en la nube. Por lo tanto, también será importante comprender cómo se relacionarán entre sí los diferentes esquemas de certificación que se espera que surjan bajo el RGPD y el Reglamento de Ciberseguridad de la UE, que busca establecer un marco de certificación europeo con un enfoque armonizado de diferentes esquemas europeos de certificación existentes.

Además, en algunos sectores, donde la seguridad es un aspecto esencial, las consideraciones de ciberseguridad deben coordinarse con otros aspectos como el funcional, la disponibilidad, la calidad, etc., lo que requiere un esfuerzo adicional para coordinar con las directivas sectoriales y otras iniciativas de estandarización relevantes para sistemas TIC, OT, IoT etc.

Para respaldar la definición y el despliegue de tales esquemas, se deben desarrollar e implementar métodos y herramientas eficaces a nivel de dispositivo, servicio y proceso del sistema. La evaluación de la ciberseguridad se beneficiará enormemente de estas herramientas lo más automatizadas posible que ayuden a la gestión de vulnerabilidades y análisis del impacto de las vulnerabilidades tanto a nivel de seguridad como de negocio, evaluar los riesgos, definir requisitos de seguridad objetivos y garantías de cumplimiento de seguridad, monitorizar continuamente la efectividad de las contramedidas de seguridad y las medidas técnicas y organizativas asociadas.

La certificación de seguridad es un medio para aumentar la confianza del consumidor y aumentar el nivel de seguridad de la oferta de productos y servicios con sello europeo. Esto requiere de una amplia adopción de los respectivos esquemas existentes, lo que sólo se logrará si los procesos son simples, el grado de automatización en la evaluación es alto, los costes son bajos y los plazos son breves.

La evaluación y certificación de las garantías de seguridad para asegurar que los productos, procesos y servicios TIC cumplen con los requisitos de seguridad especificados por el fabricante o proveedor, así como conforme a las exigencias de normativas vigentes pueden ser un valor diferenciador de las soluciones europeas al ofrecer mayor confianza en los servicios y productos digitales ofrecidos. Las necesidades específicas del mercado de los diferentes sectores, como el transporte, las finanzas, la educación, la investigación médica, por citar algunos, abren nuevos escenarios que requieran mayores garantías de seguridad, con integración de sistemas heterogéneos en un mundo cada vez más interconectado y que genera y requiere mayor volúmenes de datos.

Con la disrupción de nuevas tecnologías y la hiperconexión de sistemas se prevé un aumento continuo del marco normativo, por tanto es de esperar que se desarrollen esquemas de certificación y mecanismos de evaluación en los próximos años dirigidos a diferentes tecnologías, arquitecturas de sistemas y sectores productivos. Esto supone una conveniencia de disponer de nuevas métricas, métodos y herramientas que:

- aumenten la eficacia y eficiencia de la evaluación y certificación con alto grado de automatización particularizados para verticales y procesos específicos.
- permitan trazar la evaluación y certificación de acuerdo con el niveles de seguridad definidos por normativas y estándares;
- incluyan la certificación de cumplimiento relativos a las normativas vigentes de privacidad y protección de datos.
- sean capaces de evaluar los riesgos derivados de las vulnerabilidades HW/SW y capacidades humanas y organizacionales;
- tengan en cuenta las amenazas y los riesgos específicos de la tecnología, p. ej., aprendizaje automático contradictorio, sesgo en modelos ML, datos falsos, falsificaciones profundas y más;

- permitan una evaluación objetiva del riesgo mediante la introducción de métricas, conjuntos de datos y conjuntos de pruebas para medir la ciberseguridad así como mecanismos para descomponer riesgos hasta el nivel tecnológico del sistema;
- visualicen las garantías de seguridad de los componentes del sistema y permitan extraer conclusiones sobre sistemas completos basados en dichas garantías;
- caractericen la evidencia necesaria para evaluar la ciberseguridad de sistemas complejos y dinámicos y proporcionen las herramientas para recopilar y evaluar tal evidencia, contemplando entornos de desarrollo y despliegue complejos como los actuales.
- apoyen la evaluación continua de la seguridad durante la vida útil de un producto, servicio o proceso considerando aspectos tecnológicos (por ejemplo sistemas de software dinámicos en los que solo se incluyen partes del código conocido en tiempo de diseño) y específicos del entorno (por ejemplo, diferente vida útil, micro servicios, sistemas de distribución de energía, etc.).

Esto, a su vez, aumenta significativamente la confianza en las infraestructuras de la información y puede posicionar a Europa como líder en la protección de la vida cotidiana de los ciudadanos.

En conclusión: se precisa crear nuevas soluciones innovadoras que faciliten la evaluación y certificación del cumplimiento de los niveles de **ciberseguridad y privacidad** de procesos, productos y servicios, que den respuesta tanto a necesidades genéricas y comunes, como aquellas específicas de subgrupos de entidades de sectores concretos y líneas de actividad específica con especial atención a operadores de servicios esenciales.

De igual manera probar este tipo de soluciones en entornos de usuarios reales con el objetivo de definir vías de acción para acelerar su comercialización.

OBJETO

Descripción del reto

SISTEMAS INNOVADORES PARA LA EVALUACIÓN, CUMPLIMIENTO NORMATIVO Y CERTIFICACIÓN.

Problema a resolver

Creación de soluciones innovadoras con alto potencial de escalado y comercialización que ayuden o asistan para la evaluación, y la certificación de privacidad y (ciber) seguridad monitorizando las garantías y cumplimiento, contemplando normativas genéricas o más comunes de amplio rango de aplicación que puedan ser transversales a muchas organizaciones incluyendo pymes, como más específicas para operadores esenciales de sectores estratégicos.

Las soluciones deben incluir cierto grado de **automatización**, y **completitud** de los controles previstos en las normativas para validar el grado de cumplimiento de las mismas. Igualmente pueden ser específicas para una norma concreta o bien dar cobertura a un rango mayor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Soluciones de certificación de producto o servicio siguiendo estándares nacionales o europeos.
- Soluciones de evaluación de software con pruebas de caja blanca, gris o negra que verifique el grado de cumplimiento de seguridad del producto con respecto a estándares y buenas prácticas.

- Evaluación de pilas de protocolos, software incrustado crítico para la seguridad, técnicas de escaneo o fuzzing a nivel lógico o físico.
- Soluciones innovadoras de evaluación de integridad de archivos y librerías ejecutables de firmware o software que garanticen seguridad en la cadena de suministro.
- Soluciones que den respuesta a la certificación de producto Common Criteria siguiendo esta norma directamente, o posibles perfiles de protección existentes, con diferentes grados de cumplimiento.
- Soluciones integrales de gestión de riesgos de ciberseguridad que den respuesta a normativas para el seguimiento de determinados controles técnicos puedan apoyarse en mediciones continuas de sondas.
- Soluciones específicas para la evaluación y seguimiento del cumplimiento normativo en infraestructuras críticas.
- Creación de sondas y sensores que actúen a bajo nivel tecnológico para asegurar el cumplimiento de seguridad de activos críticos.
- Soluciones de aplicación de NLP (Natural Language Processing) para verificar la completitud, precisión, adecuación al marco normativo de documentación del tipo: políticas de privacidad, disclaimers legales, acuerdos de nivel de servicio, declaraciones de seguridad, especificaciones técnicas, procesos, etc.
- Soluciones específicas para la evaluación y seguimiento del cumplimiento normativo en sistemas de la industria 4.0 (confidencialidad e integridad de datos sensibles, comunicaciones entre dispositivos, etc.) entre otros: IIoT, impresión 3D, robótica colaborativa, realidad virtual/aumentada o gemelos digitales.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- Alto grado de cobertura y automatización en la evaluación y el cumplimento normativo.
- Soluciones integrales con paneles de control para un seguimiento visual sencillo
- Capacidad de configuración y personalización, escalabilidad en funcionalidad, interoperabilidad e integración con otras soluciones.
- Facilidad, simplicidad y transparencia en su uso
- Demostradores testados con la participación de varios usuarios finales
- Validación por agencias regulatorias y certificadoras.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Entornos operativos IT generalistas y/o Industriales específicos donde la solución muestre sus capacidades de asistencia automatiza de evaluación y cumplimiento.
- Prueba con tipología de datos y volumen de carga similares a los de un entorno real.
- Validación del usuario final respecto a la eficacia, y facilidad de uso de la herramienta.
- Listado de usuarios finales:
  - Al menos una organización ya sea PYME o del algún sector estratégico.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒

Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 05: GESTIÓN DE IDENTIDADES

MOTIVACIÓN

Una identidad digital es una representación digital de una persona física o jurídica. La información contenida en una identidad digital permite la autentificación de un usuario o la presentación de sus atributos digitales, dándole acceso a servicios públicos o privados. El objetivo general es permitir a los ciudadanos y a las empresas demostrar quiénes son o demostrar sus atributos/características, sin necesidad de documentos físicos.

Dado el aumento del ritmo de la digitalización de la economía y la sociedad, como demuestra la pandemia del covid-19, la identificación *online* y el intercambio de atributos es cada vez más importante a medida que aumenta el número de servicios personalizados y sensibles a la identidad.

Una persona promedio tiene más de 90 cuentas de usuario (identidades digitales) *online*. Tener muchas cuentas lleva a reutilizar las contraseñas, lo que aumenta el riesgo de robo de identidad y la filtración de datos personales. En 2019, más de 4.100 millones de registros de datos personales quedaron expuestos debido a fugas y filtraciones de datos. Las direcciones de correo electrónico se expusieron en el 70% y las contraseñas en el 65% de las fugas de datos notificadas. Una encuesta reciente de Eurostat refleja que el 75% de los ciudadanos de la UE utilizan herramientas de identidad de bajo nivel de seguridad proporcionadas por el sector privado (por ejemplo, la contraseña y el nombre de usuario o la dirección de correo electrónico) con riesgos potenciales para la integridad de los datos personales o incluso la suplantación de identidad. Según una encuesta de Gigya, más del 80% de los consumidores admiten haber renunciado a un formulario de registro online porque se sentían incómodos con la cantidad o el tipo de información solicitada. Una reciente encuesta del Eurobarómetro muestra que el 88% de los consumidores desea tener más control sobre sus datos.

La Brújula Digital de la Comisión Europea para 2030[16] contempla una serie de metas e hitos que la identidad digital europea ayudará a alcanzar. Así, de aquí a 2030, todos los servicios públicos clave deben estar disponibles online y todos los ciudadanos tendrán acceso por ejemplo, a datos altamente sensibles como historiales médicos electrónicos. Se prevé que el 80 % de los ciudadanos utilice una solución de identificación electrónica.

Cuando se gestiona la información de los ciudadanos, ésta puede ser proporcionada originalmente por diferentes emisores, como los certificados emitidos por organizaciones educativas, o registros médicos, en formatos electrónicos estandarizados utilizando infraestructuras de clave pública. El tiempo y el coste de emitir y mantener y verificar estos certificados son considerables. Además, infraestructuras de clave pública, requieren el uso de una autoridad de certificación como intermediario para emitir los certificados, creando una dependencia que puede ser comprometida (por ejemplo, escuchando y suplantando las interacciones entre usuarios y servicios – sniffing y spoofing en ataques man-in-the-middle –). Los actuales registros de verificación almacenados en bases de datos centralizadas también pueden ser destruidos en caso de catástrofes naturales o guerras.

En el nuevo paradigma, resultado de varios años de investigación de soluciones de tecnología distribuida para la identidad digital (DLT), se emitirá información digital firmada criptográficamente para que la tenga el ciudadano y, mediante el uso de la Blockchain pública, los datos se publicarán respetando la privacidad, lo que permitirá la verificación instantánea de las pruebas presentadas. Se prevé que las DLT del sector público europeo que cumplan con la legislación de la UE, apoyen las transacciones transfronterizas descentralizadas entre los Estados miembros, inicialmente para el sector público y gradualmente también para los servicios privados, facilitando así el desarrollo de servicios más seguros y racionalizados, la presentación de informes y las transacciones de datos entre los ciudadanos y las instituciones de la UE.

16 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

Así mismo se ve necesario facilitar al usuario la gestión de sus múltiples identidades digitales con poder de decisión sobre el acceso a su información en el uso de ellas, aunando y simplificando el número de identidades, así como disponiendo de carteras digitales que simplifique y automaticen esta gestión.

La Comisión Europea ha propuesto un marco[17] para una identidad digital europea que estará disponible para todos los ciudadanos y empresas residentes en la UE. Los ciudadanos podrán probar su identidad y compartir documentos electrónicos de sus carteras europeas de identidad digital con solo hacer clic en un botón de su teléfono. Podrán acceder a los servicios en línea con su identificación digital nacional, que será reconocida en toda Europa. Se requerirá que las plataformas de servicios digitales acepten el uso de billeteras europeas de identidad digital a pedido del usuario, por ejemplo, para demostrar su edad de una manera segura y transparente. De manera que el ciudadano decidirá cuánta información quiere compartir, con quién y con qué finalidad. Las empresas europeas, grandes y pequeñas, también se beneficiarán de esta identidad digital, para ofrecer una amplia gama de nuevos servicios ya que la propuesta ofrece una solución para servicios de identificación seguros y confiables. El marco europeo de identidad digital según el nuevo Reglamento[18] ofrecerá carteras/monederos digitales a ciudadanos y empresas que podrán vincular sus identidades digitales nacionales con pruebas de otros atributos personales (por ejemplo, permiso de conducir, diplomas, cuenta bancaria). Estos monederos pueden ser facilitados por autoridades públicas o por entidades privadas, siempre que estén reconocidas por un Estado miembro. Las nuevas carteras europeas de identidad digital permitirán a todos los europeos acceder a los servicios en línea sin tener que utilizar métodos de identificación privados o compartir datos personales innecesariamente. Con esta solución tendrán el control total de los datos que comparten.

OBJETO

Descripción del reto

GESTIÓN DE LA CONFIANZA DISTRIBUIDA Y SOLUCIONES DE IDENTIDAD DIGITAL

Problema a resolver

Muchos servicios en Internet dependen de la disponibilidad de identidades digitales seguras, que desempeñan un papel crucial para salvaguardar los datos y la privacidad de los ciudadanos, así como para protegerlos a ellos y a otros actores, como las empresas privadas o los servicios públicos, de diversas amenazas en línea. Al mismo tiempo, muchos países europeos ya tienen o están desarrollando un sistema de identidad electrónica (eID). La mayoría de estos proyectos están construidos con un nivel de seguridad muy alto, lo que los hace muy adecuados para diversos procesos de administración electrónica. Pero, a su vez, pueden carecer de utilidad/ usabilidad para las aplicaciones comerciales.

Los sistemas de gestión de la identidad digital basados en tecnologías distribuidas (DLT) desempeñarán un papel importante en el apoyo a la aplicación de derechos fundamentales como el derecho personal a una identidad centrada en el usuario de uso, con una fuerte visión de la autodeterminación y la autonomía personal de las personas físicas. Esto conducirá a formas más rápidas, baratas y más fáciles de realizar transacciones electrónicas entre los ciudadanos, empresas y gobiernos utilizando mecanismos de intercambio estandarizados de intercambio estandarizados, al tiempo que permitirá a los proveedores de la industria de la UE desarrollar más productos y servicios conformes con esas normas.

[17] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[18] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Con el fin de aprovechar plenamente los beneficios de un entorno normativo europeo establecido sobre la identidad, la confianza, la administración electrónica y la ciberseguridad (Reglamento eIDAS[19], Reglamento de la Pasarela Digital Única[20], Paquete de Ciberseguridad[21]) que apoya decisivamente el desarrollo de un mercado único digital y de algunos de sus instrumentos clave (es decir la Pasarela Digital Única y la Infraestructura Europea de Servicios de Blockchain). La prioridad está en desarrollar soluciones de gestión de la identidad innovadoras[22], seguras y que mejoren la privacidad, que sitúe a los usuarios en el centro de su administración, permitiéndoles controlar su propia información de identidad al tiempo que hacen realidad sus derechos consagrados en nuestro marco jurídico de protección de datos personales (RGPD). En un contexto de aumento de las amenazas cibernéticas, incluyendo diferentes formas de delitos relacionados con la identidad, se vuelve crítico empoderar a los usuarios con soluciones descentralizadas y eficientes para proteger quiénes son, revelando exactamente y sólo la información de identidad requerida en cada contexto de interacciones digitales bajo el control del usuario y con fuertes garantías en cuanto a la autenticidad, procedencia e integridad de dichos datos.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Desarrollar nuevos sistemas innovadores de gestión de identidades, federados, descentralizados o mixtos, para gestionar todo el ciclo de vida de las identidades digitales de personas, organizaciones, servicios, objetos y procesos, para proporcionar una capa semántica sólida y rica que permita favorecer procesos de negocio innovadores.
- Aplicar estas innovaciones en áreas o dominios específicos, poniendo el foco en el cumplimiento de la normativa (por ejemplo, tecnología financiera o sanidad), la universalidad del acceso (administración electrónica), los recursos informáticos limitados (p. ej., IoT) con proyectos piloto a gran escala.
- Apoyar la adopción de sistemas y procedimientos de identidad digital en áreas y escenarios específicos y desfavorecidos (p. ej. conectividad intermitente, personas mayores, desempleados), centrarse en la usabilidad y desarrollar compensaciones innovadoras entre seguridad y usabilidad.
- Apoyar los esfuerzos de normalización en los comités europeos e internacionales para lograr modelos de identidad digital interoperables, seguros e innovadores.
- Creación de soluciones de cartera digital que faciliten al usuario la gestión de sus múltiples identidades, y la exposición de datos personales en el uso de cada una de ellas.
- Las actividades pueden aprovechar las plataformas europeas existentes de identificación y autenticación electrónicas con interfaces claramente definidas basadas en reglamentos europeos.

Funcionalidades

[19] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[20] https://single-market-economy.ec.europa.eu/single-market/single-digital-gateway_en

[21] https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-cyber-security-package

[22] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

Se describen a continuación algunas funcionalidades de ejemplo.

- Soluciones distribuidas, dinámicas y automatizadas de gestión de la identidad digital.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba sobre servicios de Internet reales con usuarios reales.
- El **volumen y tipología de datos** han de ser similares a los de un entorno.
- La **duración** de la prueba se concepto ha de ser suficiente para abarcar las tipologías de operaciones habituales.
- Listado de usuarios finales:
  - Propietarios de los servicios en Internet que utilicen identidades digitales, puede ser cualquier tipo de organización tanto pública como privada.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 06: CIBERRESILIENCIA DE CADENA DE SUMINISTRO

MOTIVACIÓN

El *software* está presente en todos los sistemas. En su desarrollo y creación se reutilizan componentes *software* de terceros que no están exentos de vulnerabilidades por lo que están sujetos a continuas actualizaciones y parches. En las actualizaciones de seguridad de cualquier *software* comercial está involucrada toda la **cadena de suministro del *software*** que abarca desde las empresas que los comercializan hasta los desarrolladores de los componentes que lo forman. Se estima que entre el 85 y el 97% del código utilizado por la industria del *software* es reutilizado, entre otros *frameworks*, repositorios de API o librerías y *software open source*.

La cadena de suministro del *software* ha sido uno de los principales vectores de ataque de importantes incidentes recientes como el de la plataforma Solarwinds de Orion[23], Kaseya[24], Log4j[25] o Asus SadowHammer[26] y otros[27] caracterizados por su gran impacto al afectar a empresas y organismos de todo el mundo, con sospechas de implicaciones geopolíticas. Los atacantes, muchas veces conocidos grupos y actores de APT (*Advanced Persitent Threats*), consiguen acceder al código fuente de un componente *software* muy utilizado por un producto comercial, lo modifican para incluir puertas traseras o cualquier tipo de *malware* y se distribuye, por ejemplo, formando parte de una actualización legítima. Los ciberdelincuentes consiguen así perpetrar el espionaje, el robo de datos o propiedad intelectual y todo tipo de extorsiones.

Los ataques a la cadena de suministro *software* son una de las nueve mayores amenazas según ENISA[28]. La naturaleza global de las cadenas de suministro amplía la superficie de ataque e incrementa el potencial impacto de los mismos, en particular con los despliegues de servicios sobre *cloud*, 5G y con IoT, pudiendo afectar a usuarios finales, empresas y administración pública. La industria de la tecnología y los responsables de la ciberseguridad se ven ante un problema que precisa de un enfoque innovador pues mina la confianza en el ecosistema del desarrollo de *software*.

Igualmente, aunque con una dificultad añadida pues requiere acceso físico al dispositivo, los chips, *firmware*, tarjetas, interfaces y otro *hardware* que forma los sistemas TI podrían haber sido comprometidos intencionalmente durante su diseño, fabricación, distribución o mantenimiento de los sistemas finales, conteniendo vulnerabilidades que pueden llevar a exfiltrar o corromper datos que manejan o bien afectar a su funcionamiento.

OBJETO

Descripción del reto

CIBERRESILIENCIA DE LA CADENA DE SUMINISTRO SOFTWARE / HARDWARE.

Problema a resolver

Si bien existen iniciativas para atajar los problemas de seguridad inherentes a la cadena de suministro *software* desde el diseño del mismo, como Google SLSA y MITRE D3fend[29], es necesario

[23] https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/campana-explotacion-activa-solarwinds-orion-platform

[24] https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/ciberataque-cadena-suministro-el-*software*-vsa-kaseya

[25] https://www.incibe-cert.es/blog/log4shell-analisis-vulnerabilidades-log4j

[26] https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/herramienta-asus-infectada-operacion-shadowhammer

[27] *ENISA threats landscape for Supply Chain Attacks* https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[28] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

[29] https://d3fend.mitre.org/

innovar en las medidas proactivas y reactivas para incrementar la ciberresiliencia ante posibles incidentes que afecten al *software* (y al *hardware*) que actualmente está operativo en las empresas. Tanto los compradores como los integradores/proveedores de productos *software* y *hardware* necesitan de soluciones innovadoras[30] para extender sus requisitos, políticas y controles de seguridad a los proveedores en su cadena de suministro y en particular a los proveedores de servicios que incorporen IoT, 5G, *cloud* o servicios gestionados.

La seguridad en la cadena de suministro es un problema complejo con muchas interdependencias y efectos en cascada que requiere un enfoque multidisciplinar que incluya entre otros aspectos el modelado de las amenazas, la trazabilidad, la identificación de puntos de penetración y propagación, los indicadores de compromiso y la ciberresiliencia.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Desarrollar sistemas innovadores de seguridad en la cadena de suministro colaborativos y globales, para gestionar todo el ciclo de vida del *software* y *hardware* detectando posibles ataques en todas sus fases (diseño, construcción y distribución) para que puedan aplicarse a productos ya comercializados para garantizar su integridad y fiabilidad.
- Aplicar estas innovaciones en áreas o dominios específicos, poniendo el foco en el cumplimiento de la normativa (por ejemplo, industria 4.0, IoT, *cloud* o 5G) con proyectos que puedan aplicarse a gran escala.
- Creación de soluciones que faciliten al usuario final la gestión de la cadena de suministro incluyendo el control, verificación y cumplimiento según el riesgo asociado.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Identificación de cadenas de suministro y de su fiabilidad**. Aplicaciones de *blockchain* y otras tecnologías DLT (*Distributed Ledger Technologies*) para aportar trazabilidad, integridad, inmutabilidad y transparencia a la cadena de suministro *software* o *hardware* para identificar, monitorizar y auditar los componentes de forma que también pueda ser usado como garantía de cumplimiento.
- Monitorización continua y en tiempo real (SIEM, SOAR)
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia. Aplicaciones de IA/ML para el modelado de amenazas en la cadena de suministro.
- **Enriquecimiento**: posibilidad de enriquecer la información recogida con otras fuentes externas.

[30] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

- Gestión de incidentes:
  - Sistemas de identificación y detección temprana de indicadores de compromiso de la cadena de suministro.
  - Desarrollo de métodos específicos de ciberresiliencia aplicados a la cadena de suministro.
- **Métricas:** ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia del sistema.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio e interoperabilidad:** posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Escalabilidad:** se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado de la solución.
- **Simplificación:** se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución de la misma.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba con las siguientes características:

- El sistema debe estar desplegado en un entorno operativo donde se pueda realizar una demostración:
  - Detectando ataques a la cadena de suministro en un entorno nacional.
  - La funcionalidad acordada para el sistema tiene que estar completada y totalmente operativa.
  - La solución debe evidenciar también su **carácter innovador**.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 07: SISTEMAS INNOVADORES PARA EL ANÁLISIS DE SEGURIDAD DE DISPOSITIVOS IOT

MOTIVACIÓN

El IoT ha experimentado una enorme expansión en los últimos años. Esto ha generado una proliferación de soluciones por nuevos fabricantes y los ya convencionales por lo que cada vez hay mayor número de dispositivos integrados en diferentes sistemas y verticales, que van desde la electrónica de consumo para el hogar, ciudades inteligentes (movilidad, contaminación, residuos, sostenibilidad), coches conectados o autónomos, aviones, agricultura inteligente, así como el despliegue en plantas industriales (siguiendo el paradigma de Industria 4.0.) tan presentes en infraestructuras críticas.

Con respecto a su grado de seguridad y privacidad, el experto de Gartner Earl Perkins indica: "Los principales proveedores están haciendo esfuerzos para abordar las cuestiones de seguridad, pero la mayoría aún no está en esa fase. Están dando prioridad a la comodidad, la facilidad de uso y el tiempo de comercialización, por encima de cualquier otra consideración de seguridad".

Para 2025 se espera el despliegue de más de 41.000 millones de dispositivos IoT (*International Data Corporation*), lo que supondrá un crecimiento exponencial de los datos y el desplazamiento de las operaciones de procesamiento y el análisis de datos en las infraestructuras TIC de un modelo actual centralizado, a un escenario distribuido (*fog* y *edge computing*).

Estos dispositivos IoT se caracterizan por:

- Estar conectados a las redes de comunicación, lo cual maximiza su integración pero expone el dispositivo a ataques locales y remotos,
- Disponer de sondas que permiten recabar un amplio espectro de datos heterogéneos de propiedades del entorno
- Con frecuencia no contar con medidas de seguridad por diseño, ni configuraciones seguras por defecto (out-of-the-box), así como dificultades para ser actualizados (firmware, y *software*) por el fabricante de forma temporada y remota.
- Bajo coste lo que obliga a disponer de limitaciones *hardware* principalmente en batería, procesador y memoria que impiden aplicar medidas de seguridad, como por ejemplo contramedidas criptográficas siguiendo algoritmos tradicionales, lo que ha motivado versiones ligeras para este tipo de dispositivos
- Ciclo de vida corto previsto por el fabricante, lo que no incluye un plan de mantenimiento que incluya factores de actualización de seguridad.

En el marco europeo, se destacan diferentes normativas, recomendaciones y publicaciones que engloban a la seguridad de dispositivos IoT:

- Directiva 2014/53/UE donde los estados miembros ponen de manifiesto la necesidad de armonizar la legislación y la convergencia del sector de las telecomunicaciones, audiovisuales, y de las tecnologías de la información.
- Reglamento general de la protección de datos (RGPD)[31] donde se regula de manera concreta la manipulación y el tratado de los datos privados y personales. El RGPD afecta tanto a las empresas que forman parte del ecosistema de IoT como a los usuarios finales.

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- La Directiva de seguridad en redes y sistemas (NIS)[32] (y su actualización NIS2[33] que será publicada en inminentes próximas fechas) donde se establece un marco común de cómo abordar la ciberseguridad en toda la UE, así como la cibercriminalidad. Se indican pautas para actuar coordinadamente en todos los estados miembros.
- El *Cybersecurity Act* (CSA)[34] que promueve un marco de certificación de la ciberseguridad y el establecimiento de esquemas voluntarios de certificación de la ciberseguridad para los productos, servicios y procesos TIC con tres niveles de garantía (básico, sustancial y alto). El *Union Rolling Work Program* (URWP), actualmente en fase de definición, establece los ámbitos de los futuros esquemas y su priorización de un esquema IoT.
- El Reglamento sobre la identificación electrónica y los servicios de confianza (eIDAS)[35] no parece tener consecuencias directas en el ecosistema de la IoT, ya que afecta principalmente a las personas físicas y jurídicas, pero podría tener un impacto potencial, por ejemplo, vinculando potencialmente los dispositivos con las personas jurídicas.
- La Decisión del Nuevo Marco Legislativo (NLF) nº 768/2008/CE define los requisitos de seguridad que debe cumplir un producto para entrar en el mercado de la UE.
- La Directiva sobre Equipos Radioeléctricos 2014/53/UE (RED) establece un marco normativo para la comercialización de equipos radioeléctricos. Los protocolos de radio son utilizados por los dispositivos IoT para transportar datos cuando no existe una conexión física o por cable, por lo que la RED abarcará esencialmente todos los dispositivos de IoT que transmitan datos.
- Publicación de ENISA "*Baseline Security Recommendations for IoT*"[36] (Noviembre 2017) sobre la necesidad de concienciar sobre las amenazas de ciberseguridad del IoT en infraestructuras críticas y aporta recomendaciones para hacer frente a las ciberamenazas.

OBJETO

Descripción del reto

DESARROLLO DE SISTEMAS INNOVADORES PARA EL ANÁLISIS DE SEGURIDAD DE DISPOSITIVOS IOT

Problema a resolver

Urge la necesidad de estandarizar los dispositivos y las redes IoT, colaborar en un plan general de buenas prácticas de control, implementación y mantenimiento. Esto debe venir no solo a nivel gubernamental y legislativo sino de del compromiso de las empresas tecnológicas de mayor alcance y por supuesto la implicación de los fabricantes.

[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[33] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. COM(2020) 829 final.

[34] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[35] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[36] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

En cuanto las amenazas de dispositivos IoT[37], realmente casi cualquier ataque es susceptible de actuar en este campo:

- Contraseñas débiles: Uso de contraseñas predecibles, cortas o incluso están dentro del mismo código.
- Servicios de red inseguros: Comunicaciones (servicios como telnet, ftp, etc.) entre dispositivos permanecen inseguros, expuestos y desfasados.
- Ecosistemas IoT inseguros: Interfaces web, API, móviles y otros pueden ser comprometidos a través de la red
- Mecanismos de actualizaciones inseguros: Carencias de mecanismos de control de firmwares y en su envió sin cifrar, así como de mecanismos de *downgrades* controlados.
- Componentes desfasados: Librerías obsoletas y *software* de terceros desfasado. También componentes de *hardware* desfasados.
- Deficiencias en la protección de la privacidad: Se detecta información personal guardada en los propios dispositivos inseguros, que ponen en riesgo la privacidad.
- Transferencia y guardado de datos insegura: Sin cifrar la información suele fluir por la red de manera insegura hasta llegar a su destino.
- Gestión descontrolada: Controles de gestión de la seguridad y falta de planes de monitoreo y planes de contingencia y respuesta.
- Configuraciones por defecto inseguras: Algunos dispositivos se dejan con configuraciones por defecto o no permiten su incremento de la seguridad de ningún modo.
- Protección física deficiente: El acceso físico a los dispositivos no está controlado, pudiendo ser manipulado.

En este reto se buscan soluciones innovadoras[38] que analicen los problemas de seguridad que presentan los dispositivos IoT en todos sus niveles (*full stack*) y en su integración en sistemas específicos a través del desarrollo de herramientas para automatizar el cumplimiento y la comprobación de la evaluación durante su ciclo de vida.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Herramientas para la comprobación automatizada del cumplimiento, la identificación de amenazas, la evaluación del sistema y la compatibilidad de la certificación (estática) / La mayoría de las herramientas actuales se centran en el análisis dinámico del *software*.
- Herramientas para procesar y verificar las pruebas de corrección solicitadas especialmente para sistemas críticos o esenciales.

---

[37] Ciberseguridad del IoT: Un Análisis en Países de la Unión Europea: https://www.researchgate.net/publication/348692397_Ciberseguridad_del_IoT_Un_Analisis_en_Paises_de_la_Union_Europea

[38] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

- Herramientas basadas en IA para la evaluación continua de la seguridad de las funcionalidades, impacto de las actualizaciones, evaluación en tiempo real, aplicación de parches y reevaluación de la seguridad; identificación automática de vulnerabilidades y parches (dinámicos) / cooperación con iniciativas de IA.
- Utilización de herramientas automatizadas para la evaluación y las pruebas de seguridad con arreglo a una metodología basada en normas (por ejemplo, basada en ETSI EG 203 251 V1.1.1) y herramientas para el análisis de los informes de certificación de seguridad (CC EAL, FIPS140-2).
- Aplicación de *Digital Twins* para probar las funcionalidades y parches de seguridad de los dispositivos.
- Herramientas innovadoras, abiertas y laboratorios de certificación de pruebas para facilitar el acceso de las pymes a la precertificación de productos.
- Soluciones innovadoras para el desarrollo de las habilidades de los hackers éticos y los profesionales y de las habilidades de *bug bounty*.
- Identificar el estado de cumplimiento para las pruebas de penetración ocasionales /auditoría técnica y para la auditoría de seguridad continua *bug bounty*.
- Innovación y desarrollo de analizadores de firmware de los dispositivos.
- Análisis de seguridad en dispositivos asociados al uso de 5G.
- El blockchain se plantea como una solución efectiva para mantener la seguridad de los numerosos dispositivos. Por ejemplo, en un entorno IoT se podrían distribuir versiones de firmwares de forma segura a través de esta tecnología.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- Mejor adopción del proceso de certificación en la industria de la UE para aumentar la confianza de los usuarios en sus productos.
- Gestión de la cadena de suministro, pruebas de ciberseguridad de los productos, servicios y sistemas de certificación.
- Proporcionar mecanismos a las organizaciones, especialmente a las pymes para evaluar internamente los productos.
- Elevar el nivel de la seguridad estimulando competencia y mejores servicios al mercado.
- Armonizar los sistemas de certificación europeos, evitando duplicaciones y facilitando la comparabilidad de los resultados. Posibilidad de comparar diferentes sistemas o dispositivos certificados bajo diferentes esquemas.
- Aumentar la seguridad de los productos, servicios y sistemas mediante determinando un nivel de seguridad mínimo requerido a través del proceso de certificación.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba con dispositivos reales en un **entorno IoT real**.
- El **volumen y tipología de datos** han de ser similares a los de un entorno real.
- La **duración** de la prueba de concepto será suficiente para abarcar las tipologías de operaciones habituales.
- Listado de usuarios finales:
    - Proveedores y usuarios de dispositivos IoT.

- La **actuación o las** actuaciones en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 08: SISTEMAS PARA LA PROTECCIÓN FRENTE A ATAQUES CONTRA EL ESPECTRO ELECTROMAGNÉTICO

MOTIVACIÓN

Los principales organismos de ciberseguridad americanos (CISA, DHS) y de la UE, así como Informes de expertos, alertan que incidentes en el Espectro Electromagnético (EEM) pueden provocar daños en los sistemas tecnológicos que soportan nuestra sociedad. El EEM puede ser usado también como medio a través del cual realizar ataques.

Por tanto, parece clara la necesidad de desarrollar e implantar mecanismos que nos permitan defendernos y recuperarnos ante incidentes dañinos, provocados o naturales, que se puedan producir en el EEM.

OBJETO

Descripción del reto

SISTEMAS PARA LA PROTECCIÓN FRENTE A ATAQUES CONTRA EL ESPRECTO ELECTROMAGNÉTICO.

Problema a resolver

Este reto permitirá el desarrollo de tecnologías o soluciones innovadoras que permitan la protección, detección, respuesta y resiliencia ante eventos e incidentes en el EEM.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Detección y localización de amenazas en el espacio electromagnético: diseño y desarrollo de prototipos innovadores que permitan de forma autónoma la detección y localización de elementos de origen que puedan generar incidentes en el EMM
- Detección de anomalías en las comunicaciones inalámbricas: diseño y desarrollo de prototipos capaces de detectar anomalías en canales de comunicaciones inalámbricos
- Securizacion de comunicaciones satelitales: diseño y desarrollo de prototipos innovadores que permitan la integridad, disponibilidad y confidencialidad de las comunicaciones entre estaciones y satélites.
- Resiliencia de activos críticos frente a incidentes de pulso electromagnético: diseño y desarrollo de prototipos que permitan la protección de activos críticos vinculados con flujos de trabajo esenciales para las organizaciones que puedan ser objetivo de ataques con pulso electromagnético (PEM) o que puedan verse afectados por eventos geomagnéticos (GEM)

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Protección de activos**: capacidad para la protección de dispositivos considerados críticos en las diversas organizaciones y que su fallo pueda ocasionar problemas de seguridad hacia las personas o bienes físicos existentes.
- **Monitorización espectro electromagnético**: proporcionar capacidades de monitorización que permitan la detección de eventos anómalos en sistemas de comunicación inalámbricos, al menos que cubran protocolos alguno de los protocolos del espectro radioeléctrico. Como

por ejemplo: Bluetooth, Zigbee, HomeRG, HyperLan, UMTS, GPRS, 5G, TDMA, FDMA, además posibilidad de monitorizar eventos PEM y GEM, entre otros.

- **Detección anomalías**: Capacidad de detección de eventos anómalos o incidentes y capacidad de geolocalización su fuente origen.
- **Securización**: Capacidad de securización ante eventos en el EEM para protocolos de comunicación existentes.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba con las siguientes características:
  - Despliegue en entorno controlado, necesariamente en entorno de usuario final, que permita la comprobación de resultados satisfactorios en al menos un usuario final.
  - La solución debe evidenciar su **carácter innovador**.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales de la solución, que le permitirán acceder a una cuota del mercado.
- Listado de usuarios finales:
  - Se validará la solución en al menos un organismo usuario final, en un entorno representativo.
- La **actuación o las actuaciones** en las que se podría ubicar el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 09: SOLUCIONES INNOVADORAS EN CIBERSEGURIDAD PARA REDES 5G

MOTIVACIÓN

El pasado 3 de junio de 2022, el Gobierno ha lanzado una consulta pública sobre el nuevo Esquema Nacional de Seguridad de Redes y Servicios 5G. En el propio comunicado destaca que el impulso al **despliegue de la tecnología 5G y la ciberseguridad**, junto con la conectividad, son clave en el proceso de transformación digital en España, uno de los cuatro ejes fundamentales del Plan de Recuperación Soluciones innovadoras para tecnologías 5G.

El Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación menciona que para crear y reforzar la industria de 5G en España, **se impulsará la investigación, desarrollo e innovación en torno a la tecnología 5G, también en lo que a la ciberseguridad 5G se refiere**.

Mencionar que existe una estrecha vinculación entre dispositivos IoT y 5G, y es de sobra conocido que los primeros en ocasiones se desarrollan o fabrican con carencias en ciberseguridad. Dotar de soluciones innovadoras que permitan asegurar al menos todo aquello relativo a la conectividad es todo un reto para garantizar la confluencia entre ambas tecnologías. Además, **el 5G amplía notablemente las capacidades en las comunicaciones lo que podría magnificar los ataques actuales** como DDoS, botnets, etc. Por lo que proveer de mayores necesidades en ciberseguridad es una verdadera necesidad.

Y en general, todas las aplicaciones y casos de uso que se desarrollen usando las nuevas ventajas que aportan las redes 5G, podrán encontrarse con problemas de ciberseguridad que exploten las nuevas características del 5G; y estos problemas podrían ser previstos y abordados, lo que podría abre una ventana de oportunidad a la innovación.

OBJETO

Descripción del reto

SOLUCIONES INNOVADORAS PARA GARANTIZAR LA CIBERSEGURIDAD EN REDES 5G.

Problema a resolver

ENISA, en su informe THREAT LANDSCAPE FOR 5G NETWORKS[39], considera el despliegue del 5G, como **una de las mayores innovaciones de nuestro tiempo**. Por otro lado, el Real Decreto-ley 7/2022, de 29 de marzo identifica como problema a resolver el importante incremento del riesgo de ciberataques contra redes 5G desplegadas o previstas para despliegue en nuestro país, instando a establecer requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G).

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Soluciones innovadoras[40] de ciberseguridad para redes 5G o servicios basados en la tecnología 5G.

[39] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[40] vinculados con algún elemento o conjunto integrado de elementos o infraestructuras de red, ya sean *hardware* o *software*, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, incluidos los recursos asociados e

- Soluciones innovadoras de ciberseguridad que ayuden a la identificación de vulnerabilidades en redes 5G o servicios basados en la tecnología 5G.
- Soluciones innovadoras de ciberseguridad que ayuden a la detección de ciberamenazas en redes 5G o servicios basados en la tecnología 5G.
- Soluciones innovadoras de ciberseguridad destinadas a garantizar la protección de los usuarios corporativos de las redes 5G.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- La solución ha de estar diseñada para las **superficies de amenazas** 5G.
- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de esta actividad comercial, sector y/o subsector de aplicación (activos IT/OT, IoT, IIOT, etc.).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba con las siguientes características:

- Entorno operativo donde se espera recibir la demostración, deberá incluir algún elemento, infraestructura o recurso de una red pública 5G:
  - Los relativos a las funciones del núcleo de la red.
  - Las funciones de transporte y transmisión.
  - La red de acceso.
  - Los sistemas de control y gestión y los servicios de apoyo.
  - Las funciones de computación en el borde, virtualización de red y gestión de sus componentes.
  - Los relativos a intercambios de tráfico con redes externas e Internet.
  - Otros componentes y funciones de ciberseguridad innovadores que permitan elevar la resiliencia en redes y servicios 5G.

infraestructuras digitales, que permitan el transporte de señales con los que proporcionar conectividad móvil e inalámbrica y, a través de ella, prestar servicios de comunicaciones electrónicas e inalámbricas a usuarios y empresas con características avanzadas, que incorporen las funciones y capacidades y respondan a los casos de utilización recogidos en la Recomendación UIT-R M.2083, de la Unión Internacional de Telecomunicaciones, o en el estándar técnico de la organización 3GPP

- El volumen da carga o tipología de datos a probar será el adecuado para poder validar correctamente la prueba en un entorno operativo.
- La duración mínima que se espera que la prueba de concepto esté funcionando será de al menos 3 meses.
- Deberá de haber al menos un usuario final de entre los siguientes posibles candidatos:
  - Los operadores 5G.
  - Los suministradores 5G.
  - Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en auto prestación.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 10: CIBERSEGURIDAD EN EL VEHÍCULO CONECTADO

MOTIVACIÓN

La RAE define vehículo como «Medio de transporte de personas o cosas». Esto incluye a vehículos que se desplazan por tierra, mar o aire, tripulados o no. Y la ciberseguridad de estos vehículos es la meta de este reto.

Actualmente se desarrollan y comercializan vehículos inteligentes con capacidades crecientes de conectividad y automatización, incluyendo los de conducción autónoma. El aumento de conectividad incrementa el riesgo de ciberataques y el creciente nivel de automatización aumenta las oportunidades de que tengan éxito. Por ello, la ciberseguridad es uno de los retos más importantes para estos sistemas.

Para la Unión Europea la ciberseguridad en el ecosistema de movilidad conectada y automatizada es uno de los elementos de su agenda con iniciativas regulatorias y de desarrollo de estándares. Así, se aprobó el reglamento UNECE UNECE/TRANS/WP.29/2020/ el 23 de junio de 2020, que hace que sea obligatorio a partir del 1 de julio de 2022 en todo el territorio que los vehículos homologados —coches, autobuses, camiones, furgonetas y remolques— dispongan de un certificado de ciberseguridad y para los vehículos nuevos a partir del 1 de julio del 2024. Paralelamente la ISO está desarrollando la norma ISO/SAE 21434 que especifica los requisitos para gestionar los riesgos de ciberseguridad de estos vehículos durante todo su ciclo de vida. Además, se han establecido corredores en la UE[41], dos de ellos en la península ibérica, que han de servir para probar vehículos autónomos.

Por otra parte, ENISA[42] ha publicado recomendaciones en la aplicación de medidas de ciberseguridad al coche conectado, para IoT e infraestructuras inteligentes asociadas, para el sector y para los *stakeholders,* identificando los activos a proteger y medidas para conseguir esta protección.

No menos importante es el impacto que tiene en la privacidad de los individuos, conductor, propietario o pasajeros, el uso de los dispositivos electrónicos como GPS, videocámaras o sistemas eCall (llamadas de emergencia), entre otros, que tratan datos de carácter personal en los vehículos conectados, tanto en su interior como si se intercambian con dispositivos personales o se transmiten a entidades externas como fabricantes de vehículos, compañías de seguros, reparadores o administradores de infraestructuras. Así, el Comité Europeo de Protección de datos ha publicado una directiva[43] dirigida a todo el ecosistema.

Se estima que pasarán varios años hasta que la ciberseguridad de todos los modelos de vehículos conectados en circulación haya sido homologada y siga un proceso cíclico de verificación. Actualmente las empresas del sector de automoción y sus cadenas de suministro deben incorporar la ciberseguridad en sus procesos, para que sus productos y servicios dispongan de un alto nivel de ciberseguridad. También en este periodo se va a producir el despliegue de redes y servicios 5G y la próxima entrada en vigor de la directiva NIS2[44], que afectará a sectores críticos íntimamente relacionados con los vehículos conectados.

OBJETO

[41] European Commission 5G cross-border corridors https://digital-strategy.ec.europa.eu/en/policies/cross-border-corridors

[42] How to Secure the Connected & Automated Mobility (CAM) Ecosystem https://www.enisa.europa.eu/news/enisa-news/how-to-secure-the-connected-automated-mobility-cam-ecosystem

[43] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en

[44] The NIS2 Directive: A high common level of cybersecurity in the EU https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2021)689333

Descripción del reto

CIBERSEGURIDAD EN EL VEHÍCULO CONECTADO.

Problema a resolver

Durante un tiempo van a circular vehículos conectados que no han sido homologados según las nuevas normativas y que serán más vulnerables que los modelos que si estén homologados. En este escenario este parque de vehículos constituye un foco de riesgo que puede ser explotado por los cibercriminales o producir por desconocimiento o accidentalmente incidentes con alto impacto, por lo que se hace necesario innovar en productos y servicios para garantizar la seguridad de las distintas partes de este ecosistema. Es por ello importante dotar a los propietarios y usuarios, a los encargados del mantenimiento de estos vehículos y a los proveedores de *software* o *hardware* y de servicios, de herramientas para mitigar al menos las vulnerabilidades o amenazas consideraras en los vehículos homologados, tanto para los sistemas instalados como en la posible incorporación de nuevos sistemas y aplicaciones de terceros.

Se puede decir que las vulnerabilidades[45] de los vehículos interconectados se caracterizan por ser altamente explotables y de gran impacto, pues ponen en peligro la seguridad de otros vehículos y de sus usuarios, incluida su privacidad.

Las amenazas y vulnerabilidades consideradas en los vehículos homologados se agrupan en estas categorías:

- Relativas a los servidores *backend* en relación con vehículos sobre el terreno;
- De los canales de comunicación internos del vehículo;
- De los procedimientos de actualización;
- Relativas a acciones humanas involuntarias que facilitan un ciberataque;
- Relativas a la conectividad y conexiones externas;
- Relativas a los datos (brechas de datos, fugas de datos, privacidad) o al *software* de los vehículos;
- Potenciales vulnerabilidades que podrían ser explotadas si no están suficientemente protegidas o reforzadas.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

Los sistemas TI que componen los vehículos conectados y que son susceptibles de ser vulnerables son:

- los sistemas del interior del vehículo formados, entre otros, por las unidades de control electrónico o ECU, las unidades de control de dominio o DCU (los algoritmos de toma de decisión, la funcionalidad de conducción y circulación, la gestión del *software*) y los sensores y actuadores, los sistemas de info entretenimiento (incorporando redes wifi y Bluetooth, y dispositivos móviles) y el bus de comunicación interno (CAN, linbus o similar),
- Las comunicaciones, protocolos y redes del vehículo con otros vehículos, con la infraestructura o con la red (V2X) vía sistemas 4G LTE , 5G y GPS, entre otros,

[45] NIST National Vulnerability Database https://nvd.nist.gov/vuln/search/results?isCpeNameSearch=false&query=vehicles

- Los propios sistemas *backend* que analizan y tratan los datos recopilados de los vehículos, tanto del fabricante o del concesionario (servidores, sistemas y servicios *cloud*), las funcionalidades para el aislamiento de dominios y redes (como IDS/IPS o *firewalls*) y las infraestructuras de terceras partes (por ejemplo, para carga eléctrica o de combustible, parking, seguros).

Para todos estos sistemas es necesario adoptar medidas innovadoras:

- preventivas, como el diseño seguro de su arquitectura TI, la implementación de los requisitos de seguridad de los protocolos utilizados y de configuración del *software* y *hardware* que lo integran, proveer de mecanismos de actualizaciones de *software* seguras y que no afecten a la seguridad física del vehículo;
- Organizativas como el establecimiento de sistemas de gestión de ciberseguridad que permitirá la homologación o la gestión de riesgos de la cadena de suministro;
- Reactivas para la detección y reacción adecuadas para una rápida respuesta y recuperación en caso de incidente.

Funcionalidades

Incluimos un listado no exhaustivo de posibles funcionalidades u objetivos.

- Garantizar la seguridad y trazabilidad de los datos y el cumplimento legal en la prestación de servicios o uso de apps que requieran la recogida de datos personales o hábitos de uso, priorizando la utilización de medios de comunicación seguros y específicamente dedicados al sector, por ejemplo:
  - Seguros con primas según los hábitos («*Pay As You Drive*» o «*Pay How You Drive*»);
  - Arrendamiento y reserva de plazas de estacionamiento;
  - Llamada de emergencia en caso de accidente: ecall;
  - Participación en estudios de accidentología;
  - Localización de vehículo robado.
- Sistemas de inteligencia específicos para recoger, clasificar y analizar amenazas de manera que sean efectivos para conjuntos de vehículos (flotas, modelos o fabricantes), con la creación de plataformas de supervisión detección y respuesta cooperativas (centros de operación de seguridad, SOC) que puedan extenderse en el ámbito europeo.
- Soluciones para aplicar medidas técnicas que permitan a los fabricantes de vehículos o a los encargados de su mantenimiento analizar y solventar vulnerabilidades y actualizar los sistemas «*over the air*, (OTA.)» sin comprometer la seguridad física y durante toda la vida útil del vehículo.
- Soluciones de defensa activa multinivel (*cloud*, aplicación, red y terminal) con análisis de datos mediante técnicas que usen Big Data y técnicas IA, que incorporen datos de todo tipo de sistemas específicos del ecosistema, por ejemplo: IDS/IPS, *firewalls*, sistemas de autenticación o cifrado.
- Soluciones inalámbricas seguras que incorporen mecanismos de cifrado y autenticación específicos (eHSM o *Hardware Security Modules* embebidos o TPS *Trusted Platform Modules*) para proteger las comunicaciones en el interior de los vehículos.
- Soluciones para llevar a cabo la separación efectiva de las funciones vitales del vehículo de las que dependen sólo de las capacidades de telecomunicación (por ejemplo info entretenimiento).

- Alarmas en caso de detección de ataques a los sistemas del vehículo, con la posibilidad de trabajar en un modo que asegure las funciones esenciales (por ejemplo el frenado), desactivando funciones no esenciales (el geo guiado).
- Registro y análisis de accesos al sistema de información del vehículo, para analizar el origen de posibles ataques y realizar periódicamente una revisión en busca de posibles anomalías.
- Test de ciberseguridad para infraestructuras de carga eléctrica.
- Protección de la autenticidad e integridad de los sensores embebidos (cámaras, sonar, radares, laser, LiDAR) y de los componentes de la infraestructura (puntos de acceso, RSE o *Road Side Equipment*) para conducción autónoma.
- Soluciones para asegurar los vehículos conectados desde el diseño para mitigar riesgos en toda la cadena de suministro y asegurar el cumplimento de la normativa.
- Gestión de los riesgos de ciberseguridad.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- El **entorno operativo** donde se espera recibir la demostración debe **evidenciar la utilidad y carácter innovador** de la solución demostrada.
- Se valorarán pruebas en un entorno real con un número suficientemente representativo de vehículos.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores del producto o solución.
  - **Cuáles son las características específicas y diferenciales** sobre las cuales va a construir su solución especializada, indicando sobre qué y cómo se implementan las mejoras en ciberseguridad.
  - Cómo se escalaría la solución.
  - Listado de posibles usuarios finales o empresas destinatarias de la solución.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☐
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☐
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 11: CIBERDIAGNÓSTICO AUTOMATIZADO PARA PYMES Y AUTÓNOMOS

MOTIVACIÓN

La **Estrategia Nacional de Ciberseguridad**, dentro de su «Objetivo IV: Cultura y compromiso con la Ciberseguridad y potenciación de las capacidades humanas y tecnológicas», desarrolla a través de una serie de medidas incluidas en la «Línea de Acción 7: Desarrollar una cultura de Ciberseguridad», centrada en contribuir a la consolidación de la confianza digital para ciudadanos y empresas.

Adicionalmente, el Plan de digitalización de pymes 2021-2025 reconoce que «la digitalización de las pymes adquiere una especial urgencia ante las circunstancias derivadas de la pandemia COVID-19». Las pymes españolas deberán adaptar sus modelos de negocio y sus procesos para poder sobrevivir.

Es urgente que las pymes aborden la digitalización y, por ende, todas las medidas necesarias respecto a la ciberseguridad. Uno de los primeros pasos es facilitar a los usuarios finales que puedan llevar a cabo en cualquier momento un diagnóstico de los problemas de seguridad de sus activos.

OBJETO

Descripción del reto

CIBERDIAGÓSTICO AUTOMATIZADO PARA PYMES Y AUTÓNOMOS.

Problema a resolver

Se necesita resolver las carencias específicas e individualizadas de las pymes y autónomos en términos de ciberseguridad, para ello se busca con este reto la creación de tecnologías avanzadas que permitan a estas empresas o aquellas que les dan servicios de ciberseguridad, mediante mecanismos desatendidos e innovadores, el conocimiento de estado de la ciberseguridad para, así, poder aplicar las medidas necesarias, en posteriores fases.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Sistemas desatendidos de diagnosis: sistemas autónomos que sean capaces, tecnológicamente, de mapear activos, servicios, redes y sean capaces de transmitir dicha información para ser estudiada.
- Tecnologías de análisis de bastionado innovadoras: sistemas para la comprobación y gestión de los bastionados en diferentes tipos de dispositivos que permitan el conocimiento y comprensión del estado de securizacion de cada uno de los elementos tecnológicos desplegados en las organizaciones.
- Sistemas expertos de recolección de evidencias: es necesario el análisis específico y pormenorizado de los datos que puedan surgir de los procesos anteriores y que permitan de una forma rápida y desatendida el poder determinar puntos débiles de cada una de estas organizaciones.
- Análisis de datos globales: el análisis de todos los datos obtenidos de forma individualizada entre usuarios y su planteamiento de forma coordinada podrá servir para dar soporte, inteligencia y, en definitiva, ayuda al aumento de la ciberseguridad en este tipo de organizaciones.

Funcionalidades

Incluimos un listado no exhaustivo de posibles funcionalidades u objetivos.

- Análisis de nivel de parcheado: la capacidad de análisis de los activos es de vital importancia para la detección de riesgos. Tener sistemas que de forma autónoma e innovadora puedan determinar si activos están actualizados de forma correcta permite este aumento del conocimiento del riesgo en las organizaciones.
- Análisis de securizacion de configuraciones en activos y redes: en múltiples ocasiones, se cree que por tener actualizados los activos es suficiente. Se solicitan capacidades de análisis pormenorizado de los activos utilizados por pymes y autónomos en términos de configuración, tales como: endpoint (tablet, smartphone, portátil) routers, workstation, entre otros.
- Recolección y procesado de datos para crear una Base de Conocimiento de Ciberseguridad para la pyme: capacidades innovadoras de análisis de datos para conformar análisis individuales y globales de la situación de las pymes y autónomos que permitan ser utilizados para dar un seguimiento a las fases de implementación de medidas de seguridad específicas.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba con las siguientes características:

- El **entorno operativo** donde se espera recibir la demostración debe **evidenciar la utilidad y carácter innovador** de la solución demostrada.
- Se valorarán pruebas en un entorno real con un número suficientemente representativo de pymes y autónomos.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores del producto o solución.
  - **Cuáles son las características específicas y diferenciales** sobre las cuales va a construir su solución especializada, indicando sobre qué y cómo se implementan las mejoras con las ya existentes en el mercado.
- Listado de posibles usuarios finales:
  - Pymes
  - Microempresas
  - Autónomos
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☐
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 12: SISTEMAS INNOVADORES PARA EL DESCUBRIMIENTO Y ANÁLISIS DE SERVICIOS EN INTERNET

MOTIVACIÓN

La detección, identificación y monitorización de activos potencialmente vulnerables y expuestos a internet es una de las necesidades que desde entidades gubernamentales se ve necesaria para cuantificar, valorar y mitigar el riesgo nacional hacia sus ciudadanos, entidades y sectores estratégicos. El RD12/2018 de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea indica la necesidad de establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información.

Esto vinculado con la aceleración del uso de dispositivos interconectados aplicados a nuevas interdependencias de conexión, IoT, wearables, cloud computing y edge computing, hacen que el número de dispositivos y por tanto posibilidades de un riesgo nacional aumente.

OBJETO

Descripción del reto

SISTEMAS INNOVADORES PARA EL DESCUBRIMIENTO Y ANÁLISIS DE SERVICIOS EN INTERNET.

Problema a resolver

En la actualidad existen y están en uso aproximaciones tecnologías a estos problemas de origen extranjero (anglosajonas, israelíes e incluso rusas y chinas), convirtiéndose en muchas ocasiones en partes de soluciones o servicios nacionales. Un claro ejemplo son los motores de búsquedas de activos expuestos en internet: Google.com (EEUU), Shodan.io (EEUU), Censys.io (EEUU), redhuntlabs.com (England), onyphe.io (French), binaryedge.io (Zürich, CH), zoomeye (China).

En este reto se buscan aproximaciones innovadoras que permitan la realización de mecanismos de descubrimiento y análisis de servicios expuestos en internet que den respuesta a las retos tecnológicos vinculados con la temática del reto, tratando de aumentar la independencia tecnológica en detrimento de tecnologías de países extranjeros.

La implantación progresiva de IP v6 aporta nuevos desafíos al objeto de este reto, que también podrían dar lugar a soluciones innovadoras.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Innovación en algoritmos de descubrimiento de activos en redes públicas: Se buscan mecanismos, técnicas, algoritmos eficientes e innovadores de descubrimiento de activos vinculadas a las topologías de red existentes y en uso actualmente, aumentando las capacidades y eficacia en la detección e identificación de activos/servicios expuestos.
- Tecnologías de identificación innovadora de vulnerabilidades en activos expuestos de forma activa y pasiva: Diseño, desarrollo y aplicación de técnicas y procedimientos de detección de vulnerabilidades en activos existentes que de forma innovadora puedan ser usados para asegurar que ciertos activos tienen riesgo real de poder ser vulnerados por agentes malintencionados.

- Mecanismos de análisis, detección e identificación de protocolos de comunicación de nueva generación: Para la interconexión de nuevos dispositivos a las redes de comunicaciones, tal como es el caso de todo el ecosistema IoT, los fabricantes están utilizando o incluso creando nuevos protocolos de comunicación de los cuales los sistemas de descubrimiento e identificación de activos expuestos deberán de tener constancia. Es por esto que este caso de uso solicita la aplicación de técnicas y procedimientos que permitan el análisis y disección de dichos protocolos para la identificación de su uso dentro de los activos expuestos a internet.
- Detección e identificación de servicios expuestos: Diseño, desarrollo y aplicación de técnicas y procedimientos innovadores que permitan la detección e identificación de servicios expuestos.
- Detección de sistemas comprometidos expuestos a internet: Diseño, desarrollo y aplicación de técnicas y procedimientos para la identificación de activos que dada su exposición a la red pública hayan sufrido modificaciones en su flujo de servicio debido a interacciones de agentes malintencionados con dichos activos. (Botnet, *ransomware*, cryptomining, Defacement)

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Identificación protocolos:** Descubrimiento e Identificación de protocolos usados en la exposición de activos a internet.
- **Identificación activos**: Identificación de servicios/productos habilitados y expuestos a internet
- **Reconocimiento estado**: Identificación y análisis de activos expuestos a internet para la obtención de información sobre sus configuraciones y estado de exposición., y si estas ponen en riesgo la exposición de dichos activos.
- **Identificación sistemas comprometidos**: Detección e identificación de activos expuestos a internet que por actividades malintencionadas pudieran estar comprometidos por, al menos, las siguientes técnicas: Defacement, *Ransomware*, Botnet, Cryptomining.
- **Análisis Topologías de red**: Detección de activos en topologías de red IPv4 e IPv6 que permitan la detección de activos de forma rápida y eficaz.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se solicita un prototipo de servicio que rastree el espacio de topologías de red pública nacional y que cumpla con objeto descrito en este reto.

Para la definición de alcance esperado de este reto, a continuación se identifican una serie de puntos básicos para su aprobación.

- El **entorno operativo** donde se espera recibir la demostración:
  - Despliegue en entorno controlado, no necesariamente en entorno de usuario final, pero que permita la interacción por parte de al menos 5 usuarios finales al mismo tiempo y utilizando mecanismos de acceso que puedan ser diferenciados (Frontend, API).
  - La solución debe evidenciar su **carácter innovador**.
- El **volumen de información** se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar. Dado que el alcance inicial puede limitarse a nivel nacional debiera de proporcionarse una solución bien dimensionada en este sentido. La **tipología de**

datos que se espera probar son datos que permitan la obtención de resultados objeto del proyecto, siendo el capaz de identificar datos que cumplan, al menos, las siguientes pautas:

- Identificación de activos vinculados a las topologías existentes y usadas a nivel nacional.
- Se valorará la detección del mayor número de protocolos de red diferentes.
- Deberá de poder identificar productos diferentes vinculados a entornos IT, IoT, y OT, valorándose más cuanto mayor número y diversidad de productos identifique.
- Deberá ser capaz de identificar problemas de configuración de los productos detectados, como serían:
  - Necesidad de actualización
  - Credenciales por defecto
  - Autenticación deshabilitada
  - Exposición de información sensible
- Deberá de ser capaz de detectar sistemas comprometidos por distintos tipos de amenazas, como podrían ser:
  - Defacements
  - Ransomware
  - Botnet
  - Cryptomining
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - Cuáles son las características específicas diferenciales de la solución propuesta sobre otras disponibles en el mercado.
  - Cuál es el mercado para el que se espera comercializar la solución.
- Listado de usuarios finales:
  - Habrá al menos dos usuarios que validaran dicho prototipo y su validez:
    - INCIBE.
    - Al menos 1 usuario representativo que propondrá el licitador.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☐
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☐
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 13: INVESTIGACIÓN A PARTIR DE ENTORNOS SIMULADOS (SEÑUELOS)

MOTIVACIÓN

Aunque existen ya varios proyectos que implementan honeys o honeynets, los entornos que simulan y tecnologías que los monitorizan son muy escasos o se necesita trabajar en mejorarlos y en ampliarlos, **añadiendo características innovadoras** de manera que se evite ser detectados por los atacantes, o que los señuelos sean fácilmente reutilizables y escalables, entre otras cuestiones.

Los beneficios[46] de desplegar honeynets para las propias organizaciones son varios. Por ejemplo:

- Distracción para los atacantes, ya que creen que están atacando un sistema real cuando en realidad no es así.
- Obtención de información sobre quién quiere atacar la organización, la metodología que usa, y que herramientas puede estar usando.
- Sirve como herramienta para testear la seguridad que posee el proceso o servicio que simulan. Si imitan fielmente la seguridad actual que posee el sistema, puede ser utilizado en un pentesting para analizar la seguridad de manera que no haya impacto alguno en el proceso industrial real.
- Puede servir para frustrar a los atacantes y disuadirles de atacar más sistemas.

La línea de acción 1 de la Estrategia Nacional de Seguridad, en su medida 1, explica la necesidad de ampliar y mejorar las capacidades de detección de ciberamenazas. Durante los últimos años han surgido diversos proyectos de honeypots[47] orientados a la detección de ciberamenazas en entornos simulados. La mayoría de estos proyectos son desarrollados para entornos TI, pero también han surgido unos cuantos proyectos de honeypots para entornos Operacionales, o de internet de las cosas (IoT). Con el tiempo han ido evolucionado y actualmente se implementan en forma de honeynets, redes enteras de honeypots que simulan sistemas completos, permitiendo así recabar mucha más información sobre los ataques.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos[48] o soluciones que sean innovadores, **que simule un proceso o servicio expuesto en una red considerada no segura** (como internet, red corporativa, entre otras), proceso o servicio cuya ciberseguridad preocupe especialmente a la organización.

OBJETO

El objeto del reto es crear productos o soluciones innovadoras que simulen un servicio o proceso cuya ciberseguridad preocupe a un determinado sector, subsector o tipo de pyme, de manera que a partir de la puesta en marcha del mismo, se monitorice para elevar las capacidades de detección de ciberamenazas dirigidas a dicho sector, subsector o pyme.

Se persigue que el producto o solución propuesta sirva para simular no solo procesos o servicios de especial interés para sectores, subsectores o pymes nacionales y así mejorar sus capacidades de

[46] https://www.incibe-cert.es/blog/honeypot-herramienta-conocer-al-enemigo

[47] sistemas *hardware* o herramientas *software* que simulan ser equipos vulnerables para poder exponerlos sin ningún riesgo y permitir el análisis de todos los ataques efectuados sobre ellos

[48] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

detección de ciberamenzas, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

DETECCIÓN E INVESTIGACIÓN AVANZADA DE AMENAZAS A PARTIR DE ENTORNOS SIMULADOS O SEÑUELOS.

Problema a resolver

Algunos de los problemas a resolver:

- **Alto coste para simular procesos o servicios reales**: para implantar este tipo de tecnologías que simulen procesos o servicios reales (alta interacción), normalmente se han requerido equipamiento extra, con el consecuente coste, ya se trate de *software* y *hardware* real o simulado.
- **Dificultad de disponer de una simulación realista**, especialmente si se necesita simular procesos o servicios relacionados con infraestructuras críticas, ya que si se desea recibir un ataque, deben parecer lo suficiente reales para engañar al enemigo.
- **Configuración segura del entorno**: si el entorno a simular y monitorizar no está correctamente configurado, puede servir como punto de entrada, lo cual sería un problema serio, ya que en vez de dificultar el acceso a los atacantes se les facilita el mismo.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Diseño, despliegue y operación de un señuelo que simule un proceso o subproceso crítico de un sector o subsector estratégico[49]. La simulación respetaría la arquitectura propuesta en el estándar ISA 95 e incluirá elementos mínimos representativos de todos los niveles especificados en la jerarquía propuesta en dicho estándar.
- Diseño, despliegue y operación de un señuelo que simule un elemento de autoconsumo. La medida 32 del MARCO ESTRATÉGICO DE ENERGÍA Y CLIMA[50] destaca la importancia de trabajar en la ciberseguridad en el autoconsumo.
- Diseño, despliegue y operación de un señuelo que simule un elemento comúnmente utilizado por las pymes, microempresas o autónomos.
- Diseño, despliegue y operación de un señuelo que simule un elemento Iot o IIoT comúnmente utilizado.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones, tanto del señuelo como de los elementos de monitorización. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad tanto del señuelo como del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).

[49] Ver lo sectores estratégicos en el ANEXO de la ley 8/2011

[50] https://www.miteco.gob.es/es/ministerio/planes-estrategias/hoja-ruta-autoconsumo/hojaderutaautoconsumo_tcm30-534411.pdf

- **Ofuscación** del entorno a desplegar. El producto o solución propuesta ha de contar con los mecanismos necesarios para evitar que pueda ser clasificada como honey por tecnologías de gathering information, como por ejemplo metabuscadores como shodan o censys.
- **Características específicas del sector, subsector o pyme a simular.** La solución estaría personalizada a las características específicas de sector, subsector o pyme cuyos activos, proceso o servicio se fuera a simular.
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático.
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para monitorizar, detectar y clasificar eventos de ciberseguridad que afectaran al entorno simulado.
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliegue controlado del producto en sectores, subsectores o pymes de similares características. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.
- **Relación** de los ataques detectados con técnicas, tácticas y procedimientos.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:
  - Ha de estar desplegado al menos en **una entidad** que utilice los activos, proceso o servicio que se simule.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición del entorno a simular, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas del entorno simulado a la exposición normal de la infraestructura monitorizada.
- La **duración mínima** esperada para que la prueba de concepto esté funcionando, es del mínimo de meses que se consideren necesarios para probar correctamente la solución, pudiéndose valorar positivamente periodos amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los **aspectos innovadores** de su producto o solución propuesta.
  - Cuál es el **mercado potencial** del producto o solución propuesta.
- Listado de usuarios finales:
  - Al menos 1 usuario final **corporativo** representativo del mercado potencial de la solución propuesta.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐

Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 14: DETECCIÓN VÍCTIMAS CIBERDELITOS

MOTIVACIÓN

La ciberdelincuencia opera de forma globalizada por lo que para afrontar el cibercrimen se han de utilizar enfoques colectivos y supranacionales. Por ello se ha perseguido en los últimos años la armonización en tipificación de conductas delictivas y el establecimiento de procedimientos de cooperación internacional desde el punto de vista jurídico. En España, 2021 se ratificó el Convenio sobre la ciberdelincuencia[51], y posteriormente distintas directivas y decisiones marco de la Unión Europea han motivado reformas en el Código penal[52] y en la Ley de Enjuiciamiento Criminal y también la publicación de la LSSI-CE[53] entre otras[54].

En España los ciberdelitos no tienen una apartado específico en el código penal, clasificándose las conductas delictivas en base al bien jurídico lesionado, así, la Fiscalía especializada en delitos informáticos conoce de dos categorías de delitos:

- delitos cuyo objeto delictivo son los propios sistemas informáticos o las TIC entre otros:
  - sabotaje informático: suprimir, hacer inaccesible o alterar información o datos de un sistema o red, obstaculizar el funcionamiento (DDoS);
  - acceso sin autorización: intrusión e interceptación de datos, programas o sistemas informáticos;
  - revelación de secretos tanto si lesionan la intimidad personal, familiar o la propia imagen, como si afectan a una empresa: interceptación de datos (IP, datos personales, por ejemplo) en trasmisiones no públicas.
- delitos cuya actividad criminal se sirve de las TIC, entre otros:
  - estafas informáticas y fraude: *phishing*, suplantación de identidad, robo uso de tarjetas de crédito, fraude en telecomunicaciones;
  - delitos contra la propiedad intelectual, industrial y afines: plagio, distribución y comunicación de obras protegidas; creación de programas para vulnerar los sistemas de protección de obras protegidas;
  - corrupción de menores y personas discapacitadas;
  - pornografía infantil.
  - falsificación documentos informáticos: documento público oficial y mercantil, documento privado, certificados, tarjetas de crédito;
  - injurias y calumnias;
  - amenazas y coacciones;
  - delitos contra la integridad moral, apología o incitación a la discriminación, el odio y la violencia, justificación de los delitos de genocidio.

Los ciberdelincuentes aprovechan la flexibilidad de los nuevos modelos de negocio tecnológicos (campañas de *malware*, *phishing* y otros ataques *aaS, as a Service*) y la potencia de las nuevas

[51] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[52] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

[53] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

[54] Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza https://www.boe.es/buscar/act.php?id=BOE-A-2020-14046 y Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información https://www.boe.es/buscar/act.php?id=BOE-A-2021-1192

tecnologías para evadir la posible vigilancia, cambiando la ubicación de los servidores desde donde lanzan los ataques (por ejemplo, DDos, *phishing*) o donde recogen los beneficios (por ejemplo, datos de tarjetas robadas o pagos de rescates de *ransomware*). Conscientes de esto existen en marcha redes de cooperación policial[55] y para los sectores que se enmarquen dentro de la directiva NIS2[56] (energía, transporte, sanidad e infraestructuras digitales se establecerá la Red Europea de Organización para Crisis Cibernéticas (EU-CyCLONe) para el apoyo a la gestión de incidentes de ciberseguridad a gran escala de manera coordinada.

En este sentido, se han realizado cooperaciones en el marco de proyectos de INCIBE cofinanciados por la UE[57], por ejemplo 4NSEEK[58] *Forensic Against Sexual Exploitation of Children* y ASASEC[59] *Advisory Sistem Against Sexual Explotaition of Children* durante los cuales se desarrolló una herramienta con reconocimiento de imágenes vía IA para la investigación y análisis de este tipo de delitos. Se plantea la aplicación de enfoques similares de forma innovadora para la detección, investigación y análisis de los delitos anteriormente mencionados que puedan ser aprovechados tanto por las FCSE como por organismos internacionales.

OBJETO

Descripción del reto

DETECCIÓN INTELIGENTE DE VÍCTIMAS DE CIBERDELITOS UTILIZANDO TÉCNICAS INNOVADORAS.

Problema a resolver

Se hace necesaria la vigilancia, supervisión y control, incluyendo técnicas innovadoras[60], de los distintos bienes jurídicos susceptibles de ser el objeto de los ciberdelitos (identidades, datos de comunicaciones, documentos electrónicos, tarjetas, aplicaciones y sistemas) ante la sospecha de que ha ocurrido un delito o de que pueda ocurrir, incluidos los casos que hayan de ser autorizados por un juez. En esta vigilancia puede requerir además la autorización del propietario del bien supuestamente vulnerado, la colaboración de operadores de telecomunicaciones y proveedores de servicios TIC según lo establecido en la ley.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- **Organismos nacionales e internacionales con competencias en la protección de ciudadanos y empresas**. El sistema podrá será utilizado para la detección de víctimas y el origen del ataque (trazabilidad) para la posterior gestión de estos incidentes de ciberseguridad. Estos incidentes podrían ser reportados a:

[55] https://www.interpol.int/es/Delitos/Ciberdelincuencia/Respuesta-a-las-ciberamenazas

[56] https://www.europarl.europa.eu/thinktank/es/document/EPRS_BRI(2021)689333

[57] https://www.incibe.es/proyectos-europeos

[58] https://www.incibe.es/proyectos-europeos/4nseek y https://www.incibe.es/proyectos-europeos/4nseek/herramienta

[59] https://www.incibe.es/proyectos-europeos/asasec

[60] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

- Operadores de redes y proveedores de servicios, para que se encarguen de alertar a sus clientes que están siendo víctimas y pongan los medios para proteger sus equipos.
- Fuerzas y cuerpos de seguridad, para que se encarguen de tramitar las denuncias de aquellos que sean susceptibles de constituir delito.

- **Fuerzas y cuerpos de seguridad nacionales e internacionales**. El sistema podrá ser utilizado para el desmantelamiento de los servidores y otras infraestructuras de los delincuentes.
- **Empresas de ciberseguridad** que dentro de sus servicios ofrezcan:
  - **Venta de *feeds* de información de inteligencia**. Podría ser vendida a organismos nacionales o internacionales con competencias en la protección de ciudadanos y empresas, operadores de redes y proveedores de servicios que quieran proteger a sus clientes, fuerzas y cuerpos de seguridad nacionales o internacionales que traten de desmantelar los servidores y otras infraestructuras de los ciberdelincuentes u otras empresas de ciberseguridad que ofrezcan los servicios descritos.
  - **Servicios de detección y protección a ciudadanos y empresas**. Para su uso en empresas de ciberseguridad que ofrezcan medidas de protección a sus clientes contra amenazas.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- Identificación de la víctima y su fiabilidad.
- Monitorización continua y en tiempo real.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**: posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes:** elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas:** ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia del sistema.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio e interoperabilidad:** posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Escalabilidad:** se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado de la solución.
- **Simplificación:** se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución de la misma.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- El sistema debe estar desplegado en un entorno operativo donde se pueda realizar una demostración:
  - Detectando víctimas nacionales.
  - La funcionalidad acordada para el sistema tiene que estar completada y totalmente operativa.
  - La solución debe evidenciar también su **carácter innovador**.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 15: DETECCIÓN DE VÍCTIMAS DE BOTNETS A TRAVÉS DE TÉCNICAS INNOVADORAS

MOTIVACIÓN

Se puede definir *botnet* como término que hace referencia a un conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc.

Las botnets se caracterizan por tener un servidor central (C&C, de sus siglas en inglés Command & Control) al que se conectan los bots para enviar información y recibir comandos.

Existen también las llamadas botnets P2P que se caracterizan por carecer de un servidor C&C único.

Desde el descubrimiento en el año 2000 de la primera *botnet*, el número de las mismas no ha parado de crecer y de diversificarse. En la actualidad son millones de ciudadanos nacionales e internacionales que de manera inconsciente forman parte de una *botnet*.

Con el paso de los años las *botnets* han ido mutando, adaptándose a las tendencias de los usuarios respecto a sistemas operativos, *software* antimalware… y han sabido convertir el malware y su control en un negocio muy rentable para las redes criminales que hay detrás.

Debido tanto a problemas de seguridad que hacen que ciertos equipos/dispositivos sean vulnerables como al desconocimiento por parte de usuarios del riesgo al que están expuestos, el número de *bots* no para de crecer y la repercusión sobre la víctima cada vez es mayor. Con el tiempo, surgen amenazas más agresivas que pueden por ejemplo llevar a cabo acciones como cifrar los datos del dispositivo/equipo de la víctima o robar datos bancarios.

Hay muchas formas de categorizar las *botnets*, ya sea por el sistema operativo objetivo, el vector de infección, por la vía de comunicación, por el tipo de información que recopila, por las acciones que realiza, etc. Teniendo en cuenta su vía de comunicación, se pueden diferenciar dos grandes grupos: las *botnets* centralizadas y descentralizadas.

Los *bots* pertenecientes a una *botnet* centralizada, realizan las comunicaciones directamente con la consola de mando y control (C&C) o a un proxy intermedio, pero sin pasar la comunicación a otros *bots*. Esto permite al atacante mayor sigilo en el *bot* ya que este únicamente realizará peticiones (normalmente HTTP) al C&C, no siendo un comportamiento extraño ni fácilmente detectable por medidas de seguridad.

Por otro lado, al ser una comunicación centralizada, el *bot* tiene que saber dónde conectarse para comunicarse con su C&C. De este modo, mediante ingeniería inversa, un investigador podría ser capaz de ver la dirección IP, el dominio o el algoritmo de generación de dominios utilizado por la *botnet* de tal manera que podrá llevar a cabo acciones para el bloqueo de las comunicaciones o la suplantación del C&C.

En el caso de las *botnets* descentralizadas, la investigación se complica ya que no existe un nodo central al que se conecten todos los miembros de la *botnet*. Los *bots* dentro de su código tienen una serie de direcciones IP o dominios a los que conectarse, no siendo estos nada más que nodos intermedios que reciben la comunicación y la reenvían al siguiente nodo de la pirámide. Esto provoca que los nodos intermedios dispongan de puertos abiertos para la recepción de la información de los nodos inferiores, provocando un comportamiento anómalo en el equipo infectado. Según se cree, la promoción de nodo inferior a nodo intermedio, aunque varía dependiendo de la amenaza, depende de factores como tiempo que lleva el equipo infectado, servicios en funcionamiento, *software* instalado, etc., buscando evadir así los sistemas de análisis automatizado en la medida de lo posible.

Además, muchas botnets utilizan técnicas como por ejemplo FastFlux para el rotado de IPs y dominios que contribuyen a dificultar dicha investigación.

En la actualidad existen cientos de familias y amenazas que tienen a su disposición a los equipos infectados de los usuarios, sin estos siquiera saberlo. Esta dispersión ha provocado que los medios de infección y de comunicación sean muy diversos, dificultando la investigación para los organismos encargados de ello. Debido a la sofisticación de las amenazas y a la falta de mecanismos que puedan ayudar en dichas investigaciones, la investigación de este tipo de delito es muy baja y la tasa de éxito aún más baja.

OBJETO

Descripción del reto

DETECCIÓN DE VÍCTIMAS DE BOTNETS Y ANÁLISIS DEL COMPORTAMIENTO DE REDES BOTNET A PARTIR DE TÉCNICAS INNOVADORAS.

Problema a resolver

El objeto de este reto es la contratación de los servicios de investigación de técnicas avanzadas para la detección de *bots* y, opcionalmente, servidores de comando y control (C&C), además de la implementación de un sistema que permita la investigación y el tratamiento de la información recibida, siendo aplicable para cualquiera de los tipos de *botnet* (priorizando *botnets* descentralizadas).

Adicionalmente, se busca la posibilidad y facilidad de un sistema que permita a un operador interactuar con la botnet, engañando a la red y simulando ser así un bot infectado. Facilitando al operador a través de un sistema de monitorización de la red, modelar de manera sencilla las comunicaciones con la misma y seguir en todo momento su comportamiento.

Este sistema permitirá la identificación de millones de ciudadanos nacionales e internacionales que de manera encubierta forman parte de una *botnet*. Estos resultados podrán ser utilizados para comunicar a las autoridades competentes, y en último término alertar a los proveedores de servicios de las víctimas o a los propios ciudadanos infectados.

Por otra parte, con la identificación de los servidores de mando y control (C&C) se podría alertar a las Fuerzas y Cuerpos de Seguridad para tratar de ubicarlos y proceder a su desmantelamiento y con ello terminar con la *botnet*.

Además, ayudará a la investigación del comportamiento de la botnet que será clave para poder llevar a cabo las acciones anteriores de manera proactiva además de ayudar en la investigación y documentación temprana de la red.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Organismos nacionales e internacionales con competencias en la protección de ciudadanos y empresas. El sistema podrá ser utilizado para:
  - La detección de víctimas y paneles de comando y control (C&C) y la posterior gestión de estos incidentes de ciberseguridad. Estos incidentes podrían ser reportados a:
    - Proveedores de servicios, para que se encarguen de alertar a sus clientes que están siendo víctimas (*bots*) y pongan los medios para limpiar sus equipos infectados (clearing house), dejando así de pertenecer a esta red.
    - Fuerzas y Cuerpos de Seguridad, para que se encarguen de intentar desmantelar los servidores de comando y control (C&C) terminando con la *botnet*.

- Elaboración de contenidos de concienciación para ciudadanía y para las empresas.

- **Fuerzas y Cuerpos de Seguridad nacionales e internacionales**. El sistema podrá ser utilizado para el desmantelamiento de los servidores de comando y control (CYC) terminando con ello con la *botnet.*
- **Empresas de ciberseguridad** que dentro de sus servicios ofrezcan:
  - **Venta de *feeds* de información de inteligencia**. Podría ser vendida a organismos nacionales o internacionales con competencias en la protección de ciudadanos y empresas, proveedores de servicios que quieran proteger a sus clientes, Fuerzas y Cuerpos de Seguridad nacionales o internacionales que traten de desmantelar los servidores de comando y control (C&C) terminando con ello con la botnet u otras empresas de ciberseguridad que ofrezcan los servicios descritos.
  - **Servicios de detección y protección a ciudadanos y empresas**. Empresas de ciberseguridad que ofrezcan medidas de protección a sus clientes contra este tipo de amenazas.
- **Universidades, centros de investigación u otros organismos** dedicados al análisis del comportamiento de las redes:
  - **Documentación** de redes botnet que ayuden en la investigación y el conocimiento general de las mismas.
  - **Monitorización del comportamiento de las mismas** para una detección proactiva de nuevos bots o C&C.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- Gestión de amenazas y familias de amenazas.
- Monitorización del comportamiento de las redes en base a las comunicaciones.
- **Mecanismos innovadores** que, a través del análisis del comportamiento de la red, permitan **filtrar falsos positivos**.
- Monitorización continua y en tiempo real.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Envío de alertas personalizadas.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Identificación de la IP de la víctima y su fiabilidad** (probabilidad de que realmente se trata de una víctima de una *botnet*).
- **Identificación de la IP del servidor de comando y control (CYC) y fiabilidad** (probabilidad de que realmente se trata de un servidor de comando y control, detectando, por ejemplo, técnicas de *sinkhole)*.
- **Análisis del comportamiento** de la red y detección de cambios en el mismo en tiempo real.
  - Envío de alertas automatizado ante cambios en el comportamiento de las redes.
- **Exportación de bots** en base a necesidades específicas.
- Exportación de información obtenida de C&C.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.

- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia del sistema.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto.
- **Simplicidad.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba del **sistema desplegado en un entorno operativo** donde se pueda realizar una demostración:
  - Detectando víctimas nacionales (*bots*) y servidores de comando y control (C&C).
  - Posibilitando el análisis de las redes botnets.
  - Alertando de cambios en el comportamiento de las redes.
  - Facilitando la adaptabilidad ante los cambios de comportamiento anteriores.
  - La funcionalidad acordada para el sistema tiene que estar completada y totalmente operativa.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen y tipología de datos** han de ser similares a los de un entorno real.
- La **duración** de la prueba de concepto será suficiente para abarcar las tipologías de operaciones habituales.
- Listado de usuarios finales:
  - Al menos una organización.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 16: SISTEMAS PARA EL SEGUIMIENTO DE CRIPTO-TRANSACCIONES

MOTIVACIÓN

Ciberdelitos como el *ransomware* mueven anualmente casi 600 Millones de dólares en pagos solo en el primer semestre de 2021. Esto hace que organizaciones de seguridad como el FBI, NSA, FinCEN o Europol generen acciones para el análisis, seguimiento, detección y atribución de las transacciones vinculadas a este tipo de ataques. Las formas en las que los actores malintencionados o cibercriminales atacan a los sistemas están siendo cada vez más sofisticadas y con ello los flujos en los que tratan de esconder los pagos recibidos por estas acciones. Es por ello que este reto busca dar solución a los problemas actuales y futuros de trazabilidad, detección y atribución de transacciones debidas a campañas originadas por el cibercrimen.

OBJETO

El objeto del reto persigue que el producto o solución propuesta sea aplicable y desplegado no solo permita a organizaciones gubernamentales o Fuerzas y Cuerpos de Seguridad a realizar seguimientos, detecciones y/o atribuciones a nivel nacional, si no **que puedan ser capaces de apoyar a organizaciones espejo en incidentes similares a nivel internacional.**

Descripción del reto

SEGUIMIENTO DE TRANSACCIONES VINCULADAS CON *RANSOMWARE* Y OTRAS CAMPAÑAS.

Problema a resolver

El seguimiento de transacciones económicas vinculadas con acciones delictivas es una tarea ardua y compleja, más si cabe desde la aparición y uso de las criptodivisas. En este reto se tratara de dar solución a los problemas de algoritmia e investigación aplicada que se han de utilizar para el seguimiento de estos montantes económicos a lo largo de su ciclo hasta llegar a convertirse en un beneficio tangible para el actor malicioso.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Trazabilidad y seguimiento**: cada avance tecnológico en el sector fin-tech[61] y en concreto en el de criptodivisas crea situaciones que dificultan el seguimiento de estas transacciones.
- **Detección e identificación**: la facilidad de creación, eliminación y traspaso de montantes económicos en el mundo de criptodivisas dificulta la detección e identificación de cuentas o "wallets" vinculadas con acciones delictivas debido a los elementos existentes que permiten la ofuscación, tales como los mezcladores.
- **Atribución**: aunque existen avances en la materia, con frecuencia se encuentran dificultades para determinar el origen o destino de este tipo de activos, lo que dificulta en gran medida las acciones pertinentes por parte de las autoridades competentes.
- **Alcance**: el conocimiento de alcance económico que una campaña delictiva está teniendo, es uno de los factores a utilizar para saber su impacto y esto es fundamental para saber priorizar los riesgos existentes y su mitigación.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

[61] ***Fintech*** es un sector integrado por empresas que utilizan la tecnología para mejorar o automatizar los servicios y procesos financieros. El término *fintech* hace referencia a un sector en rápido crecimiento que se orienta a los intereses de los consumidores y a las empresas.

- **Algoritmos de seguimiento**: creación de nuevos algoritmos que permitan el seguimiento de transacciones y mitigar técnicas de ocultación como “chain hopping”.
- **Detección e identificación en Criptomoneda novedosas**: creación de tecnologías y métodos innovadores que permitan detección en sistemas de Criptomoneda cuyo nivel de anonimato es superior a los estándares.
- **Clasificación y atribución de direcciones de billeteras “wallets”**: crear capacidades de detección de “wallets” utilizadas para la acumulación, transacción y/o cobro de Criptomoneda y vincular estas a campañas y/o cibercriminales.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Obtención de información tangible a partir de datos en bruto de transacciones en blockchain y similares.** A partir de información que pueda ser recogida de las propias transacciones obtener inteligencia útil para los usuarios finales.
- **Capacidades de seguimiento y atribución de campañas.** Lograr vincular campañas que están sucediendo o que ya han sucedido con “wallets” para agregar información adicional a los incidentes.
- **Enriquecimiento**: Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Detección de entidades vinculadas a direcciones concretas.** Elaboración de un mapa de “wallets” y su vinculación a entidades reales que puedan ser requeridas.
- **Categorización de “wallets” por actividad:** Generación de sistema de categorización de tipos de “wallets” por su uso en el ciclo de vida de las transacciones.
- **Intercambio.** Seguimiento en cambios de criptodivisas y/o en dinero de curso real u otros medios (oro)

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:
  - Ha de estar desplegado para que pueda ser usado por al menos:
    - **una entidad** del Sector Financiero con interés en la materia.
    - INCIBE
    - Usuarios vinculados al **Sector Publico** con interés en este tipo de eventos.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de al menos 4 campañas, reales y activas en el momento de la prueba, a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son datos obtenidos derivadas de las transacciones vinculadas a las campañas monitorizadas.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- Expectativas adicionales.
  - Se espera que la oferta explique claramente cuáles son los aspectos innovadores de su producto o solución.
- Listado de posibles usuarios finales:
  - FCSE, fiscalía.

- CERTs.
- Entidades del sector financiero.

- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☐
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☐
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 17: SISTEMA DE DETECCIÓN DE SMS Y MENSAJERÍA INSTANTÁNEA FRAUDULENTOS Y CAMPAÑAS ASOCIADAS

MOTIVACIÓN

El servicio de mensajes cortos o servicio de mensajes simples, más conocido como SMS (*Short Message Service*), es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos (con un límite de caracteres) entre teléfonos móviles. Aunque fue inventado en 1985, a día de hoy es ampliamente utilizado por los usuarios. A su vez existe una evolución del servicio que permite insertar objetos multimedia MMS (*Multimedia Message Service*).

Este servicio es utilizado para muchos propósitos y sus casuísticas han ido evolucionando a lo largo del tiempo. Actualmente entre los usos más comunes se encuentra la comunicación con los usuarios de servicios o como medio para la doble autentificación *2FA.*

Su extensivo uso es aprovechado por los cibercriminales como vía de entrada para tratar de engañar y estafar a los usuarios. Entre las técnicas que utilizan está, por ejemplo, el *smishing*, una técnica concreta de *phishing* en la que envían mensajes de texto haciéndose pasar por entidades reales, buscando con ello robar datos o infectar los dispositivos de los usuarios. Otra de las técnicas sería el SMS *spoofing* que consiste en enviar un SMS falsificando el remitente de los mensajes, de forma que al usuario le aparezca como que le ha llegado un mensaje, por ejemplo, de su banco, pero en realidad detrás está un cibercriminal. En muchas ocasiones, podemos encontrar una mezcla de ambas técnicas para aumentar la probabilidad de éxito del engaño.

Lo relevante de este tipo de estafas es el contenido del SMS recibido. Normalmente incluyen un enlace que te llevará a una página diseñada haciéndose pasar por la web real de la entidad. La víctima creerá que es una entidad real, te dicen que hay un problema y te redirigen, mediante el enlace, a una web oficial en la que vas a poder solucionarlo. Por ejemplo, hay cientos de este tipo de estafas relacionada con entidades bancarias. En ellas, se te dice que tu cuenta de banco ha sido suspendida, y que tienes que seguir una dirección que te adjuntan en el mensaje para confirmar tu identidad.

En algunos tipos de ataque, lo que se pide es el inicio de sesión para robarle los datos de acceso al banco. Si el ataque es más elaborado, puede que incluso el cibercriminal utilice las credenciales de inmediato y te pida por la web fraudulenta que escribas algún tipo de código de confirmación que te llegue por mensaje.

Incluso, en otro tipo de ataques, se puede pedir la descarga de alguna aplicación de móvil, y esto podría suponer la infección por algún tipo de malware del dispositivo.

Todas estas técnicas pueden llevar a robo de datos personales, entre ellos datos bancarios, lo que podría llevar a su vez a robos de dinero en las cuentas bancarias de los usuarios. Por otro lado, la infección con malware del dispositivo puede llevar a que se hagan con el control, robando de nuevo todo tipo de información.

Más allá de las estafas enfocadas a los SMS, se pueden identificar fraudes cuyo canal de distribución se encuentra en la mensajería online como WhatsApp o Telegram.

La irrupción de los “smartphones” o teléfonos inteligentes promovió el éxito de las aplicaciones de mensajería instantánea, ya que el envío de mensajes se hace sin coste adicional para el usuario. WhatsApp, fundado en 2009 y Telegram en 2013, son dos de las aplicaciones más populares en estos últimos años, alcanzando una amplia cuota de mercado. Debido a esto, muchos de los fraudes detectados en los teléfonos móviles inteligentes se centran en estas aplicaciones de mensajería instantánea.

Existen diversos casos y a continuación se detallan algunos de ellos.

La suplantación de cuentas de conocidos, familiares o amigos para la petición de dinero o información confidencial es una técnica de fraude común dentro de la mensajería online. En estos casos la cuenta de un contacto ha sido secuestrada y es utilizada para engañar a una persona de su confianza, pidiendo cierta información confidencial o dinero con carácter urgente. Muchas de estas estafas pueden derivarse en sucesos de impacto económico y reputacional como “la estafa del CEO”.

Así mismo, el reenvío de cadenas de mensajes con información falsa sobre alguna oferta interesante o regalo de algún tipo es otra técnica habitual de fraude en mensajería online. Suelen distribuirse por estos canales mensajes con ofertas atractivas donde comparten una web fraudulenta con el objeto de recopilar información confidencial (datos personales o bancarios) o, en algunos casos, para la descarga de una aplicación maliciosa.

Se han identificado grupos de conversación en estas aplicaciones de mensajería donde se difunden fraudes generalizados, ofreciendo ciertos servicios falsos de un modo masivo.

OBJETO

Descripción del reto

SISTEMA DE DETECCIÓN DE SMS Y MENSAJERÍA INSTANTANEA FRAUDULENTOS Y CAMPAÑAS ASOCIADAS.

Problema a resolver

Este sistema permitirá evitar estafas a ciudadanos y empresas a través del envío de SMS a dispositivos móviles. Para ello, se investigará y desarrollará una aplicación móvil que instalada en los dispositivos de los usuarios permita alertarles en tiempo real sobre esta amenaza evitando el potencial fraude.

Por otro lado, el sistema permitirá analizar millones de muestras de SMS fraudulentas con el objeto de detectar de forma proactiva campañas fraudulentas contra ciudadanos y empresas, de forma que puedan hacerse públicas y se evite de nuevo el potencial fraude.

Cabría la posibilidad de atribuir el modus operandi del fraude a un mismo origen o grupo delictivo, identificando técnicas similares en diferentes campañas pudiendo de esta forma relacionarse entre sí.

Así mismo podrá considerarse la detección e identificación automática de las empresas o entidades suplantadas en la comisión del fraude o incluso las marcas o productos víctimas del hecho delictivo, usando, si así procede, técnicas de inteligencia artificial.

Incluirá dentro del alcance la posibilidad de ampliar esta monitorización y servicio de alerta temprana sobre aplicaciones móviles de mensajería instantánea tipo WhatsApp o Telegram, accediendo para ello al texto de las notificaciones que generan estas aplicaciones. De forma que si el vector de entrada no es un SMS y es un mensaje desde este tipo de aplicaciones, se pueda detectar el fraude y se trate de evitar el daño a ciudadanos o empresas.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- **Aplicación *software* instalada en dispositivo móvil de usuario**. Esta aplicación será capaz de leer los SMS que lleguen al dispositivo, los analizará en tiempo real y alertará al usuario de un potencial fraude. Se espera que los analizadores empleen técnicas de inteligencia artificial para detectar el fraude, categorizarlo y alertar al usuario con una alta probabilidad de acierto.

Esta aplicación móvil enviará información sobre las detecciones al sistema de inteligencia descrito en el tercer caso de uso.

- **Sistema virtual señuelo que simule móviles de usuarios**. Este sistema permitirá simular cientos o miles de dispositivos móviles con sus correspondientes números reales de forma que puedan hacer las funciones de señuelo, es decir, servirán para atraer el posible envío de SMS fraudulentos. Con ello, se busca disponer de una fuente amplia de información sobre esta amenaza, para su estudio y alerta temprana de campañas fraudulentas.
- **Sistema inteligente de análisis, tratamiento y explotación**. A este sistema llegará toda la información que proviene de los casos de uso anteriormente descritos. Es decir, tanto las aplicaciones móviles de los usuarios (bajo su aceptación de permisos) como el sistema virtual señuelo que simula móviles de usuarios actuarán como fuente de información. La información será analizada, se tratará y el sistema permitirá su explotación.
- Dentro del alcance del reto se considera la posibilidad de ampliar esta monitorización y servicio de alerta temprana sobre aplicaciones móviles de mensajería instantánea tipo WhatsApp o Telegram. En este caso, muchas de las estafas hacen uso de técnicas de ingeniería social y tienen como escenario un diálogo entre el cibercriminal y la víctima a través de la aplicación móvil. Por lo tanto, los analizadores que incluyan los tres casos de uso listados anteriormente, permitirán analizar las conversaciones y, haciendo uso de algoritmos de inteligencia artificial, alertarán al usuario de una potencial amenaza.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- Detección y clasificación del fraude por SMS o mensajes en aplicaciones móviles:
  - Clasificación del fraude.
    - Tipo de fraude. (bancario, logística, ofertas, etc…).
    - Nivel de riesgo.
  - Identificación y extracción de información relevante:
    - Entidad suplantada.
    - Marca o producto víctima del fraude.
- Detección de campañas de fraude por SMS o mensajes en aplicaciones móviles.
  - Identificación de campañas masivas en base a:
    - La entidad o marca suplantada.
    - Las técnicas utilizadas.
    - Información sensible que se pretende robar.
    - Otros criterios identificados.
  - Agrupación de campañas en base a su similitud.
    - Relacionar campañas de fraude masivas con otras previas detectadas por el sistema.
    - Generar indicios de autoría, origen o atribución de grupos delictivos.
- Repositorio de fraudes por SMS y aplicaciones de mensajería online.
  - Sistema de consulta de mensajes fraudulentos en base a su exactitud o similitud, usando técnicas de inteligencia artificial, reportados por las diversas fuentes.
  - Interoperabilidad del repositorio con herramientas de uso común por parte de CERT.
- Monitorización continua y en tiempo real.
  - Detección y clasificación, lo más automatizada posible, de alertas.

- Correlación de eventos y/o alertas.
- Mecanismos innovadores de detección de falsos positivos.
- Identificación de las entidades suplantadas.
- Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.

- **Enriquecimiento**: Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia del sistema.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- El sistema, para cumplir con los TRL indicados en este documento regulador, debe estar desplegado en un entorno operativo donde se pueda realizar una demostración:
  - Instalada la App en un dispositivo móvil. Detectando SMS fraudulentos o mensajes de aplicaciones y alertando al usuario y enviando la información al servicio de inteligencia.
  - Desplegados cientos de móviles señuelos. Detección de SMS fraudulentos o mensajes de aplicaciones y envío de información al servicio de inteligencia.
  - Recepción del servicio de inteligencia de información de las distintas fuentes, tratamiento de la información y explotación mediante interfaz web con opción de una API REST de consulta.
  - Evidencia de interoperabilidad con herramientas de uso común de CERT.
  - La funcionalidad acordada para el sistema tiene que estar completada y totalmente operativa.
  - La solución debe evidenciar también su **carácter innovador**.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒

Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 18: ATRIBUCIÓN DE CIBERAMENAZAS MEDIANTE TÉCNICAS INNOVADORAS

MOTIVACIÓN

La agrupación de incidentes de ciberseguridad según provengan o no del mismo actor malicioso ayuda a definir mejor la respuesta más apropiada, así como en la investigación forense del incidente y en la predicción de lo que puede ocurrir a continuación. Asimismo, el poder seguir la evolución delas TTP's de distintos actores maliciosos ayuda a planificar una mejor defensa ante ataques futuros.

Además, la Unión Europea a través de PESC[62] está en disposición de aplicar medidas o sanciones restrictivas para evitar y/o mitigar conductas delictivas orientadas hacia Europa y/o sus Estados miembros. Para que desde los Estados miembros o desde la propia Comisión Europea pueda aplicar estas sanciones se debe tener conocimiento de la atribución de los ciberataques o acciones malintencionadas por parte de actores. A nivel España y según la Estrategia Nacional de ciberseguridad 2019, en la que se manifiesta la dificultad de accionar correctas atribuciones en eventos de ciberseguridad, propone en su línea de actuación 1 "*Reforzar las capacidades ante las amenazas provenientes del ciberespacio*", en su medida 1, "*el desarrollo y elaboración de mecanismos de inteligencia necesarios",* para entre otras cosas*, "la atribución de ciberamenazas.*"

Considerando la complejidad que implica saber que actores se encuentran detrás de determinadas acciones y las diferentes aproximaciones posibles, se necesita profundizar en cómo abordar la obtención de datos de los diferentes pilares que componen la atribución y los mecanismos y algoritmos que permitan su vinculación y agrupación para dar una respuesta unificada.

OBJETO

El objeto del reto es crear tecnologías, soluciones o servicios innovadores de ciberseguridad que permitan el análisis, agrupación según actor malicioso y atribución de campañas malintencionadas.

Descripción del reto

ATRIBUCIÓN DE CIBERAMENAZAS MEDIANTE TÉCNICAS INNOVADORAS.

Problema a resolver

La atribución de acciones malintencionadas en el mundo ciber es una tarea complicada y más cuando se desea alinear y correlacionar los tres pilares principales de la ciberinteligencia: razonamiento, análisis técnico de Indicadores de Compromiso (IOC) obtenidos y datos geopolíticos que afectan al escenario.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Nivel alto de ocultación**: los ciberincidentes tiene un componente muy específico que permite a los autores capacidades de ocultación mucho mayores que los incidentes que puedan realizar de forma física.
- **Dispersión geográfica**: multitud de incidentes que se producen en territorio nacional viene orquestados y ejecutados desde fuera de nuestras fronteras, esto hace que sea complejo la atribución y seguimiento de los autores.
- **Nivel de fiabilidad**: hasta la fecha la capacidad de atribuir un incidente de ciberseguridad con un actor malintencionado es complejo y que impide aseverar de forma rotunda. Es necesario aumentar los niveles de fiabilidad de la atribución de eventos hacia actores maliciosos.

[62] https://www.sanctionsmap.eu/#/main/details/47/

- **Visión global**: la atribución de incidentes de ciberseguridad no puede basarse en factores únicos y específicos, la atribución debe de tomar varios paradigmas y múltiples factores (técnicos, sociales y geopolíticos) para poder alcanzar un nivel superior de resultado.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- **Capacidad de disuasión de ataques frente a organizaciones o estados**: la capacidad de atribución de incidentes permitiría la generación de estrategias de diplomacia, disuasión o respuesta de manera oportuna y eficaz.
- **Análisis técnico de Indicadores de Compromiso obtenidos de un incidente**: La realización de análisis forenses de las evidencias tecnológicas vinculadas a un incidente de seguridad son de alto interés para la atribución a actores malintencionados específicos.
- **Sistemas integrales de correlación de información**: sistemas que son capaces de correlacionar y aportar inteligencia agregada a partir de múltiples fuentes de información. Hasta la fecha la atribución se basa en tres tipos de fuentes: La OSINT, la inteligencia técnica y los datos privados de las organizaciones o estados que se obtienen en incidentes específicos y que no son públicos.
- **Creación de perfilado de actores malintencionados**: la creación de perfilado de actores malintencionados es una de los casos de uso de la atribución, en el los sistemas y analistas realizaran perfilados de alto nivel informativo sobre las amenazas y sus autores.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Base de Conocimiento:** se tiene necesidad de que se pueda tener una base de conocimiento con toda la información de los actores malintencionados, sus ATT&Ck e información usable y de alto valor.
- **Múltiples pilares de información:** se ha de tener capacidad de recepción de múltiples datos provenientes de varias fuentes de datos, entre las que se deberán encontrar:
  - Datos proporcionados por usuarios. (logs, muestras de malware, IOC, hashes, entre otros)
  - Datos OSINT
  - Datos enviados desde dispositivos de seguridad de forma autónoma.
  - IOC proporcionados por feeds de información publico/privada
- **Análisis y correlación innovadora de la información:** el sistema deberá realizar un análisis de los datos obtenidos de forma que, de forma innovadora y novedosa aplique matices a los sistemas actuales de atribución y como resultado de una/s serie/s de atribuciones, su porcentaje de fiabilidad en cada una de ellas y una argumentación más avanzada que las existentes por los métodos existentes.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba con las siguientes características:

- El **entorno operativo** donde se espera recibir la demostración:
  - Despliegue en entorno controlado, no necesariamente en entorno de usuario final, pero que permita la interacción por parte de al menos 5 usuarios finales al mismo

tiempo y utilizando mecanismos de acceso que puedan ser diferenciados (Frontend, API).

- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que aumente el nivel de atribución actual, mejorando sensiblemente las bases de conocimiento existentes (Mitre ATT&CK, entre otras), debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera datos reales vinculados a actores y amenazas reales que estén en ejecución en el momento de la prueba, así como resultados de amenazas y actores ya producidos y de los cuales se tienen datos fiables de atribución que permitan validar los resultados de este prototipo.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - Cuál es el mercado potencial de la solución.
- Listado de usuarios finales:
  - Al menos 2 usuarios de diferentes validaran el prototipo:
    - INCIBE.
    - 1 usuario final representativo del mercado potencial de la solución.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☐
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☐
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☒
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 19: SOC SECTOR ENERGÍA

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[63].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital o la recomendación 2019/553 de la CE que destaca incluso el efecto cascada que pueda suponer un problema de ciberseguridad en este sector.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector Energía o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR ENERGÍA O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

Los ciberataques a las infraestructuras energéticas, son una de las mayores amenazas a la ciberseguridad. Según diferentes análisis de inteligencia y las amenazas son cada vez más

[63] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

sofisticadas y numerosas por lo que se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten al sector energía, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinados por algún estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector energía, sino también a toda la cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Energía, subsector Electricidad.
- Centro de Operaciones de Ciberseguridad especializado en el sector Energía, subsector Crudo.
- Centro de Operaciones de Ciberseguridad especializado en el sector Energía, subsector Gas.
- Centro de Operaciones de Ciberseguridad especializado en el sector Energía, subsector Nuclear.
- Soluciones innovadoras específicas para la ciberseguridad en gasolineras.
- Soluciones innovadoras específicas para la ciberseguridad en centrales de producción eólicas.
- Soluciones innovadoras específicas para el autoconsumo[64].

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro

[64] Por poner un ejemplo más concreto, la aplicación de tecnologías innovadoras como por ejemplo el blockchain para compartir el uso de la energía entre los usuarios de una misma red, que permita el volcado de los excedentes de energía a otros vecinos, o consumiendo del resto de usuarios cuando estos se encuentren fuera de casa, podría cambiar para siempre el concepto de red eléctrica, permitiendo hacer un uso más eficiente y seguro garantizando una energía más sostenible y asequible.

las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).

- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector energía).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso del sector Energía (activos IT/OT, IoT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
    - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
    - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
    - Detección y clasificación, lo más automatizada posible, de alertas.
    - Correlación de eventos y/o alertas.
    - Mecanismos innovadores de detección de falsos positivos.
    - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia del SOC.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Ha de estar desplegado al menos en **una entidad** del Sector Energía, de cualquiera de su subsectores.
- Además, el entorno debe evidenciar una **convergencia IT/OT**[65].
- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas del Centro de Operaciones a la exposición normal de la infraestructura monitorizada.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector Energía**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[65] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 20: SOC SECTOR TRANSPORTE

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[66].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector Transporte o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR TRANSPORTE O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

A medida que el transporte pasa a regirse por nuevos estándares de datos y por un mayor uso compartido de los mismos, se ha convertido en el tercer sector más vulnerable del mundo en cuanto a exposición a ciberataques, según la documentación técnica publicada por Gallagher Insurance, una de las mayores empresas de correduría de seguros, gestión de riesgos y consultoría del mundo.

---

[66] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

Todos los subsectores, incluidos el marítimo, ferroviario, de camiones, proveedores de logística y repartidores de paquetes, se ven afectados.

Se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinados por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Transporte, subsector transporte aéreo.
- Centro de Operaciones de Ciberseguridad especializado en el sector Transporte, subsector transporte por ferrocarril.
- Centro de Operaciones de Ciberseguridad especializado en el sector Transporte, subsector transporte marítimo y fluvial.
- Centro de Operaciones de Ciberseguridad especializado en el sector Transporte, subsector transporte por carretera.
- Soluciones innovadoras específicas para el ecosistema del Internet de las cosas[67] desplegado en el sector transporte.
- Soluciones innovadoras específicas para la protección de las señales de navegación transmitidas a los usuarios.
- Soluciones innovadoras específicas para barcos.
- Soluciones innovadoras para puertos.
- Soluciones innovadoras para aeropuertos.

[67] El transporte es el segundo sector más grande para los inversores en el IoT. Según un informe de Ponemon de 2018 sobre seguridad de DNS y riesgos de los ciberataques, se espera que se utilicen 125 000 millones de dispositivos IoT para 2030. (kaspersky Lab)

- Solución innovadora para el desarrollo de análisis forense y eventos jurídicos ante accidentes o/y reclamaciones judiciales, siempre y cuando esté relacionado con cuestiones de ciberseguridad.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
  - Registro de eventos y registros cifrados.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los

servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.

- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba con las siguientes características:
  - Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
  - Además, el entorno debe evidenciar una **convergencia IT/OT**[68], siempre que la solución propuesta aplique a ambos tipos de activos.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[68] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 21: SOC SECTOR FINANCIERO Y TRIBUTARIO

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[69].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector Financiero y Tributario o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR FINANCIERO y TRIBUTARIO O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

Aunque es cierto que el sector Financiero y Tributario está haciendo importantes esfuerzos para elevar el nivel de ciberseguridad, su fuerte digitalización le supone una alta dependencia de su tecnología. Este elevado nivel de dependencia aumenta el riesgo de ciberincidentes. No ayuda tampoco la complejidad del entorno tecnológico, donde conviven aplicaciones antiguas con otras

[69] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

que se apoyan en tecnologías más innovadoras. Esta complejidad supone un reto para las entidades a la hora de mantener un entorno de control adecuado y, por tanto, las hace más vulnerables.

El Informe Anual de Seguridad Nacional 2019, emitido por el Departamento de Seguridad Nacional, se indica que en España el 54% de los ciberataques contra infraestructuras críticas se dieron en el sector financiero y tributario.

Un ejemplo concreto de amenaza es el número creciente de ciberataques a **cajeros automáticos**[70] y servidores centrales.

Para combatir el aumento exponencial y de complejidad de las ciberamenazas y el fraude, el sector financiero y tributario necesita herramientas innovadoras de detección de fraude y conformidad normativa que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinados por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Financiero y Tributario, subsector **Entidades de Crédito**.
- Soluciones innovadoras específicas para **cajeros automáticos**[71].

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).

[70] Un ejemplo de ciberataque a cajeros automáticos es el 'jackpotting', donde los ciberdelincuentes aprovechan las vulnerabilidades físicas y/o de *software* del cajero para intentar obtener dinero en efectivo.

[71] Los cajeros automáticos tienen puntos débiles que se podrían aprovechar por ciberdelincuentes, además, el ecosistema de un cajero automático es complejo, ya que está compuesto por una combinación de *hardware* y *software*.

- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**: Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:
  - Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.

- Además, el entorno debe evidenciar una **convergencia IT/OT**[72], siempre que la solución propuesta aplique a ambos tipos de activos.
- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[72] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 22: SOC SECTOR SALUD / BIOTECNOLÓGICO

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[73].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector Salud o biotecnológico o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR SALUD O BIOTECNOLÓGICO O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

Ataques de ransomware, correos maliciosos, *software* con vulnerabilidades o fugas de información son algunas de las amenazas que pueden afectar al sector salud. Clínicas de todo tipo, especialistas sanitarios, personal de enfermería y obstetricia, laboratorios o farmacias son algunos ejemplos de empresas de este sector. El personal de estas empresas es muy variado pero tiene en común que,

[73] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

de una manera u otra, gestiona información muy sensible que según el RGPD y la LOPDGDD requiere medidas de protección especiales, siendo la privacidad y disponibilidad de esta información factores clave para su negocio.

Ya en el 2020, la Agencia de la UE para la Ciberseguridad recibió un total de 742 informes[74] sobre incidentes de ciberseguridad con un impacto significativo sobre los sectores estratégicos. En el caso del sector de la salud, hubo un aumento del 47% de estos incidentes en comparación con el año anterior.

Se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinados por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Salud, subsector Prestadores de asistencia sanitaria.
- Soluciones innovadoras específicas para la protección de robots utilizados en el sector salud. En este sector es muy frecuente encontrarnos a cirujanos asistidos por robots, de la misma forma, la probabilidad de que estos dispositivos puedan ser objetivo de un ciberataque crece también exponencialmente.
- Soluciones innovadoras específicas para dispositivos médicos. Las vulnerabilidades en dispositivos médicos empiezan a ser explotadas, surgen nuevos ataques para manipular por ejemplo bombas de insulina o marcapasos
- Soluciones innovadoras para mejorar la seguridad en sistemas informáticos que almacenan el historial del paciente o pruebas médicas, asegurando la información en reposo y en tránsito, para robustecer su control de acceso, trazabilidad de acceso, interoperabilidad con otros sistemas, exportación de la información, etc.
- Soluciones innovadoras específicas para la biotecnología.

[74] https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:
  - Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
  - Además, el entorno debe evidenciar una **convergencia IT/OT**[75], siempre que la solución propuesta aplique a ambos tipos de activos.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[75] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 23: SOC SECTOR AGUA

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[76].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector Aguas o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR AGUAS O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

La gestión automatizada y digitalizada del agua está exponiendo a este sector a nuevas amenazas, desde potenciales ataques para conseguir recursos digitales adicionales, el secuestro de datos, a amenazas de carácter terrorista con un bien, el agua, fundamental para el desarrollo de la sociedad. Todos los agentes han remarcado la importancia de este factor y en algunos casos han reportado

[76] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

actividades (no siempre compartibles al público) en este sentido. Se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista, o patrocinados por algún estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, es frecuente encontrar activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Aguas, subsector de suministro y distribución de agua potable.
- Soluciones innovadoras específicas para EDARES (estaciones depuradoras de aguas residuales).
- Soluciones innovadoras específicas para la medición inteligente (*smart metering*) del sector aguas.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIoT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:

- Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
- Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
- Detección y clasificación, lo más automatizada posible, de alertas.
- Correlación de eventos y/o alertas.
- Mecanismos innovadores de detección de falsos positivos.
- Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.

- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:
  - Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
  - Además, el entorno debe evidenciar una **convergencia IT/OT**[77], siempre que la solución propuesta aplique a ambos tipos de activos.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas

[77] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

a la exposición normal de la infraestructura monitorizada si se tratase de una solución con capa de monitorización.

- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 24: SOC TIC

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[78].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector Tecnologías de la Información y las Comunicaciones o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

La ley 8/2011 en su preámbulo, destaca como prioridades estratégicas diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia las

[78] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

infraestructuras que estén expuestas a amenazas, tanto en el plano de la seguridad física como en el de la **seguridad de las tecnologías de la información y las comunicaciones**.

Son las tecnologías de la información y las comunicaciones sobre las que descansan el resto de servicios esenciales. Se necesitan pues soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinados por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector de **Tecnologías de la Información y las Comunicaciones**, o cualquiera de sus subsectores.
- Soluciones innovadoras específicas para **puntos neutros**[79].
- Soluciones innovadoras específicas para Soluciones innovadoras específicas para **proveedores de servicios del DNS**.
- Soluciones innovadoras específicas para elevar la resiliencia[80] en Servidores DNS Raíz.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro

[79] Un punto neutro o punto de intercambio de Internet (en inglés IXP, Internet Exchange Point) es una infraestructura física a través de la cual los proveedores de servicios de Internet (PSI o ISP, por sus siglas en inglés) intercambian el tráfico de Internet entre sus redes. Esta instalación reduce la porción del tráfico de un PSI que debe ser entregado hacia su proveedor de conectividad, lo que reduce el costo promedio por bit de la entrega de su servicio. Además, el aumento del número de rutas "aprendidas" a través del punto neutro mejora la eficiencia de enrutamiento y la tolerancia a fallos.

[80] Identificación, análisis y desarrollo de una serie de tecnologías innovadoras que puedan ser incorporadas en el ecosistema de los servidores DNS que permitan el aumento de la seguridad, privacidad, disponibilidad, o resiliencia de estos. Otro ejemplo concreto sería el poder ofrecer capacidades de detección de campañas a partir del análisis del tráfico DNS de un DNS Root.

las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).

- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**: Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
- Además, el entorno debe evidenciar una **convergencia IT/OT**[81], siempre que la solución propuesta aplique a ambos tipos de activos.
- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[81] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 25: SOC SECTOR INDUSTRIA QUÍMICA

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[82].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector de la Industria Química o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR INDUSTRIA QUIMICA O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

Ataques de *ransomware*, correos maliciosos, *software* con vulnerabilidades o fugas de información son algunas de las amenazas que pueden afectar al sector de la industria química. Aunque este tipo de ataques son importantes, las asociaciones de industria química española están poniendo el foco de actuación en ciberataques que puedan poner en riesgo dos factores aún más importantes:

[82] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

- La integridad de su propiedad intelectual, debido a fugas, robos o espionaje industrial
- Los efectos de los ciberataques a seguridad de las personas y los bienes físicos ("safety").

Se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, y en particular a su foco de interés, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: Este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinada por algún Estado.
- **Dispersión geográfica**: Se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: Aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: La ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.
- **Recursos de interés**: La existencia de bienes de interés para los ciberdelincuentes es una razón fundamental para el aumento de la seguridad en este sector. La sustracción de formulaciones o compuestos químicos puede ser objeto de desestabilización de la organización y de la pérdida de confianza de inversores y de la sociedad.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Industria Químico, subsector Fabricación de productos químicos básicos, compuestos nitrogenados, fertilizantes, plásticos y caucho sintético en formas primarias.
- Centro de Operaciones de Ciberseguridad especializado en el sector Industrial Químico, subsector Fabricación de pesticidas y otros productos agroquímicos.
- Centro de Operaciones de Ciberseguridad especializado en el sector Industrial Químico, subsector Fabricación de pinturas, barnices y revestimientos similares; tintas de imprenta y masillas
- Centro de Operaciones de Ciberseguridad especializado en el sector Industrial Químico, subsector Fabricación de jabones, detergentes y otros artículos de limpieza y abrillantamiento; fabricación de perfumes y cosméticos
- Centro de Operaciones de Ciberseguridad especializado en el sector Industrial Químico, subsector Fabricación de otros productos químicos
- Centro de Operaciones de Ciberseguridad especializado en el sector Industrial Químico, subsector Fabricación de fibras artificiales y sintéticas
- Centro de Operaciones de Ciberseguridad especializado en el sector Fabricación de productos farmacéuticos y sus subsectores.

- Centro de Operaciones de Ciberseguridad especializado en el sector Fabricación de productos de caucho y plásticos y sus subsectores.
- Soluciones innovadoras específicas para la protección frente ataques que puedan afectar a la seguridad de las personas y los bienes físicos ("*safety*").

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los

servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.

- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:
  - Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
  - Además, el entorno debe evidenciar una **convergencia IT/OT**[83], siempre que la solución propuesta aplique a ambos tipos de activos.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[83] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 26: SOC SECTOR TURÍSTICO Y OCIO

MOTIVACIÓN

El sector del turismo y ocio, aunque no considerado como estratégico, es de gran relevancia en España puesto que se trata uno de los principales motores económicos [84](12,4 PIB en 2019 -154.487 millones de euros y 2,72 millones de puestos de trabajo-) , está inmerso en una transformación digital[85] para conseguir la presencia activa en la economía digital con iniciativas como los DTI o Destinos Turísticos Inteligentes[86], o el SIT o Sistema de Inteligencia Turística[87], incorporando para ello las tecnologías habilitadoras, entre ellas: 5G, *cloud*, *blockchain*, IoT, *Big Data*, IA (Inteligencia Artificial) o drones. La transformación digital viene acompañada de una redefinición de la cadena de valor asociada a los procesos de tradicionales, integrándose empresas, organizaciones, clientes, servicios, plataformas y tecnologías en modelos empresariales más complejos que forman los **ecosistemas digitales**[88].

Este sector está formado por un conglomerado de organismos, empresas, distribuidores e intermediarios con distintos niveles de dependencia tecnológica que pueden utilizar para crear estos DTI sistemas específicos de gestión de alojamientos y canales de venta online, *Big Data* e IA para marketing online, domótica, asistentes virtuales como soporte a la experiencia del viajero, IoT para control de afluencia, aparcamientos sensorizados o *beacons* para impulsar el turismo de compras. Por otra parte, está elaborándose la Estrategia de Turismo Sostenible de España 2030[89] que como los DTI[90] ha de basarse en las TIC para su desarrollo.

En este escenario, las tecnologías que dan soporte a las actividades del sector turístico pueden tener **características diferenciales** frente a otros sectores, entre otras:

- Arquitecturas y soluciones específicas a los servicios que prestan,
- Activos y datos específicos,
- Protocolos de comunicaciones,
- Dispersión geográfica o perímetro de exposición.

La transformación y, en general, el uso de las TIC en el sector no está exenta de riesgos. Muestra de ello es que se producen ataques dirigidos contra entidades representativas del sector como por ejemplo los dirigidos contra hoteles[91] bien para afectar a su actividad o para robar de tarjetas de

---

[84] https://www.segittur.es/sala-de-prensa/en-la-prensa/dataestur-la-mejor-fuente-de-datos-publicos-y-gratuitos-para-mejorar-negocios-turisticos/

[85] https://www.segittur.es/transformacion-digital/

[86] https://www.destinosinteligentes.es/que-es-dti/

[87] https://www.segittur.es/transformacion-digital/proyectos-transformacion-digital/sistema-de-inteligencia-turistica-2/

[88] Los ecosistemas digitales pueden definirse como redes de agentes conectados que, a partir de su interacción, crean productos y servicios combinados, generando valor recíproco y al mercado. ONTSI (2020), «Tecnologías habilitadoras digitales en España: impacto en los sectores agroalimentario, turístico y medioambiental» (pag.43) https://www.ontsi.es/index.php/es/publicaciones/Tecnologias-habilitadoras-digitales-en-Espana

[89] Estrategia de Turismo Sostenible de España 2030 https://turismo.gob.es/es-es/estrategia-turismo-sostenible/Paginas/Index.aspx

[90] Distintas UNE regulan los DTI, entre ellas la UNE 178501 Sistema de Gestión DTI incluye la tecnología (y dentro de ella la seguridad) como instrumento para dar soporte a la innovación, tanto para la gestión del DTI como en las relaciones con el consumidor y el usuario de servicios turísticos. https://www.aenor.com/certificacion/administracion-publica/destino-turistico-inteligente

[91] https://www.incibe-cert.es/search/site/hotel?f%5B0%5D=bundle%3Abitacora

crédito y datos personales. Además, la proliferación de este tipo de ataques dirigidos y su complejidad, hacen necesario reforzar la creación de soluciones de seguridad **innovadoras**[92].

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR TURISMO Y OCIO O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

Según diferentes análisis de inteligencia, las amenazas son cada vez más sofisticadas y numerosas por lo que se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten al sector, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinados por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda la cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en Destinos Turísticos Inteligentes.

[92] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

- Centro de Operaciones de Ciberseguridad especializado en sistemas domotizados en el ámbito del turismo.
- Centro de Operaciones de Ciberseguridad especializado en soluciones para el ecosistema digital del sector Turismo y Ocio o alguno de sus subsectores.
- Centro de Operaciones de Ciberseguridad especializado en la hostelería.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso del sector (drones, IoT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. routers) y sistemas de protección (ej. antivirus).
  - Análisis de tráfico de red y análisis de anomalías de todo el entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia del SOC.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (por ejemplo, activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliegue controlado del producto. Por ejemplo, aprovechando al

máximo los servicios que proporcionan los distintos proveedores *cloud*, siempre que tengan en cuenta la ciberseguridad.

- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características*:*

- El **entorno operativo** donde se espera recibir la demostración:
  - Ha de estar desplegado al menos en **una entidad** del sector, de cualquiera de su subsectores.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas del Centro de Operaciones a la exposición normal de la infraestructura monitorizada.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 27: SOC SECTOR ESPACIO

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[93].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector espacial o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR ESPACIO O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

La existencia de cada vez más activos expuestos a nivel espacial es una preocupación global, actualmente existen más de 9.300 objetos en órbita[94]. A este número de sistemas potencialmente

[93] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

[94] https://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id=#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23object.status.inOrbit_s1%22,%22value%22:%22Yes%22%7D%5D,%22sortings%22:%5B%7B%22fieldName%22:%22object.launch.dateOfLaunch_s1%22,%22dir%22:

peligrosos si sufrieran una desviación o una reentrada no controlada se suman los centros de control y sus comunicaciones.

La principal característica de este sector es que según el tratado espacial de la ONU, es que no existe una legislación global de obligatoria aplicación y por lo tanto no hay una obligación de tener medidas de ciberseguridad en estos sistemas, si bien hay países que aplican medidas legislativas a estos sectores de aplicación nacional y otros países donde no hay legislación específica aplican directivas[95] que si solicitan que "…se promuevan prácticas dentro de las operaciones espaciales gubernamentales y en toda la industria espacial comercial que protejan los activos espaciales y su infraestructura de apoyo y se defiendan contra las ciberamenazas."

Dado este escenario se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, y en particular a su foco de interés, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinada por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Industria Aeroespacial y sus subsectores.
- Soluciones innovadoras específicas para la protección de activos vinculados con el sector espacial en su ciclo de vida.
- Protección frente a ciberincidentes de sistemas espaciales y/u objetos orbitales, así como a sus comunicaciones asociadas, que incluye sistemas de comunicación y datos por satélite, sistemas de posicionamiento global, etc.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

%22desc%22%7D,%7B%22fieldName%22:%22en%23object.status.objectStatus_s1%22,%22dir%22:%22desc%22%7D%5D,%22match%22:null%7D

[95] https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
- Además, el entorno debe evidenciar una **convergencia IT/OT**[96], siempre que la solución propuesta aplique a ambos tipos de activos.
- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[96] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 28: SOC SECTOR ALIMENTACIÓN

MOTIVACIÓN

Las tecnologías que dan soporte a las actividades principales de cada uno de los sectores estratégicos o subsectores pueden tener **características específicas** diferenciales en cada uno de los sectores, como pudieran ser entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Muestra de ello es que se siguen reproduciendo tipos de ataques dirigidos específicamente a un sector. Además, la proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[97].

Es razonable deducir que las diferencias específicas diferenciales entre sectores podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en un determinado sector o subsector.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística del sector de la Alimentación o cualquiera de sus subsectores**, que tenga en cuenta las limitaciones de sus activos críticos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales del sector o subsector en el que se especializa.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR ALIMENTACIÓN O EN CUALQUIERA DE SUS SUBSECTORES.

Problema a resolver

Según un informe[98] de una consultora en 2019 un 77% de las empresas de alimentación y bebidas sufrieron ciberincidentes, esto unido a la necesidad de cubrir el flujo de trabajo de sus cadenas de

[97] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

[98] Hiscox Cyber Readiness Report 2019 - https://www.hiscox.es/estudios-de-ciberpreparacion

producción para evitar daños tanto a los consumidores como a la reputación de la propia empresa hace que el sector necesite un aumento de las capacidades en ciberseguridad.

El sector alimentación tiene unas necesidades muy específicas en lo que necesita en términos de ciberseguridad, y más con la integración de la industria 4.0 en un gran porcentaje de las organizaciones:

- Integración de medidas de securización que apoyen la transformación a la industria 4.0
- Los efectos de los ciberataques a la cadena de valor completa, desde los procesos de fabricación a los canales de distribución.

Se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, y en particular a su foco de interés, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: este sector está expuesto a ataques habituales de cualquier empresa además de otros de índole terrorista o patrocinada por algún Estado.
- **Dispersión geográfica**: se requiere muchas veces que los activos de este sector estén distribuidos geográficamente en puntos lejanos, lo que complica delimitar el perímetro de seguridad de estas organizaciones, y por consiguiente, garantizar su ciberseguridad.
- **Ausencia de estandarización**: aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: la ciberseguridad del sector depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector Industria de la alimentación y sus subsectores.
- Centro de Operaciones de Ciberseguridad especializado en el sector Fabricación de bebidas y sus subsectores.
- Centro de Operaciones de Ciberseguridad especializado en el sector Industria del tabaco y sus subsectores.
- Soluciones innovadoras específicas para la protección frente ataques que puedan afectar a la seguridad de los procesos de elaboración cadena alimentaria (Por ejemplo: Procesos de mantenimiento de frio industrial para productos perecederos).
- Centro de Operaciones de Ciberseguridad especializado en el sector Agricultura.
- Centro de Operaciones de Ciberseguridad especializado en el sector Ganadería.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- Ha de estar desplegado al menos en **una entidad** de este Sector, de cualquiera de su subsectores.
- Además, el entorno debe evidenciar una **convergencia IT/OT**[99], siempre que la solución propuesta aplique a ambos tipos de activos.
- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[99] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

RETO 29: SOC SECTOR INDUSTRIAL

MOTIVACIÓN

El sector industrial español es uno de los más destacables dentro del tejido empresarial español y el más longevo, el 30,3% de las empresas de este sector tiene 20 o más años[100].

Es por ello que la digitalización del sector es una necesidad obligada que hace que la aplicación de medidas de ciberseguridad sea un reto para este sector, si a esto se le añade que la especialización de cada uno de los procesos existente en cada una de las organizaciones que componen el sector tienen **características específicas** diferenciales que se pueden determinar entre otras en:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Tipología de protocolos de comunicaciones utilizados,
- Dispersión geográfica o perímetro de exposición.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística indicada en dicho reto**, que tenga en cuenta las limitaciones de sus activos y la complejidad de sus infraestructuras.

OBJETO

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales en el sector industrial español y que pueda tener aplicación específica en su tipo de actividad económica, sector y/o subsector asociado **sin entrar en conflicto** con otros retos presentados en esta propuesta vinculados a sectores definidos como estratégicos por el RD 8/2011[101].

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN EL SECTOR INDUSTRIAL.

Problema a resolver

Ataques de *ransomware*, correos maliciosos, *software* con vulnerabilidades o fugas de información son algunas de las amenazas que pueden afectar al sector industrial español. Aunque este tipo de ataques son importantes, las asociaciones de industria española están poniendo el foco de actuación en ciberataques que puedan poner en riesgo dos factores aún más importantes:

- La integridad de su propiedad intelectual, debido a fugas, robos o espionaje industrial
- Los efectos de los ciberataques a seguridad de las personas y los bienes físicos (“safety”).

[100] https://www.ine.es/prensa/dirce_2021.pdf

[101] https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

Se necesitan soluciones innovadoras que resuelvan el problema de identificar en tiempo real la detección proactiva de eventos de ciberseguridad que afecten a este sector, y en particular a su foco de interés, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivadas por lo siguiente:

- **Alto nivel de exposición a ataques variados**: Las pymes están expuestas a ataques habituales.
- **Ausencia de estandarización**: Aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: La ciberseguridad del sector pymes depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados en el sector, sino también a toda su cadena de valor.
- **Falta de aplicación de ciberseguridad**: el nivel de capacitación y madurez en temas de ciberseguridad del sector necesita aumentar.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en el sector industrial y sus subsectores, como por ejemplo:
  - industrias extractivas
  - industria manufacturera
  - industria textil
  - industria automoción
  - industria siderúrgica
  - industria mecánica
- Soluciones innovadoras de protección: Cualquier solución o servicio que las empresas de ciberseguridad pueda dar al sector y que por su naturaleza sea innovador.
- Soluciones innovadoras específicas para la protección frente ataques que puedan afectar a la seguridad de las personas y los bienes físicos (“*safety*”).

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas del sector.** La solución estaría personalizada a las necesidades específicas de sector. (Ej. Capacidades tecnológicas de reconocer y monitorizar protocolos industriales específicos del sector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección

de amenazas en entornos híbridos como es el caso de este sector (activos IT/OT, IoT, IIOT, etc.).

- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica en el sector, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.
- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

- Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características::
  - Ha de estar desplegado al menos en **una entidad** de este sector, de cualquiera de su subsectores.
  - Además, el entorno debe evidenciar una **convergencia IT/OT**[102], siempre que la solución propuesta aplique a ambos tipos de activos.

[102] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

- La solución debe evidenciar también su **carácter innovador**.

- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del sector sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **una entidad del Sector**, o de cualquiera de sus subsectores.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☒
Actuación 4. Soluciones tecnológicas a retos del sector público.	☒
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

RETO 30: SOC ESPECIALIZADO EN PYMES

MOTIVACIÓN

Son múltiples los informes que indican el escenario nacional en cuestión a empleo y como es su estratificación a nivel nación. El Directorio Central de Empresas (DIRCE), publicado por el Instituto Nacional de Estadística, registra, a 1 de enero de 2020, un total de 2.888.317[103] empresas activas en España. Siendo la mitad de estas, pequeñas empresas de entre 0 (Autónomos) y 49 empleados.

En términos de conectividad el INE indica que ya en 2019 el 81% del total de empresas en España utiliza dispositivos electrónicos para el trabajo diario, y el 77,6% disponen de conexión a internet[104].

Las tecnologías que dan soporte a las actividades principales de las pymes nacionales, así como las particularidades de este tipo de empresas, pueden tener **características específicas** diferenciales, que podrían ser base para la generación de un servicio especializado competitivo.

Al realizar un análisis pormenorizado de sus especificidades se puede determinar entre otras:

- Arquitecturas muy orientadas al tipo de servicio que prestan,
- Tipología de activos utilizados en dichas arquitecturas,
- Dispersión geográfica o perímetro de exposición.
- Baja disponibilidad de profesionales tic en su plantilla, u otro tipo de recursos.

Adicionalmente el informe Panorama actual de la Ciberseguridad en España (2019), realizado por Google, indica que las brechas de seguridad informática seguían en claro ascenso, siendo el 43% de los ciberataques dirigidos específicamente a pymes.

La proliferación de este tipo de ataques dirigidos y cada vez más complejos, hace necesario reforzar la creación o mejora constante de productos cada vez más **innovadores**[105].

Es razonable deducir que las diferencias específicas diferenciales entre pymes segmentadas por actividad comercial también podrían dar lugar a la aparición de soluciones o servicios especializados, que podrían ser muy competitivos a nivel mundial gracias a su especialización y ser los mejores en una determinada actividad comercial, sector y subsector asociado.

Son varias las instituciones e informes que apuestan por la creación de centros de operaciones de seguridad como son la Estrategia de Ciberseguridad de la CE para la Década Digital.

Por lo expuesto, se considera lo suficientemente motivado la creación o mejora de productos o soluciones que sean innovadores (servicio, *software*, *hardware* o material), **especialmente adaptados a la casuística indicada en dicho reto**, que tenga en cuenta las limitaciones de sus activos y la complejidad de sus infraestructuras.

OBJETO

[103] http://www.ipyme.org/Publicaciones/CifrasPYME-enero2020.pdf

[104] https://www.mineco.gob.es/stfls/mineco/ministerio/ficheros/libreria/ePyme2019.pdf

[105] La Norma UNE 166002:2006 establece una serie de requisitos que se consideran relevantes para ser incluidos en un proyecto de I+D+i. Define en concreto el concepto innovación como actividad cuyo resultado es la obtención de nuevos productos o procesos, o mejoras sustancialmente significativas de los ya existentes. Especifica en concreto cuatro categorías genéricas de productos (**servicio**, ***software***, ***hardware*** y **materiales**). Por lo anterior, se considera que la innovación de esta propuesta de reto podrá descansar sobre uno o varios de los anteriores elementos.

El objeto del reto es crear soluciones o servicios innovadores de ciberseguridad cuya ventaja competitiva esté basada en su adaptación a las características diferenciales de las pymes y que pueda tener aplicación específica en su tipo de actividad económica, sector y/o subsector asociado.

Se persigue que el producto o solución propuesta sea aplicable y desplegado no solo en organizaciones similares del mismo sector o subsector a nivel nacional, si no que pueda ser comercializado en otras organizaciones similares a nivel internacional.

Descripción del reto

CENTRO DE OPERACIONES DE CIBERSEGURIDAD ESPECIALIZADO EN LAS PYMES.

Problema a resolver

Como siguiente fase de protección del ciberdiagnóstico, se presenta este reto en el que trata de resolver las siguientes fases de protección de las pymes, resolviendo las carencias específicas e individualizadas de las pymes y autónomos en términos de ciberseguridad.

Este reto busca la creación de soluciones innovadoras que permitan al tejido mayoritario de empresas nacionales y a aquellas que les dan servicios de ciberseguridad, el aumento de su nivel de ciberseguridad en términos de detección, análisis y corrección de incidentes de ciberseguridad utilizando soluciones tecnológicas y enfoques innovadoras, y en particular a su foco de interés, antes de que se materialicen.

La complejidad y la necesidad de innovación vienen motivada por lo siguiente:

- **Alto nivel de exposición a ataques variados**: Las pymes están expuestas a ataques habituales.
- **Ausencia de estandarización**: Aunque existen avances, nos encontramos aún muchas veces con activos propietarios o *software* que no se han diseñado teniendo en cuenta la ciberseguridad, por lo que las soluciones, mientras se renueva el parque de activos, pasan por implementaciones de mitigación alternativas.
- **Visión global**: La ciberseguridad de las pymes depende de su eslabón más débil. Se echa en falta soluciones de monitorización que tengan en cuenta no solo toda la tipología de activos y protocolos específicos utilizados por las pymes, sino también a toda su cadena de valor.
- **Falta de aplicación de ciberseguridad**: el nivel de capacitación y madurez en temas de ciberseguridad de las pymes es irregular, habiendo organizaciones que tienen niveles de seguridad muy elevados pero en otros casos se detectan organizaciones con bajo o nulo nivel que pueden sufrir incidentes con consecuencias graves.

Ejemplos de caso de uso

Estos casos de uso se establecen como ejemplos, con el objeto de que los investigadores dispongan de potenciales problemas de investigación, no siendo exclusivos. Es decir, las propuestas no tendrán que basarse en estos ejemplos. Se podrán establecer otros casos de uso distintos u otros casos que complementen a los citados.

- Centro de Operaciones de Ciberseguridad especializado en pymes, pudiendo ser segmentados por actividad económica, sector y/o subsector.
- Sistemas innovadores para la detección perimetral de incidentes: sistemas que sean capaces, tecnológicamente, de mapear amenazas y que sean capaces de transmitir dicha información para ser estudiada.
- Tecnologías de bastionado innovadoras: sistemas para la ejecución autónoma y temporal de los bastionados en diferentes tipos de activos existentes en este tipo de organizaciones.

- Soluciones innovadoras de protección: cualquier solución o servicio que las empresas de ciberseguridad puedan dar a las pymes y que por su naturaleza sea innovador.

Funcionalidades

Se describen a continuación algunas funcionalidades de ejemplo.

- **Ciberseguridad** del entorno a desplegar y de sus comunicaciones. El producto o solución propuesta, ha de contar con los controles y tecnologías necesarias para no poner en peligro las dimensiones básicas de ciberseguridad del entorno a monitorizar (Confidencialidad, Integridad y Disponibilidad).
- **Capacidades específicas de la organización.** La solución estaría personalizada a las necesidades específicas del tipo de pyme a tratar, su actividad económica y en definitiva toda especificidad que pueda existir. (Ej. Capacidades tecnológicas de reconocer y monitorizar activos/protocolos específicos de una actividad comercial, sector y/o subsector).
- **Integración de tendencias o tecnologías innovadoras**. Por ejemplo, capacidades de Inteligencia Artificial o Aprendizaje Automático para el reconocimiento de activos o detección de amenazas en entornos híbridos como es el caso de esta actividad comercial, sector y/o subsector de aplicación (activos IT/OT, IoT, IIOT, etc.).
- **Monitorización continua y en tiempo real.** De forma ininterrumpida se contará con las tecnologías necesarias para:
  - Monitorización pasiva de eventos de ciberseguridad de todos los activos incluidos en el alcance, teniendo en cuenta posibles elementos de conectividad (ej. Routers) y sistemas de protección (Ej. Antivirus).
  - Análisis de tráfico de red y análisis de anomalías, no solo del proceso industrial, sino del resto del entorno a monitorizar.
  - Detección y clasificación, lo más automatizada posible, de alertas.
  - Correlación de eventos y/o alertas.
  - Mecanismos innovadores de detección de falsos positivos.
  - Investigación y modelado de amenazas, realizado conforme a las técnicas, tácticas y procedimientos (TTP) de referencia.
- **Enriquecimiento**. Posibilidad de enriquecer la información recogida con otras fuentes externas.
- **Gestión de incidentes**. Elaborando y poniendo en práctica aquellos procedimientos que se necesiten.
- **Métricas.** Ha de proporcionar mecanismos lo más automatizados posibles que sean capaces de medir objetivamente la eficiencia.
- **Cuadros de mando** que permitan tener una capa de explotación de la información como por ejemplo un mapa en tiempo real de las variables de interés, así como información accionable para facilitar la toma de decisiones.
- **Intercambio.** Posibilidad de exportación estandarizada y segura de eventos claves de incidentes.
- **Exposición.** Deberán de estar monitorizados aquellos activos cuya ciberseguridad sea más crítica dependiendo de su actividad comercial, sector y/o subsector de aplicación, incluyendo aquellos que estén conectados a redes consideradas más inseguras (Ej. Activos que necesitan estar expuestos a internet).
- **Escalabilidad**. Se desea que se evidencie la estabilidad del proyecto, de manera que permita garantizar un despliego controlado del producto. Ej. aprovechando al máximo los

servicios que te proporcionan los distintos proveedores Cloud, siempre que tengan en cuenta la ciberseguridad.

- **Simplificación.** Se desea que la solución propuesta sea lo más ágil de mantener de manera que se facilite la evolución del mismo.

ALCANCE

Para cumplir con los TRL indicados en este documento regulador se espera una prueba en entorno operativo con las siguientes características:

- El **entorno operativo** donde se espera recibir la demostración:
  - Ha de estar desplegado al menos en **al menos cuatro entidades** consideradas pymes específicas de la actividad comercial, sector y/o subsector objeto de la solución propuesta.
  - Además, el entorno debe evidenciar una **convergencia IT/OT**[106], siempre que la solución propuesta aplique a ambos tipos de activos.
  - La solución debe evidenciar también su **carácter innovador**.
- El **volumen de información** que se espera que sea el que determine el nivel de exposición de la infraestructura a monitorizar, debiendo de proporcionarse una solución bien dimensionada en este sentido. La **tipología de datos** que se espera probar son respuestas a la exposición normal de la infraestructura monitorizada, si se tratase de una solución con capa de monitorización.
- La **duración mínima** que se espera que la prueba de concepto esté funcionando es de un mínimo de 3 meses, pudiéndose valorar positivamente periodos más amplios.
- **Expectativas adicionales**. Se espera que la oferta presentada explique claramente:
  - Cuáles son los aspectos innovadores de su producto o solución.
  - **Cuáles son las características específicas** diferenciales del tipo de pyme ya sea por actividad comercial, sector y/o subsector de aplicación sobre las cuales va a construir su solución especializada.
- Listado de usuarios finales:
  - Al menos **cuatro entidades** consideradas pymes específicas de la actividad comercial, sector y/o subsector objeto de la solución propuesta.
- La **actuación o las actuaciones** en las que se ubica en principio el reto son:

Actuación 2. Soluciones tecnológicas para la ciberseguridad en las pymes.	☒
Actuación 3. Soluciones tecnológicas de ciberseguridad para sectores estratégicos.	☐
Actuación 4. Soluciones tecnológicas a retos del sector público.	☐
Actuación 5. Soluciones tecnológicas para la mejora de las infraestructuras y los equipamientos propios de INCIBE.	☐
Actuación 7. Pequeños proyectos altamente innovadores en ciberseguridad realizados por pymes o por emprendedores.	☒

[106] El alcance de los activos a monitorizar por el SOC debe contar con activos IT y OT. Se ha demostrado que un compromiso de ciberseguridad de una de las partes ha afectado a la otra.

ANEXO 2. DECLARACIÓN RESPONSABLE (SOBRE A)

INSTRUCCIONES PARA CUMPLIMENTAR EL DOCUMENTO EUROPEO ÚNICO DE CONTRATACIÓN (DEUC)

La presentación de la solicitud de participación implica la aceptación de las condiciones que regirán el procedimiento de adjudicación y las condiciones de ejecución del contrato contenidas en el documento regulador del presente procedimiento.

La presentación del DEUC por el licitador sirve como prueba preliminar del CUMPLIMIENTO de los REQUISITOS PREVIOS especificados en el presente documento para participar en este procedimiento de licitación.

El DEUC consiste en una declaración responsable de la situación financiera, las capacidades y la idoneidad de las empresas para participar en un procedimiento de contratación pública, de conformidad con el artículo 59 Directiva 2014/14, (Anexo 1.5) y el Reglamento de Ejecución de la Comisión (UE) 2016/7 de 5 de enero de 2016 que establece el formulario normalizado del mismo y las instrucciones para su cumplimentación.

El órgano de contratación procederá a la comprobación de las declaraciones responsables previamente presentadas requiriendo al efecto la presentación de los correspondientes justificantes documentales a los propuestos adjudicatarios salvo que necesite la información con anterioridad que será requerida al licitador.

En cualquier caso, la presentación del DEUC por el licitador conlleva el compromiso de que, en caso de que la propuesta de adjudicación del contrato recaiga a su favor, se aportarán los documentos justificativos a los que sustituye de conformidad con lo previsto en la cláusula 3.6 Fase V: Adjudicación definitiva.

2) Formulario normalizado DEUC

El formulario normalizado del DEUC se encuentra a disposición de los licitadores en las siguientes direcciones electrónicas: https://visor.registrodelicitadores.gob.es/espd-web/filter?lang=es

3) Instrucciones

Los requisitos que en el documento se declaran deben cumplirse, en todo caso, el último día de plazo de licitación y subsistir hasta la perfección del contrato, pudiendo INCIBE efectuar verificaciones en cualquier momento del procedimiento. La declaración debe estar firmada por quien tenga poder suficiente para ello.

En caso de que la solvencia o adscripción de medios exigidas se cumpla con medios externos al licitador, deberá presentarse un DEUC por el licitador y por cada uno de los medios externos.

Cuando el documento prevea la división en lotes del objeto del contrato y los requisitos de solvencia variaran de un lote a otro, se aportará un DEUC por cada lote o grupo de lotes al que se apliquen los mismos requisitos de solvencia.

Si varias empresas concurren constituyendo una unión temporal, cada una de las que la componen deberá acreditar su personalidad, capacidad y solvencia, presentando todas y cada una de ellas un formulario normalizado del DEUC. Además del formulario o formularios normalizados del DEUC y del compromiso de constitución de la UTE, en su caso, en el sobre A deberá incluirse la declaración de los licitadores de su pertenencia o no a un grupo empresarial, conforme a este anexo.

Las empresas que figuren inscritas en el Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público no estarán obligadas a facilitar aquellos datos que ya figuren inscritos de manera

actualizada, siempre y cuando se indique dicha circunstancia en el formulario normalizado del DEUC. En todo caso, es el licitador quien debe asegurarse de qué datos figuran efectivamente inscritos y actualizados y cuáles no. Cuando alguno de los datos o informaciones requeridos no conste en los Registros de Licitadores citados o no figure actualizado en los mismos, deberá aportarse mediante la cumplimentación del formulario.

Sobre la utilización del formulario normalizado DEUC los licitadores podrán consultar los siguientes documentos:

- Reglamento UE/2016/7 disponible en la página web: https://www.boe.es/doue/2016/003/L00016-00034.pdf
- Recomendación de la Junta Consultiva de Contratación Administrativa del Estado, de 6 abril de 2016, disponible en: http:www.minhap.gob.es/Documentacion/Publico/D.G.%20PATRIMONIO/Junta%20Consultiva/informes/Informes%202016/Recomendación%20de%20la%20JCCA%20sobre%20el%20aprobada%20el%206%20abril%20de%202016%20 3.pdf

Deberán cumplimentarse necesariamente los apartados (del Índice y Estructura del DEUC) que se encuentran marcados en este Anexo.

PARTE I: INFORMACIÓN SOBRE EL PROCEDIMIENTO DE CONTRATACIÓN Y EL PODER ADJUDICADOR (Identificación del contrato y la entidad contratante; estos datos deben ser facilitados o puestos por el poder adjudicador)

- Identidad del contratante:
    - Nombre oficial: Dirección General del Instituto Nacional de Ciberseguridad de España S.A. (INCIBE)
- Información sobre el procedimiento:
    - Tipo de procedimiento: Open procedure
    - Título: Documento Regulador de Compra Pública Precomercial: Servicios de I+D+i en materia de ciberseguridad (actuaciones 2, 3, 4, 5 y 7 de la consulta preliminar al mercado) MRR C15.I7
    - Número de referencia del expediente […]: CPP002/22

PARTE II: INFORMACIÓN SOBRE EL OPERADOR ECONÓMICO

Sección A: INFORMACIÓN SOBRE EL OPERADOR ECONÓMICO

- Identificación. Como n º de IVA se deberá indicar el NIF o CIF (ciudadanos o empresas españolas), el NIE (ciudadanos extranjeros residentes en España), y el VIES o DUNS (empresas extranjeras).
- Información general.
- Forma de participación.
    - Si se presenta en UTE responda afirmativamente a la pregunta: ¿Está participando el operador económico en el procedimiento de contratación junto con otros?

En este caso se desplegarán tres apartados que ha de completar con la siguiente información:

- Complete esta casilla indicando en cada caso: “Representante principal, XX % de participación” o “Miembro con XX % de participación”. Tenga en cuenta que el representante principal es quien presenta la oferta en la PCSP.
- Los nombres de los demás operadores económicos que forman la UTE.
- Nombre previsto o registrado de la UTE.

- Lote o lotes para los cuales el operador económico desea presentar oferta: se ha de indicar **solo un lote por DEUC** (cada lote se corresponde con un reto) con un **máximo de 3 lotes por licitador**. Cada uno de los operadores que vayan en UTE, tendrá que rellenar un DEUC por cada reto al que se presenten.

Sección B: INFORMACIÓN SOBRE LOS RERESENTANTES DEL OPERADOR ECONÓMICO

- Representación, en su caso (datos del representante)

Sección C: INFORMACIÓN SOBRE EL RECURSO A LA CAPACIDAD DE OTRAS ENTIDADES

- Recurso (Sí o No). Responda afirmativamente si para la capacidad (solvencias) cuenta con el aporte de otras empresas en UTE o de subcontratas.
- Sección D: INFORMACIÓN RELATIVA A LOS SUBCONTRATISTAS
- Subcontratación (Sí o No) y, en caso afirmativo, indicación de los subcontratistas conocidos)

PARTE III: MOTIVOS DE EXCLUSIÓN (en el servicio electrónico DEUC los campos de los apartados A, B y C de esta parte vienen por defecto con el valor 'No' y tienen la utilidad de que el operador pueda comprobar que no se encuentra en causa de prohibición de contratar o que, en caso de encontrarse en alguna, puede justificar la excepción)

- Sección A: MOTIVOS REFERIDOS A CONDENAS PENALES. Motivos referidos a condenas penales establecidos en el art. 57, apartado 1, de la Directiva
- Sección B: MOTIVOS REFERIDOS AL PAGO DE IMPUESTOS O DE COTIZACIONES A LA SEG. SOCIAL. Pago de impuestos o de cotizaciones a la Seguridad Social (declara cumplimiento de obligaciones)
- Sección C: MOTIVOS REFERIDOS A LA INSOLVENCIA, LOS CONFLICTOS DE INTERESES O LA FALTA PROFESIONAL.

  Información relativa a toda posible insolvencia, conflicto de intereses o falta profesional

- Sección D: OTROS MOTIVOS DE EXCLUSIÓN QUE ESTÉN PREVISTOS EN LA

LEGISLACIÓN NACIONAL. Motivos de exclusión puramente nacionales (si los hay, declaración al respecto).

PARTE IV: CRITERIOS DE SELECCIÓN

- El poder adjudicador exige la declaración de cumplimiento de los criterios específicamente (cumplimentar todas las secciones). Deben indicar sí a la pregunta ¿Quiere usar los criterios de selección de A a D?
- Sección A: IDONEIDAD: (información referida a la inscripción en el Registro Mercantil u oficial o disponibilidad de autorizaciones habilitantes).

- Sección B: SOLVENCIA ECONÓMICA Y FINANCIERA (datos a facilitar según las indicaciones del presente documento).
  - Se ha de completar por cada operador económico que contribuya a la capacidad (solvencia) el apartado de "Volumen de negocios anual general".
  - En "Otros requisitos económicos o financieros" se ha de incluir el compromiso de suscribir una póliza de seguro con un texto como el siguiente: "El licitador se compromete a obtener una Póliza de seguros que dé cobertura para todos los riesgos por un importe equivalente al 50% del valor económico del contrato."
  - No es necesario rellenar el apartado de "Volumen de negocios anual específico" ni "Volumen de negocio medio específico".
  - El patrimonio neto y capital social no es necesario cumplimentarlo en el DEUC si bien se confirma que se cumple con el requisito en caso de ser primer clasificado.
- Sección C: CAPACIDAD TÉCNICA Y PROFESIONAL (datos a facilitar según las indicaciones del presente documento).
  - Se ha de completar el apartado "Cuando se trate de contratos de servicios: Prestación de servicios del tipo especificado", indicando los proyectos que se aporten como solvencia técnica y profesional. Cada miembro de una UTE o subcontrata que aporte solvencia ha de incluir la parte que aporte en su propio DEUC.
  - En el apartado "Parte de subcontratación" en su caso se ha de completar el nombre de los subcontratistas, el porcentaje de participación y las actividades previstas que vayan a realizar según la memoria del proyecto. Tenga en cuenta que, si el operador económico ha decidido subcontratar una parte del contrato y cuenta con la capacidad del subcontratista para llevar a cabo esa parte, deberá cumplimentar un DEUC separado en relación con dicho subcontratista.
- Sección D: SISTEMAS DE ASEGURAMIENTO DE LA CALIDAD Y NORMAS DE GESTIÓN MEDIOAMBIENTAL. (No aplica a este documento)

PARTE V: REDUCCIÓN DEL NÚMERO DE CANDIDATOS CUALIFICADOS

PARTE VI: DECLARACIONES FINALES (declaración responsable de veracidad y disponibilidad de documentos acreditativos de la información facilitada, y acceso a la misma por el poder adjudicador)

NOTA.

- DEBERÁ PRESENTARSE UN DEUC DIFERENTE POR RETO O LOTE AL QUE SE LICITA.
- PARA CADA RETO AL QUE SE LICITA, DEBERÁ PRESENTARSE DEUC POR CADA UNO DE LAS ENTIDADES INTEGRANTES DE LA AGRUPACIÓN TEMPORAL Y DE LOS SUBCONTRATISTAS EN CUYA SOLVENCIA EL LICITADOR SE QUIERA BASAR. CADA DEUC IRÁ FIRMADO DIGITALMENTE POR LA ENTIDAD INTEGRANTE O SUBCONTRATISTA QUE HACE LA DECLARACIÓN.
- LOS SUBCONTRATISTAS EN CUYA CAPACIDAD SE BASA LA EMPRESA PARTICIPANTE DEBERÁN UTILIZAR EL DEUC (EN LO RELATIVO A LAS PARTES DE QUE SE TRATE). LOS DEMÁS SUBCONTRATISTAS NO TIENEN QUE CUMPLIMENTAR EL DEUC.

ANEXO 3. MODELO DE FICHA DE SUBCONTRATACIÓN (SOBRE A)

ACUERDO DE PARTICIPACIÓN EN LA EJECUCIÓN DE PROYECTOS DE I+D ENTRE [EMPRESA LICITADORA] Y [SUBCONTRATISTA]

Reto al que está asignado el contrato
Fecha

DATOS DEL LICITADOR U OFERENTE

Nombre: Apellidos: NIF:
Teléfono: Fax: Correo electrónico:
Dirección a efectos de práctica de notificaciones:
(en caso de actuar en representación)
Entidad mercantil a la que representa:
NIF: Cargo:

El presente documento es un acuerdo de participación en la ejecución del proyecto I+D en el marco de la Iniciativa Estratégica de Compra Pública de Innovación del S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) entre la empresa [EMPRESA LICITADORA], que encabeza una de las propuestas presentadas a la licitación realizada por INCIBE, y [SUBCONTRATISTA] que participa como subcontratado en dicha propuesta. El presente acuerdo solo entrará en vigor si la [EMPRESA LICITADORA] resulta adjudicataria de dicho contrato.

[SUBCONTRATISTA] declara que está informado y manifiesta su consentimiento con las disposiciones y requisitos que contiene el documento regulador de la licitación (especialmente las relacionadas con los derechos de propiedad intelectual e industrial), que cumple los requisitos de solvencia para la provisión de los servicios subcontratados y que pone sus recursos a disposición del licitador durante toda la duración de su contrato.

[SUBCONTRATISTA] declara que tiene la suficiente capacidad de obrar para ejecutar el contrato y que no se encuentra incurso en ninguna de las causas de prohibición de contratar del artículo 71 de la LCSP.

En _____, a _ de _____ de 2022,

Por [EMPRESA LICITADORA],

Fdo.: _____

Por [SUBCONTRATISTA],

Fdo.: _____

ANEXO 4. MODELO DE PRESUPUESTO DE PROYECTOS (SOBRE B)

Reto al que está asignado el contrato
Fecha
DATOS DEL LICITADOR U OFERENTE

Nombre: Apellidos: NIF:
Teléfono: Fax: Correo electrónico:
Dirección a efectos de práctica de notificaciones:
(en caso de actuar en representación)
Entidad mercantil a la que representa:
NIF: Cargo:

DECLARA:

Primero. - Que a todos los efectos debe de entenderse que, dentro de la presente propuesta, ha sido comprendido no sólo el precio de ejecución del objeto de contratación, sino asimismo la totalidad de gastos y compromisos que se definen en el documento regulador para el contratista, a excepción del Impuesto sobre el Valor Añadido, el cual será repercutido como partida independiente, indicando el tipo impositivo aplicado, en el documento que presente al cobro.

Segundo. -Que el desglose económico del presupuesto del proyecto propuesto es el siguiente:

- TÍTULO DE PROYECTO: [DESARROLLAR POR EL LICITADOR]
- ACRÓNIMO DE PROYECTO: [DESARROLLAR POR EL LICITADOR]
- PRESUPUESTO GLOBAL DEL PROYECTO: [DESARROLLAR POR EL LICITADOR]

Categoría de gasto (1)	Etapa (2)	Descripción	Actividad / Paquete de trabajo	Número de unidades	Precio unitario (3)	Importe Total	Justificación valor de mercado (4)	2023 (5)	2024	2025	2026
Gasto 1											
Gasto N											
TOTAL (6)	N/A						N/A				
TOTAL ETAPA 1											
TOTAL ETAPA 2											
TOTAL ETAPA 3											

Tabla 4: Desglose del presupuesto 1

(1) Deberá ser alguna de estas categorías:

- Personal propio.
- Personal de nueva contratación.
- Subcontratación.
- Activos tangibles aportados por el licitador (se aplicará un coeficiente de uso y tasa de amortización anual).
- Activos intangibles aportados por el licitador (se aplicará un coeficiente de uso y tasa de amortización anual).
- Nuevas inversiones en compra de activos (se aplicará un coeficiente de uso y tasa de amortización anual).
- Activos tangibles e intangibles que se obtendrán a la finalización de los proyectos en forma de prototipos o preseries y que se ofrece a INCIBE para su adquisición. **No podrán superar el 50% del valor del presupuesto pues esto implicaría que el contrato sea calificado como suministro de I+D y no como un servicio de I+D, lo que queda fuera del alcance de esta licitación**.
- Otros (especificar en el apartado de descripción).
- Costes indirectos (máximo 15% del coste de personal propio y de nueva contratación).

(2) Se debe indicar a qué etapa del proyecto corresponden estos gastos, teniendo en cuenta que el presupuesto máximo de la etapa 1 (Proyecto de Ingeniería de Detalle) es de 25.000 €+IVA. Las propuestas que no cumplan esta condición o no indiquen a que etapa del proyecto corresponden los gastos podrán subsanarlo a requerimiento del Órgano de Contratación y en última estancia, si la subsanación no es aceptada, excluidas.
(3) Todas las partidas deberán desglosarse en número de unidades y precio unitario, con excepción de las subcontrataciones. Los importes deberán expresarse en base imponible (es decir, excluyendo el IVA) y en €.
(4) Deberá justificarse por que el importe total es un valor de mercado, con detalles de cálculos que se podrán adjuntar o precios públicos de referencia, incluidas las subcontrataciones. INCIBE podrá solicitar ampliación de información sobre este aspecto en cualquier momento.
(5) Deberá desglosarse la previsión anual de gasto de cada partida, sin implicar esta declaración que los pagos por parte de INCIBE se adapten a dicho desglose, tal y como se indica en el documento regulador, en caso de ser seleccionado este proyecto.
(6) Suma total de gastos 1 a N.

Categoría de gasto (1)	Descripción	Actividad /Número de Paquete de trabajo	Precio unitario	Importe total	País ejecución gasto	% (2)
Gasto 1						
Gasto N						
TOTAL(3)	n/a	n/a	n/a	n/a		

Tabla 5: Desglose del presupuesto 2

(1) Deberán de coincidir con los gastos de la tabla anterior.
(2) Deberá indicarse su peso respecto al presupuesto total del proyecto.
(3) Deberá coincidir con el presupuesto total del proyecto, indicado en la tabla anterior.

El abajo firmante, en virtud de la representación que ostenta, se compromete, en nombre de su representado, a la ejecución del contrato en estos términos.

En _____, a _____, de _____, de 2022

ANEXO 5. MODELO DE COMPROMISO CON ENTIDAD USUARIA FINAL DE PROYECTO DE I+D (SOBRE B)

Reto al que está asignado el contrato
Fecha

DATOS DEL LICITADOR U OFERENTE

Nombre: Apellidos: NIF:
Teléfono: Fax: Correo electrónico:
Dirección a efectos de práctica de notificaciones:
(en caso de actuar en representación)
Entidad mercantil a la que representa:
NIF: Cargo:

El presente documento es un acuerdo de participación en la ejecución del Proyecto de I+D en el marco de la Iniciativa Estratégica de Compra Pública de Innovación del S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) entre la empresa [EMPRESA LICITADORA], que encabeza una de las propuestas presentadas a la licitación realizada por INCIBE, y [ENTIDAD USUARIA PÚBLICA O PRIVADA] que participa como entidad usuaria final en dicha propuesta aportada por el licitador. El presente acuerdo solo entraría en vigor si la [EMPRESA LICITADORA] resulta adjudicataria de dicho contrato.

[ENTIDAD USUARIA PÚBLICA O PRIVADA] declara que está informado y manifiesta su consentimiento con las disposiciones y requisitos que contiene el documento regulador de la licitación (especialmente las relacionadas con el apartado de ejecución del contrato y el apartado que regula los derechos de propiedad intelectual e industrial), y que cumple con los requisitos descritos en la definición de los usuarios finales de los proyectos de I+D aportados por las partes.

En _____, a _ de _____ de 2022,

Por [EMPRESA LICITADORA],

Fdo.: _____

Por [ENTIDAD USUARIA PÚBLICA O PRIVADA],

Fdo.: _____

ANEXO 6. PRESUPUESTO POR RETO

El presupuesto máximo para cada uno de los retos y aportación mínima y máxima de INCIBE para los contratos se desglosa en la siguiente tabla:

NOMBRE DEL RETO	Presupuesto máximo para cada **reto** (inversión máxima de INCIBE por reto)	Aportación mínima de INCIBE por **contrato** para cada reto (sin IVA)	Aportación máxima de INCIBE por **contrato** para cada reto (sin IVA)
Reto 01: Lucha contra los *insiders*	3.800.000 €	300.000,00 €	1.500.000,00 €
Reto 02: Criptografía avanzada resistentes a ataques cuánticos	3.800.000 €	300.000,00 €	1.500.000,00 €
Reto 03: Soluciones para la seguridad de datos y prevenir su uso malicioso	2.700.000 €	300.000,00 €	1.350.000,00 €
Reto 04: Sistemas innovadores para la evaluación, cumplimiento normativo y certificación	2.100.000 €	300.000,00 €	1.050.000,00 €
Reto 05: Gestión de identidades	2.700.000 €	300.000,00 €	1.350.000,00 €
Reto 06: Ciberresiliencia de cadena de suministro	3.800.000 €	300.000,00 €	1.500.000,00 €
Reto 07: Sistemas innovadores para el análisis de seguridad de dispositivos IoT	2.700.000 €	300.000,00 €	1.350.000,00 €
Reto 08: Sistemas para la protección frente a ataques contra el espectro electromagnético	2.100.000 €	300.000,00 €	1.050.000,00 €
Reto 09: Soluciones innovadoras en ciberseguridad para redes 5G	3.800.000 €	300.000,00 €	1.500.000,00 €
Reto 10: Ciberseguridad en el vehículo conectado	2.100.000 €	300.000,00 €	1.050.000,00 €
Reto 11: Ciberdiagnóstico automatizado para pymes y autónomos	5.000.000 €	300.000,00 €	1.500.000,00 €
Reto 12: Sistemas innovadores para el descubrimiento y análisis de servicios en internet	4.200.000 €	300.000,00 €	1.500.000,00 €
Reto 13: Investigación a partir de entornos simulados (señuelos)	4.200.000 €	300.000,00 €	1.500.000,00 €
Reto 14: Detección víctimas ciberdelitos	4.000.000 €	300.000,00 €	1.500.000,00 €

NOMBRE DEL RETO	Presupuesto máximo para cada **reto** (inversión máxima de INCIBE por reto)	Aportación mínima de INCIBE por **contrato** para cada reto (sin IVA)	Aportación máxima de INCIBE por **contrato** para cada reto (sin IVA)
Reto 15: Detección de víctimas de botnets a través de técnicas innovadoras	3.600.000 €	300.000,00 €	1.500.000,00 €
Reto 16: Sistemas para el seguimiento de cripto-transacciones	1.100.000 €	300.000,00 €	550.000,00 €
Reto 17: Sistema de detección de sms y mensajería instantánea fraudulentos y campañas asociadas	1.100.000 €	300.000,00 €	550.000,00 €
Reto 18: Atribución de ciberamenazas mediante técnicas innovadoras	4.000.000 €	300.000,00 €	1.500.000,00 €
Reto 19: SOC sector energía	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 20: SOC sector transporte	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 21: SOC sector financiero y tributario	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 22: SOC sector salud / biotecnológico	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 23: SOC sector agua	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 24: SOC TIC	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 25: SOC sector industria química	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 26: SOC sector turístico y ocio	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 27: SOC sector espacio	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 28: SOC sector alimentación	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 29: SOC sector industrial	6.700.000 €	300.000,00 €	1.500.000,00 €
Reto 30: SOC especializado en pymes	6.700.000 €	300.000,00 €	1.500.000,00 €
VALOR ESTIMADO TOTAL RETOS SIN IVA	137.200.000,00 €		
VALOR ESTIMADO TOTAL RETOS CON IVA	166.012.000,00 €		

Tabla 6: Presupuesto máximo para cada reto (inversión máxima de INCIBE por reto)

ANEXO 7. MODELO EVALUACIÓN AUTOMÁTICA (SOBRE C)

Reto al que está asignado el contrato:
Fecha

DATOS DEL LICITADOR U OFERENTE

Nombre: Apellidos: NIF:
Teléfono: Fax: Correo electrónico:
Dirección a efectos de práctica de notificaciones:
(en caso de actuar en representación)
Entidad mercantil a la que representa:
NIF: Cargo:

DECLARA:

Primero. - Que a todos los efectos debe de entenderse que, dentro de la presente propuesta, ha sido comprendido no sólo el precio de ejecución del objeto de contratación, sino asimismo la totalidad de gastos y compromisos que se definen en el documento regulador para el contratista.

Segundo. - Su propuesta respecto:

CRITERIO N.º 7: PORCENTAJE DE COINVERSIÓN + ROYALTIES

	Porcentaje Ofertado (%)
Porcentaje de coinversión: porcentaje del presupuesto del proyecto de I+D que es financiado directamente por el contratista.	%
Porcentaje de royalties: porcentaje calculado sobre la base del presupuesto del proyecto de I+D que el contratista desembolsará durante los 5 años posteriores a la finalización del proyecto, a INCIBE, en los términos establecidos en el apartado de Derechos de Propiedad Intelectual e Industrial, como pago de la licencia que INCIBE emitirá a su favor para la explotación de los resultados del proyecto de I+D. Durante cada uno de los 5 años posteriores el contratista desembolsará la quinta parte del porcentaje ofertado.	%

NOTA: Se deberá atender a los siguientes límites:

- El porcentaje de coinversión deberá ser como mínimo, mayor igual que el 4%.
- El porcentaje de *royalties* deberá ser como mínimo, mayor o igual que el 1%.
- En cualquier caso, si la propuesta ofrece valores inferiores a los mínimos, se asumirá que se está ofertando el valor mínimo.
- La suma de los dos porcentajes deberá ser como máximo de un 80%, de tal forma que en las propuestas que planteen un porcentaje superior, se asumirá que ofertan un 80%.

CRITERIO N. º 8: AUMENTO DEL PLAZO DE ROYALTIES

	Indicar si o no
Se oferta un año adicional de royalties a favor de INCIBE en las mismas condiciones ofertadas en el criterio nº 7 anualizado	
Se oferta dos años adicionales de royalties a favor de INCIBE en las mismas condiciones ofertadas en el criterio nº 7 anualizado	

El abajo firmante, en virtud de la representación que ostenta, se compromete, en nombre de su representado, a la ejecución del contrato de CPP002/22 en estos términos.

En _____, a _____, de _____, de 2022

ANEXO 8. MODELO DE DOCUMENTO DE PROPUESTA DE CAMBIOS (DPC) Y RESPUESTA (R-DPC)

SOLICITUD DE CAMBIO

Número de DPC	
Fecha de presentación	

1. Datos del solicitante

Entidad (es)	
Representante(s)	
Datos de contacto	

2. Identificación del cambio

Título del cambio	
Razón de la petición de cambio, resumen	
Descripción del cambio	
Urgencia	
Categoría del cambio (eliminar la opción que no proceda)	Complejidad baja / Complejidad media / Complejidad alta
Etapa del proyecto	

3. Detalle del cambio

Justificación del cambio	
Objetivo del cambio	
Riesgos del cambio	
Inicio previsto	dd/mm/aaaa
Finalización prevista	dd/mm/aaaa

1. Descripción de impacto[107]

CLASIFICACIÓN DEL IMPACTO (eliminar las opciones que no procedan)	1. Impacto sobre el alcance 2. Impacto técnico 3. Impacto económico-financiero 4. Impacto sobre la planificación 5. Impacto administrativo-legal 6. Impacto en el proceso de comunicación 7. Impacto sobre la subcontratación 8. Impacto sobre el empleo 9. Impacto de la actividad sobre el país de ejecución 10. Otros impactos
TIPO DE IMPACTO	Breve descripción
Alcance	Ejemplo: implica cambio de especificación
Técnico	
Económico-financiero	Ejemplo: implica actualización de costes
Compromisos	
Planificación	
Administrativo-legal	Ejemplo: modifica la propiedad
Comunicación	
Subcontratación	
Empleo	
Otros	

[107] Se deberán adjuntar las versiones anteriores y versiones nuevas de todos los documentos implicados en el contrato que van a ser modificados con motivo del DPC para incluirse en la NCC.

ANEXO 9. MODELO DE NOTA DE CAMBIOS EN EL CONTRATO (NCC)

NOTA DE CAMBIOS EN EL CONTRATO, NCC

Número de DPC (dado por el Adjudicatario)	
Número de NCC	
Número de versión	
Fecha de presentación de la NCC	

2. Datos de contacto

Empresa	
Representante(s)	
Datos de contacto	

Empresa	
Representante(s)	
Datos de contacto	

entidad (es)	
Representante(s)	
Datos de contacto	

3. Identificación del cambio aceptado

Título del cambio	
Solicitante del cambio	
Razón de la petición de cambio, resumen	
Descripción del cambio	
Urgencia	
Solución propuesta	
Categoría del cambio (eliminar la opción que no proceda)	Complejidad Simple / Complejidad Media / Complejidad alta
Etapa del proyecto	

4. Detalle del cambio aceptado

Justificación del cambio	
Objetivo del cambio	
Riesgos del cambio	
Inicio previsto	dd/mm/aaaa
Finalización prevista	dd/mm/aaaa

5. Descripción de impacto[108]

CLASIFICACIÓN DEL IMPACTO (eliminar las opciones que no procedan)	1. Impacto sobre el alcance 2. Impacto técnico 3. Impacto económico-financiero 4. Impacto sobre la planificación 5. Impacto administrativo-legal 6. Impacto en el proceso de comunicación 7. Impacto sobre la subcontratación 8. Impacto sobre el empleo

[108] Se deben adjuntar todos los documentos de origen, las modificaciones aceptadas en el NCC y los documentos que describen o son producto del impacto.

	9. Impacto de la actividad sobre el país de ejecución 10. Otros impactos
TIPO DE IMPACTO	Breve descripción
Alcance	Ejemplo: implica cambio de especificación
Técnico	
Económico-financiero	Ejemplo: implica actualización de costes
Compromisos	
Planificación	
Administrativo-legal	Ejemplo: modifica la propiedad
Comunicación	
Subcontratación	
Empleo	
Otros	

6. Firmas

AUTORIZADO EN NOMBRE DEL CONTRATISTA	
Firma	
Fecha	
AUTORIZADO EN NOMBRE DEL ADJUDICATARIO	
Firma	
Fecha	
AUTORIZADO EN NOMBRE DE LA ENTIDAD CONTRATANTE	
Firma	
Fecha	

ANEXO 10. TRL DE LA IECPI

Nº	TRL	Descripción del *hardware*	Descripción del *software*	Criterio de salida
1	PRINCIPIOS BÁSICOS OBSERVADOS Y REPORTADOS	Nivel inicial de la tecnología. La investigación científica comienza a traducirse en la investigación aplicada[109] y desarrollo (I + D). Se compone de estudios teóricos o análisis de las propiedades básicas y prestaciones de la tecnología.	Existe el conocimiento científico que fundamenta propiedades de la arquitectura de *software* y de la formulación matemática.	Han sido publicados en revistas científicas de prestigio los resultados de investigación que subyacen al concepto/aplicación propuesta.
2	CONCEPTO Y / O APLICACIÓN TECNOLOGÍA FORMULADO	Se inicia la invención, esto es la actividad de I+D propiamente dicha. Se diseñan aplicaciones concretas sobre la base de los principios básicos observados. Se trata de aplicaciones puramente especulativas, en las que no tiene que haber demostraciones o análisis detallados que las justifiquen. Se trata de estudios analíticos.	Se ha identificado la aplicación práctica, pero de forma especulativa; no existe prueba experimental o análisis detallado que apoyen la conjetura. Se han definido las propiedades básicas de algoritmos, las representaciones y los conceptos. Se han codificado los principios básicos. Se ha probado el resultado con datos simulados.	Descripción documentada de la aplicación / concepto aborda la viabilidad y las mejoras o beneficios.
3	FUNCIÓN CRÍTICA ANALIZADA Y PROBADA O PRUEBA DE CONCEPTO DEMOSTRADA EXPERIMENTALMENTE.	Se inicia la I+D efectiva. Incluye tanto los estudios analíticos para establecer la tecnología en un contexto apropiado como los ensayos de laboratorio para validar físicamente que las predicciones analíticas son correctas. Los diferentes componentes aún no están integrados o no son representativos. Estos estudios y experimentos de validación deben constituir una "prueba de concepto" de las aplicaciones / conceptos formulados en TRL 2.	Desarrollo de una funcionalidad limitada para validar las propiedades críticas y las predicciones mediante componentes de *software* no integrado.	Documentación de resultados analíticos o experimentales que las predicciones relativas a los parámetros clave.
4	VALIDACIÓN DE COMPONENTE O DISPOSICIÓN DE ESTOS, ESTO ES VALIDACIÓN DE TECNOLOGÍ	Los componentes tecnológicos básicos se integran para establecer cómo van a trabajar juntos con un rendimiento adecuado. La validación debe ser diseñada para soportar el concepto formulado en fases previas y, al mismo tiempo, ser	Los componentes de *software* clave, funcionalmente críticos se integran para establecer su interoperabilidad e iniciar el desarrollo de la arquitectura. Se definen los entornos relevantes y se estima el rendimiento en entorno.	Ensayo documentado del rendimiento demostrativo el cumplimiento de las predicciones analíticas. Definición

[109] **investigación aplicada**»: investigación industrial, desarrollo experimental, o cualquier combinación de ambos

Nº	TRL	Descripción del *hardware*	Descripción del *software*	Criterio de salida
	A, EN ENTORNO DE LABORATORIO	coherente con los requisitos de las aplicaciones potenciales del sistema. Se trata de prototipos representativos del sistema final, pero sin incorporar fielmente los elementos de diseño final. Puede incluir la integración de *hardware* "ad hoc" en el laboratorio.		documentada del entorno.
5	VALIDACIÓN DE COMPONENTE O DISPOSICIÓN DE ESTOS, ESTO ES VALIDACIÓN DE TECNOLOGÍA, EN UN ENTORNO REPRESENTATIVO	La aproximación del prototipo al sistema final se incrementa de forma significativa. Los componentes tecnológicos básicos se integran con elementos de soporte razonablemente realistas para ser examinados en un entorno simulado. Se trata de prototipos que integran componentes en sistemas de soporte similares a la realización final del sistema.	Se implementan los componentes de *software* de extremo a extremo y se interconectan con Sistemas o simulaciones existentes según el entorno. Se prueba el sistema de *software* completo, en entorno relevante, cumpliendo las expectativas previstas. Se establece el rendimiento operativo esperado. Se desarrollan los prototipos de implementación.	Documentación de ensayo que demuestre un rendimiento acorde Con las previsiones analíticas. Documentación de requisitos escalados.
6	MODELO DE SISTEMA O SUBSISTEMA O DEMOSTRACIÓN DE PROTOTIPO EN UN ENTORNO REPRESENTATIVO	Un modelo o prototipo de sistema representativo se prueba en un entorno relevante. Es un paso importante de evolución de TRL. Incluye el ensayo de un prototipo del sistema en un entorno de laboratorio representativo o en un entorno operativo simulado.	Implementaciones prototipo del *software* probadas y demostradas sobre problemas realistas a escala completa. Integrados con sistemas reales. Dispone de un nivel de documentación limitada. Se demuestra plenamente la viabilidad técnica.	Documentación de ensayo que demuestre un rendimiento acorde con las previsiones analíticas.
7	DEMOSTRACIÓN DE PROTOTIPO DEL SISTEMA EN UN ENTORNO OPERATIVO	Prototipo del sistema real funcionando en el entorno operativo real previsto. Exige la demostración de un prototipo real, fiel, del sistema en un entorno operativo.	Se construye un prototipo de *software* con todas las funcionalidades clave que disponible para demostración y prueba. Se debe producir una integración realista con los sistemas de HW/SW que permita demostrar la viabilidad operativa. Los principales errores de *software* se depuran. Se dispone de un nivel de documentación limitada.	Documentación de ensayo que demuestre un rendimiento acorde con las previsiones analíticas.
8	SISTEMA COMPLETO Y CERTIFICADO A TRAVÉS DE PRUEBAS Y DEMOSTRACIONES	La tecnología ha demostrado que funciona en su forma final, a nivel sistema y bajo las condiciones previstas. En general, este TRL representa el final del desarrollo del sistema. Debe incluir ensayos del sistema completo y	El *software* ha sido completamente depurado y totalmente integrado con los sistemas operacionales de *hardware* y *software*. Se completa la documentación de usuario, de formación y de mantenimiento. Todas las funcionalidades demostradas satisfactoriamente en escenarios	Documentación de ensayo que verifique las previsiones analíticas. Certificaciones. Documentación de productos, formación,

Nº	TRL	Descripción del *hardware*	Descripción del *software*	Criterio de salida
		evaluación del cumplimiento de las especificaciones de diseño. Puede incluir la integración de las nuevas tecnologías en un sistema existente.	operacionales simulados Verificación y Validación (V & V) completada.	mantenimiento, etc.
9	SISTEMA PROBADO CON ÉXITO EN ENTORNO REAL	Demostración de una misión completa del sistema en su forma definitiva y en condiciones reales. Uso del sistema en condiciones de misión operacionales.	El *software* ha sido completamente depurado y totalmente integrado con los sistemas operacionales de *hardware* y *software*. Toda la documentación se ha completado. La ingeniería de soporte de *software* está operativa. El sistema ha sido ejecutado con éxito en el entorno operativo real.	Resultados operativos de la misión probados documentalmente.

ANEXO 11. MEMORIA TÉCNICA (SOBRE B)

Las memorias técnicas han de entregarse siguiendo esta **distribución de contenido**:

Nombre del apartado	Subapartado	Contenido que se espera	Págs.[110]
1. DESCRIPCIÓN DEL PROYECTO DE I+D	1.1 Problema a resolver	Una descripción introductoria de cuál es el caso o casos de uso que se proponen para resolver la problemática o necesidad propuestas en el reto.	14
	1.2 Estado del arte	Descripción de los antecedentes y de que el estado actual de las aproximaciones científicas, tecnologías o soluciones existentes sea suficiente y correcto, referenciando las últimas investigaciones nacionales e internacionales que justifican la pertinencia de la actividad.	
	1.3 Funcionalidades	Listado de las funcionalidades más importantes de la Solución que pueden ser similares a las propuestas indicadas como ejemplo en el reto o pueden ser otras diferentes.	
	1.4 Inventario de tecnologías	Listado de una tabla a alto nivel del *software*, *hardware*, servicios o material que se va a utilizar como base en la Solución, describiendo brevemente para cada elemento: (1) nombre (2) tipo: SW/HW/servicio/material (3) para qué se utilizará en la Solución y (4) grado de importancia que tiene en el resultado final.	
	1.5 Mejoras técnicas innovadoras	Descripción de aquellas mejoras innovadoras que aportará la Solución propuesta para resolver el problema. Cada innovación propuesta, si se desea que se evalúe, deberá estar suficientemente detallada, explicando las ventajas y valor diferencial que aporta frente a las Soluciones disponibles en el mercado.	
	1.6 Resultado cedido[111] a INCIBE	Descripción de activos tangibles o intangibles que se obtengan como resultado del proyecto, cuya propiedad se cederá a INCIBE. Se explicará el valor que tendrá según el licitador, para INCIBE, esta cesión.	
	1.7 Plan de trabajo	Deberá de presentar un plan de trabajo que incluya (1) los medios materiales y perfiles anonimizados puestos a disposición de cada una de las 3 etapas, (2) reparto de funciones de cada perfil, (3) cronograma de tareas, (4) entregables, (5) indicadores de ejecución y (6) actividades que vayan a ser subcontratadas o realizadas en colaboración con otra entidad, entre otras cuestiones, de manera que sea posible una adecuada valoración del criterio.	
	1.8 Plan de riesgos	Deberá de describirse (1) la metodología de gestión de riesgos que se va a utilizar, (2) una identificación	

[110] Se indica el límite de folios a destinar a cada apartado de la propuesta. Cada folio cumplirá las siguientes características: DIN A4, a una cara, tipo de letra ARIAL, tamaño 11, márgenes superior e inferior a 2,5 cm y márgenes izquierdo y derecho a 3 cm, con interlineado sencillo en 1, exceptuando información gráfica (planos y esquemas, que podrán presentarse en formato A3). **Los folios que excedan del límite no serán objeto de evaluación**.

[111] En ningún caso el valor de estos activos podrá supera el 50% del presupuesto del proyecto pues esto implicaría cambiar la calificación del contrato de servicios a suministros de I+D, lo que queda fuera del alcance de esta licitación.

Nombre del apartado	Subapartado	Contenido que se espera	Págs. 110
		inicial de riesgos así como (3) las acciones preventivas y correctivas para solventar o minimizar su impacto en los resultados.	
2. IMPACTO SOCIO ECONÓMICO DEL PROYECTO	2.1 Impacto en la Unión Europea	Deberá describirse (1) qué método o referencias va a utilizar el licitador para indicar una estimación del impacto socio económico del proyecto en la Unión Europea a nivel cuantitativo, y a continuación, proporcionará los siguientes aspectos concretos: (2) generación estimada de empleo en profesionales dedicados a la ciberseguridad, (3) generación estimada de nuevo conocimiento en el ámbito de la ciberseguridad y (4) generación estimada de nueva actividad económica/creación de riqueza.	1
	2.2 Impacto en la *start-up*, pyme y organismos de investigación	Deberá describirse (1) qué actividades del proyecto van a desarrollar otras organizaciones, si es el caso, (*start-up*, pyme u organismos de investigación), (2) y en caso afirmativo, cómo se prevé el reparto de la propiedad y explotación de los resultados generados con dichas organizaciones, y (3) cómo considera el licitador que impactarán las dos cuestiones anteriores en dichas organizaciones.	1
3. PLAN DE VERIFICACIÓN EN ENTORNO OPERACIONAL	3.1 Plan de verificación	Deberá describirse, personalizado al TRL que se pretende alcanzar con la solución, (1) qué metodologías va a seguir para la verificación en entorno operacional del prototipo construido desde un punto de vista **funcional**, y **no funcional**[112] (seguridad, mantenibilidad, disponibilidad, rendimiento, interoperabilidad y usabilidad) y (2) el plan a llevar a cabo en el proyecto para cumplir con las metodologías que utilizará.	1
4. USUARIOS FINALES APORTADOS	4.1 Usuarios finales	Deberá describirse (1) el número de usuarios finales de los que se adjunta *ANEXO 5. Modelo de compromiso con entidad usuaria final de proyecto de I+D (sobre B)* completado correctamente y (2) el trabajo que va a desempeñar cada uno de estos usuarios en el proyecto respecto al cronograma que el licitador ha presentado en el Plan de trabajo.	Variable (1-3)[113]
5. PLAN DE TRANSFERENCIA DE RESULTADOS	5.1 Plan de transferencia al mercado	Deberá describirse una planificación de explotación de la solución una vez finalizado el proyecto dentro del alcance de la IECPI. El plan deberá de recoger (1) actuaciones propuestas, (2) medios humanos y materiales a utilizar, (3) porcentajes y alcance de la titularidad que corresponderá a cada parte de los derechos de propiedad nacidos bajo el ámbito del contrato, (4) previsiones de internacionalización de la solución, y (5) identificación de riesgos de explotación y tratamiento que se prevé hacer de los mismos.	2

Tabla 7: Estructuración del contenido de una memoria técnica

[112] Algunos ejemplos a tener en cuenta, dependiendo de cada proyecto: ISO/IEC 25030, requisitos de accesibilidad impuestos por el Real Decreto 1112/2018 de 7 de septiembre o certificado en seguridad por el CCN (Centro Criptológico Nacional)

[113] Si solo se aporta un usuario, el máximo de páginas será de una. Si se aportan más usuarios, el máximo de páginas será de tres.

INCIBE se reserva el derecho que ante una memoria técnica **entregada incorrectamente** o **no respetando esta propuesta de distribución** de contenido, pueda excluirla del proceso.
Los **criterios mínimos** que ha de respetar una memoria técnica son los siguientes:

- La estructura de índice propuesto en la tabla anterior.
- El número máximo de páginas a desarrollar por cada punto.
- El orden secuencial de los apartados a desarrollar, utilizando los nombres de apartados tal cual se expresan en la *Tabla 6: Estructuración del contenido de una memoria técnica*.
- El nombre del fichero a entregar, ha de respetar la siguiente sintaxis:

  IECPI_MemoriaTecnica_RetoNN_Nombre_Empresa.pdf

  Siendo:

  - RetoNN, el número del reto según se enumeran en el ANEXO 1. Retos
  - Nombre_Empresa, el nombre corto del licitador

  Ejemplo: IECPI_MemoriaTecnica_Reto01_INCIBE.pdf
- La memoria técnica deberá estar redactada de forma que pueda ser valorada, procurando la precisión y evitando la ambigüedad.
- Se requerirá un lenguaje claro, preciso, libre de vaguedades y términos ambiguos, coherente con la terminología empleada en los diferentes capítulos y con una mínima calidad literaria.
- La primera vez que se utilice un acrónimo o abreviatura en el texto se presentará, entre paréntesis, detrás de la palabra o texto completo al que en lo sucesivo reemplazará.
- El uso del tiempo futuro indicará requisitos obligatorios. Las sugerencias o propuestas no obligatorias se expresarán mediante la utilización del tiempo condicional o subjuntivo.

ANEXO 12: CRITERIOS EVALUABLES PARA EL SOBRE B

Los criterios sujetos a **juicio de valor** tendrán un peso total de **100 puntos** del conjunto de la oferta.

Para la valoración de los diferentes criterios sujetos a juicio de valor se debe tener en cuenta que 0 puntos corresponde a cumplir con los mínimos exigidos en el documento regulador. De igual modo y manera, aquellas descripciones en relación con criterios o subcriterios que sean imprecisas y/o no se hallen en relación con los propios objetos de valoración, en caso de que las mismas no impliquen incumplimientos de mínimos exigidos, serán igualmente valoradas con 0 puntos.

CRITERIO 1. DESCRIPCIÓN DEL PROYECTO DE I+D

Este criterio valorará el contenido descrito en el apartado "1. DESCRIPCIÓN DEL PROYECTO DE I+D" de la memoria técnica entregada en la oferta.

Puntuación: **de 0,00 a 55,00** puntos, que se valorará en base al siguiente baremo:

Puntuación	Explicación
De 0,00 a 3,00 puntos	Se puntuará **de 0,00 a 1,50 puntos**, si el contenido del subapartado "**1.1 Problema a resolver**" de la memoria técnica evidencia que el caso o casos de uso propuestos son parcialmente adecuados para resolver el problema identificado en el reto, o que son parcialmente vagos, inexactos o abstractos, o que no están completamente justificados. Se puntuará **de 1,50 a 3,00 puntos**, si el contenido del subapartado "**1.1 Problema a resolver**" de la memoria técnica evidencia que el caso o casos de uso propuestos son adecuados para resolver el problema identificado en el reto, son concretos, y además están justificados correctamente.
De 0,00 a 7,00 puntos	Se puntuará **de 0,00 a 3,00 puntos**, si el contenido del subapartado "**1.2 Estado del arte**" de la memoria técnica evidencia que los antecedentes y el estado actual del tema es **parcialmente** suficiente, no referencia correctamente las últimas investigaciones nacionales e internacionales que justifican la pertinencia de la propuesta o tampoco expresa ningún argumento ni estudio adicional que lo demuestre. Se puntuará **de 3,00 a 7,00 puntos**, si el contenido del subapartado "**1.2 Estado del arte**" de la memoria técnica evidencia que los antecedentes y el estado actual del tema sean **suficientes y correctos**, referenciando las últimas investigaciones nacionales e internacionales que justifican la pertinencia de la actividad.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 2,50 puntos**, si el contenido del subapartado "**1.3 Funcionalidades**" de la memoria técnica evidencia **parcialmente** la adecuación de la oferta al problema a resolver. Se puntuará **de 2,50 a 5,00 puntos**, si el contenido del subapartado "**1.3 Funcionalidades**" de la memoria técnica evidencia **totalmente** la adecuación de la oferta al problema a resolver.
	Se puntuará **0,00 puntos** si el contenido del subapartado "**1.4 Inventario de tecnologías**" de la memoria técnica evidencia un **uso nulo** [114]de tecnologías o

[114] **IMPORTANTE**: Si se puntúa como 0,00, se puede considerar que el servicio no es de i+d, por lo tanto, no procedería compra por esta vía.

Puntuación	Explicación
De 0,00 a 10,00 puntos	procesos innovadores que supongan una clara mejora frente a las soluciones habituales y el nivel de avance esperado de la tecnología.
	Se puntuará de **0,00** a **3,00** puntos si el contenido del subapartado "**1.4 Inventario de tecnologías**" de la memoria técnica evidencia un uso escaso de tecnologías o procesos innovadores que supongan una clara mejora frente a las soluciones habituales y el nivel de avance esperado de la tecnología.
	Se puntuará **de 3,00 a 6,00 puntos**, si el contenido del subapartado "**1.4 Inventario de tecnologías**" de la memoria técnica, evidencia un **uso moderado de algunas** tecnologías o procesos innovadores que supongan una clara mejora frente a las soluciones habituales y el nivel de avance esperado de la tecnología. Se considerarán con esta puntuación, por ejemplo, aquellas propuestas que aporten alguna tecnología habilitadora digital y su aportación sea relevante en algún sentido en la Solución.
	Se puntuará **de 6,00 a 10,00 puntos**, si el contenido del subapartado "**1.4 Inventario de tecnologías**" de la memoria técnica, evidencia un **uso alto de** tecnologías o procesos innovadores que supongan una clara mejora frente a las soluciones habituales y el nivel de avance esperado de la tecnología. Se considerarán con esta puntuación, por ejemplo, aquellas propuestas que aporten un importante uso cuantitativo o cualitativo de alguna tecnología habilitadora digital, o su aportación sea disruptiva en la Solución.
De 0,00 a 15,00 puntos	Se puntuará **0,00 puntos**, si el contenido del subapartado "**1.5 Mejoras técnicas innovadoras**" de la memoria técnica, evidencia un aporte innovador **nulo**[115]**.**
	Se puntuará **de 0,00 a 2,00 puntos**, si el contenido del subapartado "**1.5 Mejoras técnicas innovadoras**" de la memoria técnica, evidencia un aporte innovador que se considera **bajo.** Por ejemplo, cuando introduce técnicas ya existentes en el mercado, **adaptándolas** simplemente a la Solución propuesta. Se considerarán con esta puntuación aquellas Soluciones que ofrezcan mejoras innovadoras de carácter no tecnológico, como por ejemplo, mejoras innovadoras en las funcionalidades de la Solución o el diseño, entre otras.
	Se puntuará **de 2,00 a 7,00 puntos**, si el contenido del subapartado "**1.5 Mejoras técnicas innovadoras**" de la memoria técnica evidencia un aporte innovador que se considera **medio.** Por ejemplo, cuando introduce elementos innovadores a la Solución de **escaso alcance o proyección**. Se considerarán con esta puntuación aquellas Soluciones que ofrezcan mejoras innovadoras mediante tecnologías ya desarrolladas pero que aún no han sido implementadas en este caso en particular.
	Se puntuará **de 7,00 a 15,00 puntos**, si el contenido del subapartado "**1.5 Mejoras técnicas innovadoras**" de la memoria técnica evidencia un aporte innovador que se considera **alto.** Por ejemplo, cuando introduce elementos innovadores a la Solución de **gran alcance o proyección**.

[115] **IMPORTANTE**: Si se puntúa como 0,00, se puede considerar que el servicio no es de i+d, por lo tanto, no procedería compra por esta vía.

Puntuación	Explicación
	Se considerarán con esta puntuación aquellas Soluciones que ofrezcan mejoras innovadoras mediante tecnologías ya desarrolladas todas pero que aún no han sido implementadas en este caso en particular. Se considerarán con esta puntuación aquellas Soluciones que ofrezcan mejoras innovadoras y que requieran de la realización de actividades específicas de investigación industrial o desarrollo experimental[116] relevantes para alcanzar las funcionalidades propuestas. No se trata aquí pues de simplemente integrar tecnologías ya existentes, sino de desarrollar la tecnología necesaria para la mejora innovadora.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 1,50 puntos**, si el contenido del subapartado "**1.6 Resultado cedido a INCIBE**" de la memoria técnica, evidencia un aporte de valor que se considera **bajo.** Por ejemplo, se considerará bajo, si no se apreciara un encaje cuantitativo o cualitativo directo en la actividad encomendada a INCIBE.
	Se puntuará **de 1,50 a 3,00 puntos**, si el contenido del subapartado "**1.6 Resultado cedido a INCIBE**" de la memoria técnica, evidencia un aporte de valor que se considera **medio.** Por ejemplo, se considerará medio, si se apreciara un posible aporte cuantitativo o cualitativo de valor en alguna de las competencias encomendadas a INCIBE.
	Se puntuará **de 3,00 a 5,00 puntos**, si el contenido del subapartado "**1.6 Resultado cedido a INCIBE**" de la memoria técnica, evidencia un el aporte de valor que se considera **alto.** Por ejemplo, se considerará alto, si se aprecia un posible aporte cuantitativo o cualitativo de valor alto en las actividades estratégicas que INCIBE tiene encomendadas.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 1,50 puntos**, si el contenido del subapartado "**1.7 Plan de trabajo**" de la memoria técnica, tras analizar su coherencia, credibilidad del mismo en su conjunto y grado de concreción, se valora como **bajo.**
	Se puntuará **de 1,50 a 3,00 puntos**, si el contenido del subapartado "**1.7 Plan de trabajo**" de la memoria técnica, tras analizar su coherencia, credibilidad del mismo en su conjunto y grado de concreción, se valora como **medio.**
	Se puntuará **de 3,00 a 5,00 puntos**, si el contenido del subapartado "**1.7 Plan de trabajo**" de la memoria técnica, tras analizar su coherencia, credibilidad del mismo en su conjunto y grado de concreción, se valora como **alto.**
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 1,50 puntos**, si el contenido del subapartado "**1.8 Plan de riesgos**" de la memoria técnica, tras analizar la adecuación de la metodología propuesta al proyecto de I+D que se propone, el grado de conocimiento de los riesgos asociados a este tipo de proyectos y al problema a resolver así como el nivel

«**desarrollo experimental**»: la adquisición, combinación, configuración y empleo de conocimientos y técnicas ya existentes, de índole científica, tecnológica, empresarial o de otro tipo, con vistas a la elaboración de productos, procesos o servicios nuevos o mejorados; podrá incluir también, por ejemplo, actividades de definición conceptual, planificación y documentación de nuevos productos, procesos o servicios; el desarrollo experimental podrá comprender la creación de prototipos, la demostración, la elaboración de proyectos piloto, el ensayo y la validación de productos, procesos o servicios nuevos o mejorados, en entornos representativos de condiciones reales de funcionamiento, siempre que el objetivo principal sea aportar nuevas mejoras técnicas a productos, procesos o servicios que no estén sustancialmente asentados; podrá incluir el desarrollo de prototipos o proyectos piloto que puedan utilizarse comercialmente cuando sean necesariamente el producto comercial final y su fabricación resulte demasiado onerosa para su uso exclusivo con fines de demostración y validación; el desarrollo experimental no incluye las modificaciones habituales o periódicas efectuadas en productos, líneas de producción, procesos de fabricación, servicios existentes y otras operaciones en curso, aun cuando esas modificaciones puedan representar mejoras de los mismos;

Puntuación	Explicación
	de anticipación para establecer medidas correctoras, evidencia en su conjunto un **Plan de riesgos inicial trabajado parcialmente de forma correcta**.
	Se puntuará **de 1,50 a 3,00 puntos**, si el contenido del subapartado "**1.8 Plan de riesgos**" de la memoria técnica, tras analizar la adecuación de la metodología propuesta al proyecto de I+D que se propone, el grado de conocimiento de los riesgos asociados a este tipo de proyectos y al problema a resolver así como el nivel de anticipación para establecer medidas correctoras, evidencia en su conjunto un **Plan de riesgos trabajado de forma correcta**.
	Se puntuará **de 3,00 a 5,00 puntos**, si el contenido del subapartado "**1.8 Plan de riesgos**" de la memoria técnica, tras analizar la adecuación de la metodología propuesta al proyecto de I+D que se propone, el grado de conocimiento de los riesgos asociados a este tipo de proyectos y al problema a resolver así como el nivel de anticipación para establecer medidas correctoras, evidencia en su conjunto un **Plan de riesgos trabajado de forma excelente**.

CRITERIO 2. IMPACTO SOCIO ECONÓMICO DEL PROYECTO

Este criterio valorará el contenido descrito en el apartado "2. IMPACTO SOCIO ECONÓMICO DEL PROYECTO" de la memoria técnica entregada en la oferta.

Puntuación: **de 0,00 a 15,00** puntos, que se valorará en base al siguiente baremo:

De 0,00 a 10,00 puntos	Se puntuará **de 0,00 a 5,00 puntos**, si el contenido del subapartado "**2.1 Impacto en la Unión Europea**" de la memoria técnica: tras analizar el método utilizado para hacer la estimación, se concluye que es **parcialmente coherente**; y se evidencia que, tras valorar los datos estimados cuantitativamente, son **parcialmente realistas** o su impacto es sólo **en parte relevante** para la Unión Europea.
	Se puntuará **de 5,00 a 10,00 puntos**, si el contenido del subapartado "**2.1 Impacto en la Unión Europea**" de la memoria técnica: tras analizar el método utilizado para hacer la estimación, se concluye que es **suficientemente coherente**; y se evidencia que, tras valorar los datos estimados cuantitativamente, son **suficientemente realistas** y su impacto **es en gran medida relevante** para la Unión Europea.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 1,50 puntos**, si del análisis del contenido del subapartado "2**.2 Impacto en *start-ups*, pymes y organismos de investigación**" de la memoria técnica, se interpreta que la valoración estratégica e impacto sobre la ciberseguridad es **bajo**.
	Se puntuará **de 1,50 a 3,50 puntos**, si del análisis del contenido del subapartado "2**.2 Impacto en *start-ups*, pymes y organismos de investigación**" de la memoria técnica, se interpreta que la valoración estratégica e impacto sobre la ciberseguridad es **medio**.
	Se puntuará **de 3,50 a 5,00 puntos**, si del análisis del contenido del subapartado "2**.2 impacto en *start-ups*, pymes y organismos de investigación**" de la memoria técnica, se interpreta que la valoración estratégica e impacto sobre la ciberseguridad es **alto**.

CRITERIO 3. PLAN DE VERIFICACIÓN EN ENTORNO OPERACIONAL

Este criterio valorará el contenido descrito en el apartado "3. PLAN DE VERIFICACIÓN EN ENTORNO OPERACIONAL" entregado en la oferta.

Puntuación: **de 0,00 a 5,00** puntos, que se valorará en base al siguiente baremo:

De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 2,00 puntos**, si el contenido del subapartado "**3.1 Plan de verificación**" de la memoria técnica evidencia que las metodologías propuestas, y el plan propuesto para cumplir con ellas, son **parcialmente coherentes** con el proyecto.
	Se puntuará **de 2,00 a 5,00 puntos**, si el contenido del subapartado "**3.1 Plan de verificación**" de la memoria técnica evidencia que la metodología o metodologías propuestas, y el plan propuesto para cumplir con ellas, son **completamente coherentes** con el proyecto.

CRITERIO 4. PLAN DE TRANSFERENCIA DE RESULTADOS

Este criterio valorará el contenido descrito en el apartado "5. PLAN DE TRANSFERENCIA DE RESULTADOS" entregado en la oferta.

Puntuación: **de 0,00 a 5,00** puntos, que se valorará en base al siguiente baremo:

De 0,00 a 5,00 puntos	Se puntuará de **0,00 a 1,00** puntos, dependiendo del nivel de coherencia y credibilidad de las actuaciones propuestas en el subapartado **"5.1 Plan de transferencia al mercado".**
	Se puntuará de **0,00 a 1,00** puntos, dependiendo del nivel de suficiencia de los medios humanos y materiales propuestos en el subapartado **"5.1 Plan de transferencia al mercado".**
	Se puntuará de **0,00 a 1,00** puntos, dependiendo del nivel de coherencia y credibilidad de los porcentajes y alcance de la titularidad propuestas en el subapartado "**5.1 Plan de transferencia al mercado".**
	Se puntuará **de 0,00 a 1,00 puntos**, dependiendo del nivel de **coherencia, credibilidad y alcance** de las previsiones de internacionalización, propuestas en el subapartado "**5.1 Plan de transferencia al mercado**".
	Se puntuará **de 0,00 a 1,00 puntos**, dependiendo del nivel de **coherencia y credibilidad** de la identificación de riesgos y su tratamiento, propuesto en el subapartado "**5.1 Plan de transferencia al mercado**".

CRITERIO 5. PRESUPUESTO DEL PROYECTO

Este criterio valorará el contenido descrito en el ANEXO 4. MODELO DE PRESUPUESTO DE PROYECTOS (SOBRE B), entregado en la oferta.

Puntuación: **de 0,00 a 10,00** puntos, que se valorará en base al siguiente baremo:

De 0,00 a 10,00 puntos	Se puntuará **de 0,00 a 5,00 puntos**, si teniendo en cuenta el alcance del proyecto que describe la memora técnica, menos de la mitad de las partidas presupuestarias se adecuan correctamente a dicho alcance y los valores de mercado propuestos se estiman poco o parcialmente creíbles.

	Se puntuará **de 5,00 a 10,00 puntos**, si teniendo en cuenta el alcance del proyecto que describe la memora técnica, más de la mitad de todas las partidas presupuestarias se adecuan correctamente a dicho alcance y los valores de mercado propuestos se estiman creíbles.

CRITERIO 6. USUARIOS FINALES APORTADOS

Este criterio valorará el contenido descrito en el apartado "4. USUARIOS FINALES APORTADOS" entregado en la oferta.

Puntuación: **de 0,00 a 10,00** puntos, que se valorará en base al siguiente baremo:

De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 1,00 puntos**, si el contenido del subapartado "**4.1 Usuarios finales**" de la memoria técnica, evidencia una **pertinencia** y **relevancia** del usuario final, así como de **compromiso,** con un **nivel bajo**, teniendo en cuenta su implicación en las actividades relevantes descritas en el cronograma.
	Se puntuará **de 1,00 a 3,00 puntos**, si el contenido del subapartado "**4.1 Usuarios finales**" de la memoria técnica, evidencia una **pertinencia** y **relevancia** del usuario final, así como de **compromiso,** con un **nivel medio**, teniendo en cuenta su implicación en las actividades relevantes descritas en el cronograma.
	Se puntuará **de 3,00 a 5,00 puntos**, si el contenido del subapartado "**4.1 Usuarios finales**" de la memoria técnica, evidencia una **pertinencia** y **relevancia** del usuario final, así como de **compromiso,** con un **nivel alto**, teniendo en cuenta su implicación en las actividades relevantes descritas en el cronograma.
De 0,00 a 5,00 puntos	Se puntuará **1,00 puntos** por cada usuario final adicional al mínimo exigido y que esté correctamente justificado mediante el *ANEXO 5. MODELO DE COMPROMISO CON ENTIDAD USUARIA FINAL DE PROYECTO DE I+D (SOBRE B),* y **hasta un máximo de 5 puntos**.

ANEXO 13: CRITERIOS EVALUABLES PARA EL SOBRE C

Los criterios sujetos a **evaluación automática** tendrán un peso total de **100 puntos** del conjunto de la oferta.

Los criterios se establecen en los siguientes apartados:

CRITERIO 7. PORCENTAJE DE COINVERSIÓN Y *ROYALTIES*

Este criterio valorará el contenido descrito en el ANEXO 7. Modelo evaluación automática (sobre C).

Puntuación: **de 0,00 a 90,00** puntos, que se valorará en base al siguiente baremo:

Se valorará el mayor porcentaje del presupuesto, a valor de mercado de los proyectos, que se comprometerá el licitador a asumir, vía coinversión y *royalties* según las definiciones establecidas en el presente documento regulador.

- El porcentaje de coinversión deberá ser como mínimo, mayor o igual que el 4%.
- El porcentaje de *royalties* deberá ser como mínimo, mayor o igual que el 1%.
- En cualquiera de los dos casos, si la propuesta ofrece un valor inferior al mínimo, se asumirá que se está ofertando el valor mínimo.
- La suma de los dos porcentajes deberá ser como máximo de un 80%, de tal forma que en las ofertas que planteen un porcentaje superior se asumirá que ofertan un 80%.
- El reparto de los puntos del criterio se repartirá atendiendo a la siguiente fórmula:

  - Pcoinv (n) = ((Porcentaje coinv (n) + Porcentaje *royalties* (n)-5%) / 75)*90

Siendo:

- Pcoinv (n) la puntuación alcanzada en el criterio por la propuesta del licitador n.
- Porcentaje coinv (n) el porcentaje de coinversión ofertado en su propuesta.
- Porcentaje *royalties* (n) el porcentaje de royalties ofertado.

CRITERIO 8. AUMENTO DEL PLAZO DE ROYALTIES

Se valorará cada año adicional de *royalties* en las mismas condiciones ofertadas en el criterio nº 7 hasta un máximo de 2 años.

Puntuación: **de 0,00 a 10,00 puntos**, que se valorará en base al siguiente baremo:

Se puntuará **5,00 puntos por cada año adicional en las mismas condiciones** ofertadas en el criterio nº 7 anualizado, hasta **un máximo de 10,00 puntos**.

Ej. Proyecto 350.000 €.

Porcentaje de royalties ofertado: 2%.

Porcentaje de coinversión ofertado: 12%.

Criterio 7 coinversión: 350.000 €*12%= 42.000 €; 350.000€ - 42.000€ =308.000€ > 300.000€ inversión mínima que aportara INCIBE

Criterio 7 royalties: 350.000 €*2%= 7.000 € en cinco años

Criterio 8: Si se oferta un año adicional se ofertan 1.400 € en el año 6.

Criterio 8: Si se ofertan dos años adicionales se ofertan 1.400 € en el año 6 y 1.400 € en el año7.

ANEXO 14. CONTENIDO DEL PROYECTO DE INGENIERÍA

El proyecto de ingeniería ha de entregarse siguiendo esta **distribución de contenido**:

Nombre del apartado	Subapartado	Contenido que se espera	Págs.[117]
1. INTRODUCCIÓN DEL PROYECTO DE INGENIERÍA	1.1 Estructura del contenido del documento	Ha de ser una breve explicación del objetivo, contenido y estructura del documento constitutivo del proyecto de ingeniería.	6
	1.2 Objeto del proyecto de ingeniería	Se trata de una descripción breve del objetivo final del proyecto y de la finalidad que justifica su ejecución.	
	1.3 Bibliografía	En este apartado se debe contemplar una relación de aquellos estudios, libros, referencias relevantes en internet u otros textos que se considere de interés para justificar las soluciones o alcance adoptado en el proyecto de ingeniería.	
	1.4 Definiciones y abreviaturas	Persigue facilitar la comprensión del texto mediante la descripción de la terminología empleada. Se deberán relacionar en este apartado todas las definiciones, abreviaturas, etc. que se han utilizado a lo largo del contenido del proyecto de ingeniería y su significado.	
	1.5 Disposiciones legales y normas aplicables	Es imprescindible a la hora de abordar un proyecto de ingeniería en ciberseguridad tener bien identificado el conjunto de posibles disposiciones legales (leyes, reglamentos, ordenanzas, etc.) y las normas que son aplicables durante toda la vida del proyecto. Deberá incluirse pues una **relación de la legislación y demás normas**[118] que se han tenido en cuenta para: (1) el diseño del proyecto de ingeniería, (2) para llegar al TRL que se propone llegar y (3) para su puesta en producción o servicio (TRL9).	
2. ANTECEDENTES	2.1 Descripción de la situación actual	Dar una visión concisa y clara del TRL de partida del proyecto de ingeniería.	2
	2.2 Deficiencias identificadas	Se indicarán en este apartado la lista de las deficiencias en materia de ciberseguridad que tras la ejecución del proyecto de ingeniería quedarán superadas.	
	2.3 Estudio de viabilidad	Enumeración de posibles alternativas que se han tenido en cuenta a la hora de proponer este proyecto como solución del reto propuesto por INCIBE y justificación de la alternativa elegida y las razones por las que las otras han sido descartadas a la hora de presentar este proyecto de ingeniería.	
3. DESCRIPCIÓ	3.1 Requisitos de la Solución	La participación del usuario final en la Solución es clave, especialmente a la hora de identificar requisitos.	1

[117] Se indica el límite de folios a destinar a cada apartado de la propuesta. Cada folio cumplirá las siguientes características: DIN A4, a una cara, tipo de letra ARIAL, tamaño 11, márgenes superior e inferior a 2,5 cm y márgenes izquierdo y derecho a 3 cm, con interlineado sencillo en 1, exceptuando información gráfica (planos y esquemas, que podrán presentarse en formato A3). **Los folios que excedan del límite no serán objeto de evaluación**.

[118] Adquieren especial relevancia, si fuera el caso del sistema de información que es objeto el proyecto, la legislación relacionada con la protección de datos de carácter personal (LOPD, RDLOPD, LSSI, etc.). Se deberá tener en cuenta que la evolución de la legislación prevista en este sentido, es exigir la privacidad y seguridad desde el propio diseño del proyecto. Y así mismo la relacionada con la **ciberseguridad**, interoperabilidad y **accesibilidad** en proyectos de sistemas de información realizados para las AA.PP. (ENI, ENS, etc.). En el caso de que la Solución deba cumplir legislación sectorial, como sería el caso de sistemas industriales, sistemas financieros, etc. se hará referencia a la misma y su cumplimiento.

Nombre del apartado	Subapartado	Contenido que se espera	Págs.[117]
N DE LA SOLUCIÓN PROPUESTA		Se deberá en este apartado recoger una matriz que incluya: (1) requisito para la Solución, (2) usuario final que lo ha propuesto y (3) breve descripción del requisito.	
	3.2 Objetivos científicos de la solución	La Solución ha de responder a los requisitos de los usuarios finales, y los objetivos específicos han de alinearse con dichos requisitos. El contratista describirá aquí proponer los objetivos específicos, en base a los 5 puntos de la metodología SMART[119], tiene para la Solución, de manera que permitan juzgarla. Los objetivos han de estar agrupados por cada una de las 3 etapas del proyecto.	1
	3.3 Especificaciones funcionales	Los requerimientos funcionales son declaraciones de los servicios que proveerá la Solución. Ya no se trata de lo que hará la Solución, sino de "cómo" lo hará. También pueden declarar explícitamente lo que el sistema no debe hacer. Este apartado recogerá la matriz nombre de especificación funcional / Objetivo que trata / requerimiento que implementa.	5
	3.4 Especificaciones no funcionales	Son aquellos requerimientos que no se refieren directamente a las funciones específicas que se esperan de la Solución, sino a las propiedades emergentes de ésta como la fiabilidad, la respuesta en el tiempo, capacidad de almacenamiento, ciberseguridad, interoperabilidad, calidad del *software*, rendimiento, escalabilidad, mantenibilidad, entre otras.	
	3.5 Resultado cedido[120] a INCIBE	Descripción ya acotada de activos tangibles o intangibles que se obtengan como resultado del proyecto, cuya propiedad se cederá a INCIBE. Se explicará el valor que tendrá según el licitador, para INCIBE, esta cesión.	1
	3.6 Plan específico de validación de la etapa 2	Debido a la importancia de cambio de etapa 2 a 3, se deberá trabajar y presentar este plan específico que deberá contemplar, personalizado al TRL que se pretende alcanzar con la Solución en la etapa 2, (1) qué metodologías va a seguir para la verificación en entorno operacional del prototipo construido desde un punto de vista funcional, y no funcional (seguridad, mantenibilidad, disponibilidad, rendimiento, interoperabilidad y usabilidad), entre otras en esta etapa y (2) el plan de pruebas específico para llevar a cabo para validar esta etapa 2 del proyecto, de manera que cumpla con dichas metodologías y garantice el éxito del proyecto en este punto.	3
	3.7 Plan específico de validación de la etapa 3	Debido a la importancia de validación de la etapa 3, se deberá trabajar y presentar este plan específico que deberá contemplar, personalizado al TRL que se pretende alcanzar con la Solución en la etapa 3, (1) qué	3

[119] El método SMART define los objetivos de un proyecto conforme a cinco puntos para que este tenga éxito. Así pues, las metas deben ser **específicas**, **medibles**, **alcanzables**, **relevantes** y **estar sujetas a un plazo concreto**.

[120] En ningún caso el valor de estos activos podrá supera el 50% del presupuesto del proyecto pues esto implicaría cambiar la calificación del contrato de servicios a suministros de I+D, lo que queda fuera del alcance de esta licitación y del contrato que se formalice.

Nombre del apartado	Subapartado	Contenido que se espera	Págs.[117]
		metodologías va a seguir para la demostración en entorno operacional del prototipo construido desde un punto de vista funcional, y no funcional (seguridad, mantenibilidad, disponibilidad, rendimiento, interoperabilidad y usabilidad, entre otras) en esta etapa y (2) el plan de pruebas específico para llevar a cabo para validar esta etapa 3 del proyecto, de manera que cumpla con dichas metodologías y garantice el éxito del proyecto en este punto.	
	3.8 Plan específico de transferencia de resultados	Debido a la importancia de la transferencia de resultados al mercado, se deberá de entregar una planificación exhaustiva de explotación de la Solución una vez finalizado el proyecto dentro del alcance de la IECPI. El plan deberá de recoger (1) actuaciones propuestas, (2) medios humanos y materiales a utilizar, (3) porcentajes y alcance de la titularidad que corresponderá a cada parte de los derechos de propiedad nacidos bajo el ámbito del contrato, (5) previsiones de internacionalización de la Solución, y (6) identificación de riesgos de explotación y tratamiento que se prevé hacer de los mismos.	3
4. PLAN PARA LA DIRECCIÓN DEL PROYECTO[121]	4.1 Alcance del proyecto de ingeniería	Enumeración y contenido de todos los entregables del proyecto.	10
	4.2 Cronograma del proyecto de ingeniería	Cronograma explicitando las entregas parciales, hitos intermedios y duración del proyecto a partir de la fecha de iniciación del mismo, incluyendo la duración de las etapas 2 y 3 previstas	
	4.3 Presupuesto del proyecto de ingeniería	Explicitar coste total de la ejecución para la organización que ha de hacerse cargo de este proyecto. En este apartado debe tenerse especial cuidado en presentar las cifras de manera no ambigua, completa, sin costes ocultos y dando un total general, desglosado por partidas.	
	4.4 Planes de Gestión del proyecto	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	25
	4.5 Plan de gestión de la configuración del proyecto	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.6 Plan de gestión del cambio	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.7 Plan de gestión del alcance	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	

[121] Según el alcance y la complejidad del proyecto el objetivo de este anexo es describir la forma en la que se realizará la gestión del proyecto. El plan de dirección de proyecto se compone de: las líneas bases del proyecto (Alcance, cronograma y costes) más los 14 planes de gestión del proyecto. La realización de la documentación de este apartado se llevará a cabo siguiendo los estándares o normas internacionales: Guía del PMBOK®- Quinta Edición "PMI - Guía de los Fundamentos para la Dirección de Proyectos" (o su versiones más actualizadas) o UNE - ISO 21500:2013 "Directrices para la dirección y gestión de proyectos" (o su revisión más actual la ISO 21502:2020 "Gestión de proyectos, programas y carteras de proyectos. Contexto y conceptos").

Nombre del apartado	Subapartado	Contenido que se espera	Págs. 117
	4.8 Plan de gestión de los requisitos	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.9 Plan de gestión del cronograma	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.10 Plan de gestión de los costos	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.11 Plan de gestión de la calidad	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.12 Plan de mejoras del proceso	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.13 Plan de gestión de los recursos humanos	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.14 Plan de gestión del personal	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.15 Plan de gestión de las comunicaciones	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.16 Plan de gestión de los riesgos	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.17 Plan de gestión de las adquisiciones y contrataciones	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	
	4.18 Plan de gestión de los interesados	Se deberá de detallar este plan de gestión, personalizándolo al proyecto de ingeniería.	

Tabla 8: Estructuración del contenido de un proyecto de ingeniería

INCIBE se reserva el derecho que ante proyecto de ingeniería **entregado incorrectamente** o **no respetando esta propuesta de distribución** de contenido, pueda excluirlo del proceso.
Los **criterios mínimos** que ha de respetar son los siguientes:

- La estructura de índice propuesto en la tabla anterior.
- El número máximo de páginas a desarrollar por cada punto.
- El orden secuencial de los apartados a desarrollar, utilizando los nombres de apartados tal cual se expresan en la *Tabla 7: Estructuración del contenido de un proyecto de ingeniería.*
- El nombre del fichero a entregar, ha de respetar la siguiente sintaxis:
- IECPI_Proyecto_Ingenieria_RetoNN_Nombre_Empresa.pdf
- Siendo:
  - RetoNN, el número del reto según se enumeran en el ANEXO 1. Retos
  - Nombre_Empresa, el nombre corto del licitador

Ejemplo: IECPI_ Proyecto_Ingenieria_Reto01_INCIBE.pdf

- El proyecto deberá estar redactado de forma que pueda ser pueda ser valorado, procurando la precisión y evitando la ambigüedad.
- Se requerirá un lenguaje claro, preciso, libre de vaguedades y términos ambiguos, coherente con la terminología empleada en los diferentes capítulos y apartados de los diferentes documentos del proyecto y con una mínima calidad literaria.
- La primera vez que se utilice un acrónimo o abreviatura en el texto se presentará, entre paréntesis, detrás de la palabra o texto completo al que en lo sucesivo reemplazará.
- El uso del tiempo futuro indicará requisitos obligatorios. Las sugerencias o propuestas no obligatorias se expresarán mediante la utilización del tiempo condicional o subjuntivo.

ANEXO 15: CRITERIOS PARA EVALUAR EL PROYECTO DE INGENIERÍA

Los criterios para evaluar el proyecto de ingeniería tendrán un peso total de **100 puntos**.

La distribución de puntos se hace en base a los siguientes criterios:

CRITERIO 1. INTRODUCCIÓN DEL PROYECTO DE INGENIERÍA

Este criterio valorará el contenido descrito en el apartado "**1. Introducción del proyecto de ingeniería**" del proyecto de ingeniería.

Puntuación: **de 0,00 a 3,00** puntos, que se valorará en base al siguiente baremo:

Puntuación	Explicación
0,50 puntos	El contenido del subapartado "**1.1 Estructura del contenido del documento**" del proyecto de ingeniería permite hacerse a una idea clara del ámbito del documento y de la información que contiene. No se limita a ser un índice del contenido.
0,50 puntos	El contenido del subapartado "**1.2 Objeto del proyecto de ingeniería**" del proyecto de ingeniería describe de forma clara y precisa el objetivo del proyecto. Dicho objetivo es coherente con lo que se espera.
0,50 puntos	El contenido del subapartado "**1.3 Bibliografía**" y del proyecto de ingeniería hace una relación completa de referencias, y éstas son de relevancia para el objeto del proyecto de ingeniería.
0,50 puntos	El contenido del subapartado "**1.4 Definiciones y abreviaturas**" del proyecto de ingeniería es completo y ayuda a comprender el contenido del documento. No se ha observado ningún concepto que no sea auto-entendible o que no esté bien definido en este subapartado.
1,00 puntos	El contenido del subapartado **"1.5 Disposiciones legales y normas aplicables"** del proyecto de ingeniería es completo. No se echa en falta ninguna referencia relevante para para las etapas de diseño del proyecto, para llegar al TRL propuesto ni para su puesta en producción posterior, una vez entregado el proyecto.

CRITERIO 2. ANTECEDENTES

Este criterio valorará el contenido descrito en el apartado "**2. Antecedentes**" del proyecto de ingeniería.

Puntuación: **de 0,00 a 3,00** puntos, que se valorará en base al siguiente baremo:

Puntuación	Explicación
1,00 puntos	El contenido del subapartado "**2.1 Descripción de la situación actual**" del proyecto de ingeniería permite hacerse a una idea clara del TRL de partida, justificando correctamente por qué se considera ése y no otro como TRL de partida.
1,00 puntos	El contenido del subapartado "**2.2 Deficiencias identificadas**" del proyecto de ingeniería evidencia una correcta identificación de las principales deficiencias en materia de ciberseguridad que tras la ejecución del proyecto de ingeniería quedarán

Puntuación	Explicación
	superadas. Estas deficiencias se consideran realistas y relevantes teniendo en cuenta el alcance global del proyecto.
1,00 puntos	El contenido del subapartado "**2.3 Estudio de viabilidad**" del proyecto de ingeniería permite evidenciar que se ha llevado a cabo un estudio previo de viabilidad y este se ha realizado de forma correcta.

CRITERIO 3. DESCRIPCIÓN DE LA SOLUCIÓN

Este criterio valorará el contenido descrito en el apartado "**3. Descripción de la solución propuesta**" del proyecto de ingeniería.

Puntuación: **de 0,00 a 64,00** puntos, que se valorará en base al siguiente baremo:

Puntuación	Explicación
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 2,00 puntos**, si el contenido del subapartado "**3.1 Requisitos de la Solución**" del proyecto de ingeniería **evidencia parcialmente** que se ha contado con el usuario final a la hora de definir la Solución. Esta interpretación se hace en base al número de usuarios finales involucrados, número de requisitos, grado de concreción y realismo de su descripción.
	Se puntuará **de 2,00 a 5,00 puntos**, si el contenido del subapartado "**3.1 Requisitos de la Solución**" del proyecto de ingeniería **evidencia de forma completa** que se ha contado con el usuario final a la hora de definir la Solución. Esta interpretación se hace en base al número de usuarios finales involucrados, número de requisitos, grado de concreción y realismo de su descripción.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 2,00 puntos**, si el contenido del subapartado "**3.2 Objetivos científicos de la solución**" del proyecto de ingeniería **evidencia parcialmente** que el contratista los ha definido de manera que cumplen con las 5 características del método *SMART*[122]. **Los objetivos están agrupados por cada una de las tres etapas del proyecto.**
	Se puntuará **de 2,00 a 5,00 puntos**, si el contenido del subapartado "**3.2 Objetivos científicos de la solución**" del proyecto de ingeniería **evidencia de forma completa** que el contratista los ha definido de manera que cumplen con las 5 características del método *SMART*. **Los objetivos están agrupados por cada una de las tres etapas del proyecto.**
De 0,00 a 10,00 puntos	Se puntuará **de 0,00 a 5,00 puntos**, si el contenido del subapartado "**3.3 Especificaciones funcionales**" del proyecto de ingeniería es **parcialmente** completo, o parcialmente consistente respecto a los objetivos y requerimientos definidos previamente.
	Se puntuará **de 5,00 a 10,00 puntos**, si el contenido del subapartado "**3.3 Especificaciones funcionales**" del proyecto de ingeniería es **completo**, y **consistente** respecto a los objetivos y requerimientos definidos previamente.

[122] El método SMART define los objetivos de un proyecto conforme a cinco puntos para que este tenga éxito. Así pues, las metas deben ser **específicas**, **medibles**, **alcanzables**, **relevantes** y **estar sujetas a un plazo concreto**.

Puntuación	Explicación
De 0,00 a 10,00 puntos	Se puntuará **de 0,00 a 5,00 puntos**, si el contenido del subapartado "**3.4 Especificaciones no funcionales**" del proyecto de ingeniería es **parcialmente** completo, o **parcialmente** consistente respecto a las propiedades emergentes de la Solución que se esperarían contemplar (fiabilidad, la respuesta en el tiempo, capacidad de almacenamiento, ciberseguridad, interoperabilidad, calidad del *software*, rendimiento, escalabilidad, mantenibilidad, entre otras).
	Se puntuará **de 5,00 a 10,00 puntos**, si el contenido del subapartado "**3.4 Especificaciones no funcionales**" del proyecto de ingeniería es **completa**, y **consistente** respecto a las propiedades emergentes de la Solución que se esperarían contemplar (fiabilidad, la respuesta en el tiempo, capacidad de almacenamiento, ciberseguridad, interoperabilidad, calidad del *software*, rendimiento, escalabilidad, mantenibilidad, entre otras).
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 1,50 puntos**, si el contenido del subapartado "**3.5 Resultado cedido a INCIBE**" del proyecto de ingeniería, evidencia un aporte de valor que se considera **bajo.** Por ejemplo, cuando no se aprecia un encaje directo en las actividades encomendadas a INCIBE.
	Se puntuará **de 1,50 a 3,00 puntos**, si el contenido del subapartado "**3.5 Resultado cedido a INCIBE**" del proyecto de ingeniería, evidencia un aporte de valor que se considera **medio.** Por ejemplo, cuando se prevé el posible aporte de valor en algunas de las actividades encomendada a INCIBE.
	Se puntuará **de 3,00 a 5,00 puntos**, si el contenido del subapartado "**3.5 Resultado cedido a INCIBE**" del proyecto de ingeniería, evidencia un aporte de valor que se considera **alto.** Por ejemplo, cuando se prevé un posible aporte de alto valor en actividades estratégicas que INCIBE tiene encomendadas.
De 0,00 a 14,00 puntos	Se puntuará **de 0,00 a 3,00 puntos**, si el contenido del subapartado "**3.6 Plan específico de validación de la etapa 2**" del proyecto de ingeniería, evidencia un aporte de valor **parcialmente** completo. Por ejemplo, ha tenido **parcialmente en cuenta** las especificaciones funcionales o las no funcionales a la hora de proponer metodologías más adecuadas para su validación, el plan de pruebas descrito **no es completo** o se observa cualquier otro aspecto crítico que pueda poner en riesgo el proyecto al no haberlo contemplado en este punto.
	Se puntuará **de 3,00 a 7,00 puntos**, si el contenido del subapartado "**3.6 Plan específico de validación de la etapa 2**" del proyecto de ingeniería, evidencia un aporte de valor **completo**. Por ejemplo, ha tenido en cuenta de forma **correcta** las especificaciones funcionales o las no funcionales a la hora de proponer metodologías más adecuadas para su validación, el plan de pruebas descrito es **completo** y no se observa ningún aspecto crítico que pueda poner en riesgo el proyecto al no haberlo contemplado en este punto.
	Se puntuará **de 7,00 a 14,00 puntos**, si el contenido del subapartado "**3.6 Plan específico de validación de la etapa 2**" del proyecto de ingeniería, evidencia un aporte de valor **excelente**. Por ejemplo, ha tenido en cuenta de forma **sobresaliente** las especificaciones funcionales o las no funcionales a la hora de proponer metodologías más adecuadas para su validación, el plan de pruebas descrito **mejora las expectativas** y no se observa ningún aspecto crítico que pueda poner en riesgo el proyecto al no haberlo contemplado en este punto.
	Se puntuará **de 0,00 a 3,00 puntos**, si el contenido del subapartado "**3.7 Plan específico de validación de la etapa 3**" del proyecto de ingeniería, evidencia un aporte de valor **parcialmente completo.** Por ejemplo, ha tenido **parcialmente** en

Puntuación	Explicación
De 0,00 a 12,00 puntos	cuenta las especificaciones funcionales o las no funcionales a la hora de proponer metodologías más adecuadas para su validación, el plan de pruebas descrito no es completo, o se observa cualquier otro aspecto crítico que pueda poner en riesgo el proyecto al no haberlo contemplado en este punto.
	Se puntuará **de 3,00 a 7,00 puntos**, si el contenido del subapartado "**3.7 Plan específico de validación de la etapa 3**" del proyecto de ingeniería, evidencia un aporte de valor **completo.** Por ejemplo, ha tenido en cuenta de **forma correcta** las especificaciones funcionales o las no funcionales a la hora de proponer metodologías más adecuadas para su validación, el plan de pruebas descrito es **completo**, y no se observa ningún aspecto crítico que pueda poner en riesgo el proyecto al no haberlo contemplado en este punto.
	Se puntuará **de 7,00 a 14,00 puntos**, si el contenido del subapartado "**3.7 Plan específico de validación de la etapa 3**" del proyecto de ingeniería, evidencia un aporte de valor **excelente.** Por ejemplo, ha tenido en cuenta de **forma sobresaliente** las especificaciones funcionales o las no funcionales a la hora de proponer metodologías más adecuadas para su validación, el plan de pruebas descrito **mejora las expectativas**, y no se observa ningún aspecto crítico que pueda poner en riesgo el proyecto al no haberlo contemplado en este punto.
De 0,00 a 5,00 puntos	Se puntuará de 0,00 a 1,00 puntos, dependiendo del nivel de coherencia y credibilidad de las actuaciones propuestas en el subapartado "3.8 Plan específico de transferencia de resultados".
	Se puntuará de 0,00 a 1,00 puntos, dependiendo del nivel de suficiencia de los medios humanos y materiales propuestos en el subapartado "3.8 Plan específico de transferencia de resultados".
	Se puntuará de 0,00 a 1,00 puntos, dependiendo del nivel de coherencia y credibilidad de las porcentajes y alcance de la titularidad propuestas en el subapartado "3.8 Plan específico de transferencia de resultados".
	Se puntuará **de 0,00 a 1,00 puntos**, dependiendo del nivel de **coherencia, credibilidad y alcance** de las previsiones de internacionalización, propuestas en el subapartado "**3.8 Plan específico de transferencia de resultados**".
	Se puntuará **de 0,00 a 1,00 puntos**, dependiendo del nivel de **coherencia y credibilidad** de la identificación de riesgos y su tratamiento, propuesto en el subapartado "**3.8 Plan específico de transferencia de resultados**".

CRITERIO 4. PLAN PARA LA DIRECCIÓN DEL PROYECTO

Este criterio valorará el contenido descrito en el apartado "**4. Plan para la dirección del proyecto**" del proyecto de ingeniería.

Puntuación: **de 0,00 a 30,00** puntos, que se valorará en base al siguiente baremo:

Puntuación	Explicación
De 0,00 a 6,00 puntos	Se puntuará **de 0,00 a 2,00 puntos**, si el contenido del subapartado "**4.1 Alcance del proyecto de ingeniería**" del proyecto de ingeniería **evidencia parcialmente** su coherencia con los requisitos, objetivos y funcionalidades definidas para la Solución.

Puntuación	Explicación
	El número y contenido de los entregables propuestos justifica parcialmente el proyecto de ingeniería.
	Se puntuará **de 2,00 a 6,00 puntos**, si el contenido del subapartado "**4.1 Alcance del proyecto de ingeniería**" del proyecto de ingeniería **evidencia completamente** su coherencia con los requisitos, objetivos y funcionalidades definidas para la Solución. El número y contenido de los entregables propuestos justifica correctamente todo el proyecto de ingeniería.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 2,00 puntos**, si el contenido del subapartado "**4.2 Cronograma del proyecto de ingeniería**" del proyecto de ingeniería **evidencia parcialmente** su coherencia con los requisitos, objetivos y funcionalidades definidas para la Solución. La distribución de entregas parciales e hitos justifica parcialmente una correcta distribución de actividades.
	Se puntuará **de 2,00 a 5,00 puntos**, si el contenido del subapartado "**4.2 Cronograma del proyecto de ingeniería**" del proyecto de ingeniería **evidencia completamente** su coherencia con los requisitos, objetivos y funcionalidades definidas para la Solución. La distribución de entregas parciales e hitos justifica una correcta distribución de actividades.
De 0,00 a 5,00 puntos	Se puntuará **de 0,00 a 2,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**" del proyecto de ingeniería, hay alguna partida presupuestaria que se **adecua parcialmente**.
	Se puntuará **de 2,00 a 5,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**" del proyecto de ingeniería, todas las partidas presupuestarias se **adecuan correctamente**.
De 0,00 a 14,00 puntos	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de la configuración del proyecto ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia [123]cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión del cambio ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión del alcance ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de los requisitos ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo

[123] Son las guías de referencia que indica el apartado 4. PLAN PARA LA DIRECCIÓN DEL PROYECTO del ANEXO 14. Contenido del proyecto de ingeniería.

Puntuación	Explicación
	dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión del cronograma ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de los costos ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de la calidad ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de mejoras del proceso ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de los recursos humanos ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión del personal ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de las comunicaciones ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de los riesgos ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de las adquisiciones y contrataciones ha sido diseñado de forma **completa**, **realista**, con

Puntuación	Explicación
	concreción, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.
	Se puntuará con **1,00 puntos**, si teniendo en cuenta el contenido del subapartado "**4.3 Presupuesto del proyecto de ingeniería**", el Plan de gestión de los interesados ha sido diseñado de forma **completa**, **realista**, con **concreción**, **respetando** cómo dicen las guías de referencia cómo se ha de describir este proceso, y **está personalizado** al proyecto de ingeniería.

ANEXO 16: INFORME DE EVALUACIÓN (USUARIO FINAL - ETAPA 1)

Reto al que está asignado el contrato	
Fecha	

DATOS DELCONTRATISTA

Nombre:		Apellidos:		NIF:	
Teléfono:		Fax:		Correo electrónico:	
Dirección a efectos de práctica de notificaciones:					
(en caso de actuar en representación) Entidad mercantil a la que representa:					
NIF:		Cargo:			

El presente documento es un **informe de valoración de usuario final**, que se encuadra dentro de su participación en la ejecución de la **etapa 1**, de un Proyecto de I+D en el marco de la Iniciativa Estratégica de Compra Pública Innovadora del S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) entre la empresa [EMPRESA CONTRATISTA], que lidera una de las propuestas presentadas a la licitación realizada por INCIBE, y [ENTIDAD USUARIA PÚBLICA O PRIVADA].

Seleccionar / marcar por parte del usuario final **SOLO** aquellos enunciados en los que esté de acuerdo:

La empresa contratista ha contactado conmigo durante los trabajos de toma de requerimientos	☐
He propuesto algún requisito y éste ha sido tenido en consideración	☐
Las especificaciones funcionales del producto son de interés para mi organización	☐
Las especificaciones no funcionales del producto son de interés para mi organización	☐
Voy a participar activamente en el Plan específico de validación del entorno operacional	☐
La Solución, una vez finalizada, puede elevar sustancialmente el nivel de ciberseguridad de mi organización	☐
La Solución, una vez finalizada, cumple con los objetivos generales que espero yo para este tipo de proyectos	☐
Veo factible utilizar la Solución, una vez esté finalizada	☐
Recomendaría la Solución, una vez finalizada, a otras organizaciones similares	☐
La Solución, una vez finalizada, tiene potencial para poder ser comercializada en otros países de la UE	☐

En total, he considerado seleccionar ____ opciones. Como cada opción se valora con 10 puntos, mi valoración global del proyecto durante esta **etapa 1** es de _____ puntos[124].

[124] Por ejemplo, si el usuario ha seleccionado 6 opciones, los puntos finales serían el resultado de multiplicar 6 x 10, es decir 60 puntos. La puntuación final estará comprendida entre 0 y 100, en intervalos de 10 puntos.

Adicionalmente, como usuario final, me gustaría completar mi valoración con los siguientes comentarios:

Comentario 1: Mi participación durante la siguiente etapa se **estima** que se centrará en las siguientes actividades:

-
-
-
-
-
-

Comentario 2: Durante mi participación en la siguiente etapa se **estima** que aportaré los siguientes activos al proyecto (instalaciones, juegos de datos, entornos, simulaciones o activos específicos, tangibles o intangibles):

-
-
-
-
-
-

Comentario 3: Durante mi participación en la siguiente etapa éstas serían las **expectativas mínimas** que me gustaría que se cumpliesen:

-
-
-
-
-
-

En _____, a __, de _____, de 202_,

Por [EMPRESA CONTRATISTA],

Fdo.:

Por [ENTIDAD USUARIA PÚBLICA O PRIVADA],

Fdo.:

ANEXO 17: INFORME DE EVALUACIÓN (USUARIO FINAL - ETAPA 2)

Reto al que está asignado el contrato:
Fecha de la evaluación:

DATOS DEL CONTRATISTA

Nombre: Apellidos: NIF:
Teléfono: Fax: Correo electrónico:
Dirección a efectos de práctica de notificaciones:
(en caso de actuar en representación)
Entidad mercantil a la que representa:
NIF: Cargo:

El presente documento es un **informe de valoración de usuario final**, que se encuadra dentro de su participación en la ejecución de la **etapa 2**, de un Proyecto de I+D en el marco de la Iniciativa Estratégica de Compra Pública Innovadora del S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) entre la empresa [EMPRESA CONTRATISTA], que lidera una de las propuestas presentadas a la licitación realizada por INCIBE, y [ENTIDAD USUARIA PÚBLICA O PRIVADA].

Seleccionar / marcar por parte del usuario final **SOLO** aquellos enunciados en los que esté de acuerdo:

He participado activamente en las actividades previstas para esta etapa.	☐
La comunicación durante esta etapa con la empresa contratista ha sido fluida.	☐
Se están teniendo en cuenta los requisitos en cuya definición he participado.	☐
El prototipo previsto para esta etapa ha alcanzado el nivel de madurez previsto (TRL).	☐
He estado en la presentación del prototipo planificada para esta etapa y ha sido satisfactoria.	☐
La Solución, una vez finalizada, cumple con los objetivos parciales para esta etapa esperaba.	☐
Voy a participar activamente en la etapa 3.	☐
No observo un riesgo alto en esta etapa que impida cumplir los objetivos del proyecto.	☐
Veo factible utilizar la Solución, una vez finalizada.	☐
La Solución, una vez finalizada, tiene potencial para poder ser comercializada en otros países de la UE	☐

En total, he considerado seleccionar ____ opciones. Como cada opción se valora con 10 puntos, mi valoración global del proyecto durante esta **etapa 2** es de _____ puntos[125].

[125] Por ejemplo, si el usuario ha seleccionado 6 opciones, los puntos finales serían el resultado de multiplicar 6 x 12,5, es decir 75 puntos. La puntuación final estará comprendida entre 0 y 100, en intervalos de 12,5 puntos.

Adicionalmente, como usuario final, me gustaría completar mi valoración con los siguientes comentarios:

Comentario 1: Mi participación durante esta etapa, se ha centrado principalmente en las siguientes actividades:

-
-
-
-

Comentario 2: Mi participación durante la siguiente etapa se **estima** que se centrará en las siguientes actividades:

-
-
-
-

Comentario 3: Durante mi participación en la siguiente etapa se **estima** que aportaré los siguientes activos al proyecto (instalaciones, entornos, simulaciones o activos específicos, tangibles o intangibles):

-
-
-
-

Comentario 4: Durante mi participación en la siguiente etapa éstas serían las **expectativas mínimas** que me gustaría que se cumpliesen:

-
-
-
-

En _____, a __, de _____, de 202_,

Por [EMPRESA CONTRATISTA],

Fdo.:

Por [ENTIDAD USUARIA PÚBLICA O PRIVADA],

Fdo.:

ANEXO 18: INFORME DE EVALUACIÓN (USUARIO FINAL - ETAPA 3)

Reto al que está asignado el contrato:
Fecha de la evaluación:

DATOS DELCONTRATISTA

Nombre: Apellidos: NIF:
Teléfono: Fax: Correo electrónico:
Dirección a efectos de práctica de notificaciones:
(en caso de actuar en representación)
Entidad mercantil a la que representa:
NIF: Cargo:

El presente documento es un **informe de valoración de usuario final**, que se encuadra dentro de su participación en la ejecución de la **etapa 3**, de un Proyecto de I+D en el marco de la Iniciativa Estratégica de Compra Pública Innovadora del S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) entre la empresa [EMPRESA CONTRATISTA], que lidera una de las propuestas presentadas a la licitación realizada por INCIBE, y [ENTIDAD USUARIA PÚBLICA O PRIVADA].

Seleccionar / marcar por parte del usuario final **SOLO** aquellos enunciados en los que esté de acuerdo:

He participado activamente en las actividades previstas para esta etapa.	☐
La comunicación durante esta etapa con la empresa licitadora ha sido fluida.	☐
Se están teniendo en cuenta los requisitos en cuya definición he participado.	☐
El prototipo previsto para esta etapa ha alcanzado el nivel de madurez previsto (TRL)	☐
He estado en la presentación del prototipo planificada para esta etapa y ha sido satisfactoria.	☐
La Solución, una vez finalizada, cumple con los objetivos generales que espero yo para este tipo de proyectos.	☐
Veo factible utilizar la Solución, una vez finalizada.	☐
Veo factible recomendar la Solución, una vez finalizada, a otras organizaciones similares.	☐
La Solución, una vez finalizada, tiene potencial para poder ser comercializada en otros países de la UE.	☐
Estoy satisfecho, en líneas generales, con el trabajo realizado por la empresa licitadora.	☐

En total, he considerado seleccionar ____ opciones. Como cada opción se valora con 10 puntos, mi valoración global del proyecto durante esta **etapa 3** es de _____ puntos[126].

[126] Por ejemplo, si el usuario ha seleccionado 6 opciones, los puntos finales serían el resultado de multiplicar 6 x 10, es decir 60 puntos. La puntuación final estará comprendida entre 0 y 100, en intervalos de 10 puntos.

Adicionalmente, como usuario final, me gustaría completar mi valoración con los siguientes comentarios:

Comentario 1: Mi participación durante esta etapa se ha centrado principalmente en las siguientes actividades:

-
-
-
-

Comentario 2: Durante mi participación en esta etapa he aportado finalmente los siguientes activos al proyecto (instalaciones, entornos, simulaciones o activos específicos, tangibles o intangibles):

-
-
-
-

Comentario 3: Mi opinión sobre los trabajos realizados por la empresa licitadora es la siguiente:

-
-
-
-

Comentario 4: Mi opinión sobre la Solución entregada es la siguiente:

-
-
-
-

En _____, a __, de _____, de 202_,

Por [EMPRESA CONTRATISTA],	Por [ENTIDAD USUARIA PÚBLICA O PRIVADA],
Fdo.:	Fdo.:

ANEXO 19: MODELO DE CONTRATO

CONTRATO

EXP. CPP002/22

RETO __Nº_____ (MRR C15.I7)

NOMBRE PROYECTO _____

En la fecha que consta pie de firma.

REUNIDOS

De una parte, D. Félix Barrio Juárez, mayor de edad, en su calidad de Director General de **S.M.E INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A.** (en adelante, "INCIBE"), con domicilio en 24005-León, Edificio INCIBE, Avda. José Aguado, 41 y C.I.F. A-24530735, facultado para este acto conforme consta en los acuerdos del acta del Consejo de Administración de la Sociedad de _____.

D. FÉLIX ANTONIO BARRIO JUÁREZ declara ausencia de conflicto de intereses (DACI), manifestando que no se encuentra incurso en ninguna situación que pueda calificarse de conflicto de intereses o de causa de abstención, y se compromete a poner en conocimiento, sin dilación, cualquier situación de conflicto de intereses o causa de abstención que dé o pudiera dar lugar a dicho escenario, y que es conocedora de las consecuencias que pudieran derivarse de la falsedad de una declaración de ausencia de conflicto de intereses.

De otra parte, _____ con DNI _____ en nombre y representación de _____con CIF _____ y domicilio en calle _____, según escritura de elevación a público de acuerdos sociales otorgada ante el notario _____, con fecha _____, bajo el número de protocolo _____.

INCIBE y _____ (en adelante, podrán ser denominadas, individualmente, "la Parte" y, conjuntamente, "las Partes"), reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente contrato.

EXPONEN

I. Que INCIBE ha incoado el correspondiente procedimiento abierto Servicios de I+D en materia de ciberseguridad (actuaciones 2, 3, 4, 5 y 7) con 30 retos. El contrato tiene financiación europea con cargo al Mecanismo para la Recuperación y Resiliencia (MRR).

II. Que INCIBE el _____ acordó la adjudicación del Contrato CPP002/22 Reto nº _ Nombre del proyecto _____(en adelante, "el Contrato") a _____

III. Que a través de la Plataforma del Estado y por correo electrónico el día _____, INCIBE ha comunicado a _____que ha resultado adjudicataria del Contrato, convocándola en la sede social de INCIBE, a efectos de su formalización.

IV. Que INCIBE y _____reunidas en la sede social de INCIBE, acuerdan celebrar el Contrato de acuerdo con las siguientes.

CLÁUSULAS

PRIMERA.- OBJETO

El objeto del presente contrato es la prestación del servicio I+D _____ _____.

La definición del reto nº ____ se recoge en el anexo I del Documento Regulador.

La oferta de _____ recoge las condiciones de la oferta adjudicada. La oferta presentada por el contratista tiene carácter contractual, con todo su alcance, y para su constancia se adjunta al presente contrato como Anexo.

Igualmente, revisten carácter contractual el plan de verificación en entorno operacional, los compromisos con las entidades usuarias finales de los proyectos de I+D, y el plan de transferencia de resultados.

(Se pueden recoger aspectos relevantes de las ofertas)

SEGUNDA.- CAPACIDAD PARA CONTRATAR

_____declara no estar incursa en ninguna de las causas de incompatibilidad o incapacidad fijadas por la legislación para contratar.

TERCERA.- DERECHOS Y OBLIGACIONES DE LAS PARTES

El contrato se ejecutará en los términos y condiciones previstas en el Documento de licitación.

De manera especial las partes manifiestas que:

3.1. _____se compromete a realizar el servicio objeto del presente contrato en el plazo que figura en la Cláusula Cuarta del presente Contrato y de acuerdo con las condiciones técnicas establecidas en el Documento Regulador.

3.2. Se comprometen a satisfacer el precio de acuerdo con lo dispuesto en la Cláusula Quinta del Contrato. INCIBE no satisfará el precio sin la previa la justificación de los trabajos realizados y su aceptación por INCIBE y la emisión de las correspondientes facturas a su nombre.

3.3. _____hará constar en el encabezamiento de toda la documentación y facturas que remita a INCIBE en relación con el Contrato el número de expediente de contratación: CPP002/22 Reto nº _ Nombre del proyecto.

3.4. El centro habitual de trabajo será en las oficinas del contratista salvo los supuestos recogidos en el Documento Regulador.

3.5. De manera ocasional y justificándose adecuadamente, INCIBE podrá requerir la presencia puntual del equipo, o de parte del mismo, en las instalaciones de INCIBE, con el objeto de resolver cuestiones técnicas u organizativas que puedan surgir durante la ejecución del servicio.

3.6. _____se compromete a ser titular de los derechos necesarios para poder ejecutar el objeto del contrato. _____asignará los recursos profesionales adecuados para realizar con garantía las tareas definidas en el contrato. Además, nombrará un Jefe de Proyecto cuyas funciones serán realizar las funciones de contacto directo con el equipo de Seguimiento y Control designado por INCIBE.

INCIBE pondrá a disposición de los contratistas con los que firme él o los contratos:

3.7. El conocimiento de los gestores de INCIBE y la información sobre estos servicios para la identificación de necesidades, diseño de procedimientos operacionales y desarrollo de soluciones.

Los permisos requeridos para realizar la investigación y las pruebas en cuanto sean competencia de INCIBE.

Su inversión económica en los términos recogidos en el documento regulador y en el contrato.

3.8. Durante la ejecución de los trabajos objeto del contrato, _____se compromete, en todo momento, a facilitar a las personas designadas por el equipo de Seguimiento y Control de INCIBE, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

3.9. _____deberá desarrollar y aportar los conocimientos, metodologías y herramientas necesarias para asegurar el desarrollo óptimo del contrato.

3.10. _____ejecutará las mejoras a las que se ha comprometido en su oferta. Igualmente tienen carácter esencial el cumplimiento de las obligaciones establecidas en su oferta en materia de coinversión, y el pago de royalties correspondiente.

3.11. _____ deberá contratar y mantener con una aseguradora una póliza o pólizas de seguro que ofrezca un nivel adecuado de cobertura para todos los riesgos en que pueda incurrir derivados de la ejecución y cumplimiento del contrato por un importe equivalente al 50% del valor económico del contrato.

3.12. El contrato se ejecutará en los términos y condiciones previstas en el Documento Regulador.

3.13. _____se compromete a ser titular de los derechos necesarios para poder ejecutar el objeto del contrato.

3.14. _____ asignará los recursos profesionales adecuados para realizar con garantía las tareas definidas en el contrato. Además, nombrará un Jefe de Proyecto cuyas funciones serán realizar las funciones de contacto directo con el Director Técnico del proyecto designado por INCIBE.

CUARTA.- PLAZOS

La **duración máxima de los servicios de I+D**, será desde el día siguiente a la formalización del contrato hasta el 30 de junio de 2026. Los proyectos podrán tener una duración menor, de acuerdo con la planificación que se acuerde durante la ejecución del contrato. **No se prevén prórrogas** en cuanto a este plazo, salvo que INCIBE indique lo contrario durante la ejecución de éste.

La duración incluye el plazo para ejecutar todos los compromisos adquiridos por el contratista, incluido el cierre administrativo del proyecto y su carga justificativa necesaria por el uso de fondos PRTR.

El contrato seguirá vigente para dar cumplimento a los compromisos asumidos en relación con los derechos de propiedad intelectual e industrial, que se mantendrán hasta el momento de la finalización del plazo legal de duración de esos derechos.

El servicio se iniciará a partir de la celebración de la reunión de lanzamiento, que tendrá lugar en un plazo no superior a un mes desde la firma del presente documento.

Todos los plazos establecidos en el presente contrato, salvo que se indique que son laborables, se entenderán referidos a días naturales.

El cumplimiento de estos plazos tiene carácter esencial, no obstante, dicho plazo podrá extenderse si se registran retrasos que sean justificados a juicio de la Sociedad.

Tendrán carácter esencial las obligaciones que se establezcan en cuanto al cumplimiento de plazos totales o parciales, y los establecidos en los programas de trabajo. No obstante, dicho plazo podrá extenderse si se registran retrasos que sean justificados a juicio de la Sociedad.

QUINTA.- PRECIO

El presupuesto global del contrato asciende a _____:

a) El precio total máximo del contrato que si se cumplen las condiciones se abonará por INCIBE asciende a _____ IVA excluido conforme al siguiente presupuesto.

   Dentro del precio total y máximo de adjudicación quedan comprendidos igualmente el resto de criterios objetivos ofertados por _____ En concreto, quedan comprendidos en el precio total y máximo de adjudicación las mejoras ofertadas en los siguientes criterios: _____

   Quedan incluidos dentro del presupuesto máximo Todo lo previsto en el documento regulador y la oferta.

b) El contratista por su parte se obliga a aportar al proyecto el % de coinversión comprometido que asciende a un importe de _____

Asimismo, el contratista se obliga al pago de _____ en concepto de royalties durante cinco años en los términos recogidos en del documento regulador.

(Se modificará para adaptar la cláusula si se ha ofertado mayor numero años de royalties a favor de INCIBE)

SEXTA.- CESIÓN DEL CONTRATO Y SUBCONTRATACIÓN

Conforme al Documento Regulador se permite la subcontratación. Sin embargo _____en el ámbito del procedimiento de adjudicación ha manifestado no tener intención de subcontratar prestación alguna del servicio. Se permite la cesión en los supuestos y con las formalidades previas previstos en el documento regulador/ o subcontratar los siguientes servicios _____ con _____

Los eventuales subcontratistas que intervengan durante la ejecución del contrato quedarán obligados sólo ante el contratista, que asumirá la responsabilidad integra de la ejecución del contrato frente a INCIBE, con arreglo estricto al Documento Regulador y a los términos de su oferta.

La intervención de subcontratistas diferentes de los indicados por el contratista en su oferta requerirá de su previa autorización por INCIBE. No se admitirá la sustitución de subcontratistas que afecten a las condiciones tenidas en cuenta para el cumplimiento de los criterios de solvencia, o la adjudicación.

No se admitirán cambios en relación con los subcontratistas si ello genera problemas o conflictos en materia de derechos de propiedad intelectual o industrial.

Aun cuando se produzca una subcontratación de acuerdo con el presente apartado, el contratista seguirá siendo responsable ante la entidad contratante de la ejecución y cumplimiento de todas sus obligaciones, establecidas en el Contrato, siendo responsable asimismo de los daños causados por cualquier negligencia imputable a su subcontratista.

SÉPTIMA.- GARANTÍAS GENERALES

_____garantiza:

a) Que es titular de los derechos, autorizaciones y poderes necesarios para el desarrollo y ejecución del Contrato. _____deberá gestionar y obtener todas las autorizaciones, licencias y permisos que sean necesarios para la realización de las actuaciones que se desarrollen en ejecución del Contrato, incluyendo el abono de las tasas correspondientes.
b) INCIBE se reserva el derecho de comprobar y exigir a _____copia de los documentos acreditativos del cumplimiento de la obligación establecida en esta Cláusula.
c) Que, en todo lo relacionado con el objeto del Contrato, no se encuentra incursa en ningún litigio en cuanto a derechos de uso, licencias, patentes, utilización de marcas o nombres comerciales, u otro tipo de propiedades industriales o intelectuales.
d) Que el objeto del Contrato se realizará cumpliendo todas las condiciones técnicas establecidas, así como los requisitos de aceptación que sean establecidos.
e) Que procederá por su propia cuenta y riesgo a subsanar los errores imputables a su actuación sin cargo alguno para INCIBE.

OCTAVA.- GARANTÍA

_____ha solicitado que la constitución de la garantía definitiva le sea retenida en el precio conforme a lo previsto en el documento regulador, por un importe que cubra

1. Garantía por el 5% del importe de la inversión de INCIBE.
2. Garantía por el 20% del importe comprometido en concepto de *royalties*.

Esta garantía sirve para asegurar el correcto funcionamiento de los trabajos realizados en ejecución del contrato conforme a lo previsto en el documento regulador.

En caso de que se hagan efectivas sobre la garantía las penalidades o indemnizaciones exigibles al contratista, éste deberá reponer o ampliar aquélla, en la cuantía que corresponda, en el plazo de quince días desde la ejecución, incurriendo en caso contrario en causa de resolución.

NOVENA.- SEGURO DE RESPONSABILIDAD CIVIL

_____deberá tener un seguro de Responsabilidad Civil a efectos de cubrir posibles eventualidades que pudieran surgir en la realización del objeto del contrato en los términos recogidos en el documento regulador.

DECIMA.- TRATAMIENTO DE DATOS PERSONALES

No se prevé necesidad de tratar datos personales para la prestación del servicio por el contratista.

En el caso de que deban tratarse _____deberá informar a INCIBE y deberá firmarse un anexo al presente contrato. Si hubiera que tratar datos personales, tanto INCIBE como el contratista, quedan obligados por las disposiciones de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que se adapta en base al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones, y normativa de desarrollo.

Todos los datos obtenidos en el marco de la ejecución del presente contrato serán propiedad exclusiva de INCIBE y deberán ser tratados por el contratista con la máxima confidencialidad. No se podrán utilizar estos datos por parte del contratista salvo que así se autorice por INCIBE mediante escrito en el que se determinarán las condiciones a las que se deberá ajustar dicho uso.

En todo caso, las obligaciones establecidas en relación al tratamiento de datos personales tienen el carácter de obligación contractual esencial a los efectos del régimen de resolución del contrato.

UNDÉCIMA.- OBLIGACIONES DERIVADAS DE FINANCIACIÓN EUROPEA

El contrato está financiado con fondos Europeos dentro del Plan de Recuperación, Transformación y Resiliencia con cargo al Mecanismo para la Recuperación y Resiliencia (MRR).

Es obligación esencial de _____colaborar con INCIBE para la consecución de los hitos, objetivos y carga justificativa que sea necesaria del MRR. En especial en la elaboración de los informes de gestión del proyecto y del subproyecto.

_____declara que cumplirá con la normativa europea y nacional que les resulte aplicable, y en particular, con las obligaciones que se derivan del Reglamento del MRR, especialmente en materia de etiquetado digital, fraude, corrupción, no concurrencia de doble financiación. _____de actuar con los estándares más exigentes en relación con el cumplimiento de las normas jurídicas, éticas y morales, adoptando las medidas necesarias para prevenir y detectar el fraude, la corrupción y los conflictos de interés, comunicando en su caso a las autoridades que proceda los incumplimientos observados.

Es de aplicación obligatoria al contrato el plan de medidas antifraude y anticorrupción –incluyendo el conflicto de intereses-correspondiente al contrato, que se apruebe y se informen por INCIBE.

El contratista manifiesta con la firma de este contrato Declaración de Ausencia de Conflicto de Intereses (DACI) y se compromete a la actualización de dicha declaración si cambian las circunstancias. La falta de estas declaraciones o la falsedad de las mismas será causa de resolución del contrato si se perjudica significativamente a INCIBE.

Este contrato está sujeto a los controles de la Comisión Europea, la Oficina de Lucha Antifraude, el Tribunal de Cuentas Europeo y la Fiscalía Europea y el derecho de estos órganos al acceso a la información sobre el contrato.

Adicionalmente, atendiendo al contenido del PRTR, _____se compromete a respetar los principios de economía circular y evitar impactos negativos significativos en el medio ambiente («DNSH» por sus siglas en inglés «do no significant harm») en la ejecución de las actuaciones llevadas a cabo en el marco de dicho Plan, y manifiesta que no incurre en doble financiación y que, en su caso, no le consta riesgo de incompatibilidad con el régimen de ayudas de Estado.

_____beneficiaria de ayudas financiadas con recursos provenientes del PRTR que participa como contratista en el desarrollo de actuaciones necesarias para la consecución de los objetivos definidos en el Componente 15 *« Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G*», declara conocer la normativa que es de aplicación, en particular las siguientes apartados del artículo 22, del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia:

1. La letra d) del apartado 2: «recabar, a efectos de auditoría y control del uso de fondos en relación con las medidas destinadas a la ejecución de reformas y proyectos de inversión en el marco del plan de recuperación y resiliencia, en un formato electrónico que permita realizar búsquedas y en una base de datos única, las categorías armonizadas de datos siguientes:
   i. El nombre del perceptor final de los fondos;
   ii. el nombre del contratista y del subcontratista, cuando el perceptor final de los fondos sea un poder adjudicador de conformidad con el Derecho de la Unión o nacional en materia de contratación pública;
   iii. los nombres, apellidos y fechas de nacimiento de los titulares reales del perceptor de los fondos o del contratista, según se define en el artículo 3, punto 6, de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo (26);

iv. una lista de medidas para la ejecución de reformas y proyectos de inversión en el marco del plan de recuperación y resiliencia, junto con el importe total de la financiación pública de dichas medidas y que indique la cuantía de los fondos desembolsados en el marco del Mecanismo y de otros fondos de la Unión».

2. Apartado 3: «Los datos personales mencionados en el apartado 2, letra d), del presente artículo solo serán tratados por los Estados miembros y por la Comisión a los efectos y duración de la correspondiente auditoría de la aprobación de la gestión presupuestaria y de los procedimientos de control relacionados con la utilización de los fondos relacionados con la aplicación de los acuerdos a que se refieren los artículos 15, apartado 2, y 23, apartado 1. En el marco del procedimiento de aprobación de la gestión de la Comisión, de conformidad con el artículo 319 del TFUE, el Mecanismo estará sujeto a la presentación de informes en el marco de la información financiera y de rendición de cuentas integrada a que se refiere el artículo 247 del Reglamento Financiero y, en particular, por separado, en el informe anual de gestión y rendimiento». En consecuencia, _____acepta la cesión de datos entre entidades del Sector Público implicadas para dar cumplimiento a lo previsto en la normativa europea que es de aplicación y de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

_____deberá incluir en la documentación del proyecto referencia al “Plan de Recuperación, Transformación y Resiliencia- Financiado por la Unión Europea- NextGenerationUE. En la exposición de la información y de los logos se estará a las instrucciones de INCIBE y lo dispuesto en la normativa.

Dichas obligaciones se establecen en cumplimiento de lo recogido en las Órdenes Ministeriales HFP/1030/2021 y HFP/1031/2021, ambas de 29 de septiembre, que regulan respectivamente el sistema de gestión del PRTR y el suministro de información sobre el cumplimiento de sus hitos y objetivos.

Son de aplicación las normas sobre conservación de la documentación, de acuerdo con lo dispuesto en el artículo 132 del Reglamento Financiero.

DUODÉCIMA.- DOCUMENTACIÓN DE ALTAS Y RELACIÓN NOMINAL DEL PERSONAL ADSCRITO AL CONTRATO

Antes de iniciarse la ejecución del contrato deberá presentarse el alta de los trabajadores asignados al mismo. .

_____se compromete a remitir mensualmente la relación nominal de los trabajadores adscritos al contrato.

DECIMOTERCERA.- ANEXOS

Se recogen como anexos al presente contrato:

- el documento regulador firmado por el contratista;
- el contenido de los sobres B y C;
- la planificación aprobada de la ejecución económica de los desembolsos de los *royalties*;
- la calendarización aprobada de pagos de la inversión de INCIBE.

Y en prueba de cuanto antecede, las Partes suscriben el Contrato, en dos ejemplares y a un solo efecto, en el lugar y fecha señalados en el encabezamiento.

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

D. FÉLIX ANTONIO BARRIO JUÁREZ
DIRECTOR GENERAL

D._____