INSTITUTO NACIONAL DE CIBERSEGURIDAD

España | digital 2026

Compra Pública Precomercial CPP001/23

CPP3-R3. DETECCIÓN Y ANÁLISIS DEL COMPORTAMIENTO DE REDES *BOTNETS* Y SERVIDORES DE COMANDO Y CONTROL A TRAVÉS DE TÉCNICAS INNOVADORAS.

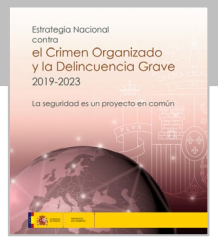
Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

Alineamiento estratégico

MARCO ESTRATÉGICO SEGURIDAD NACIONAL



- Fortalecimiento de las capacidades de ciberseguridad de ciudadanos, pymes y profesionales.
- Impulso del ecosistema empresarial del sector ciberseguridad.
- Impulso de España como nodo internacional en el ámbito de la ciberseguridad.

Iniciativa Estratégica de Compra Pública de Innovación

IMPACTO

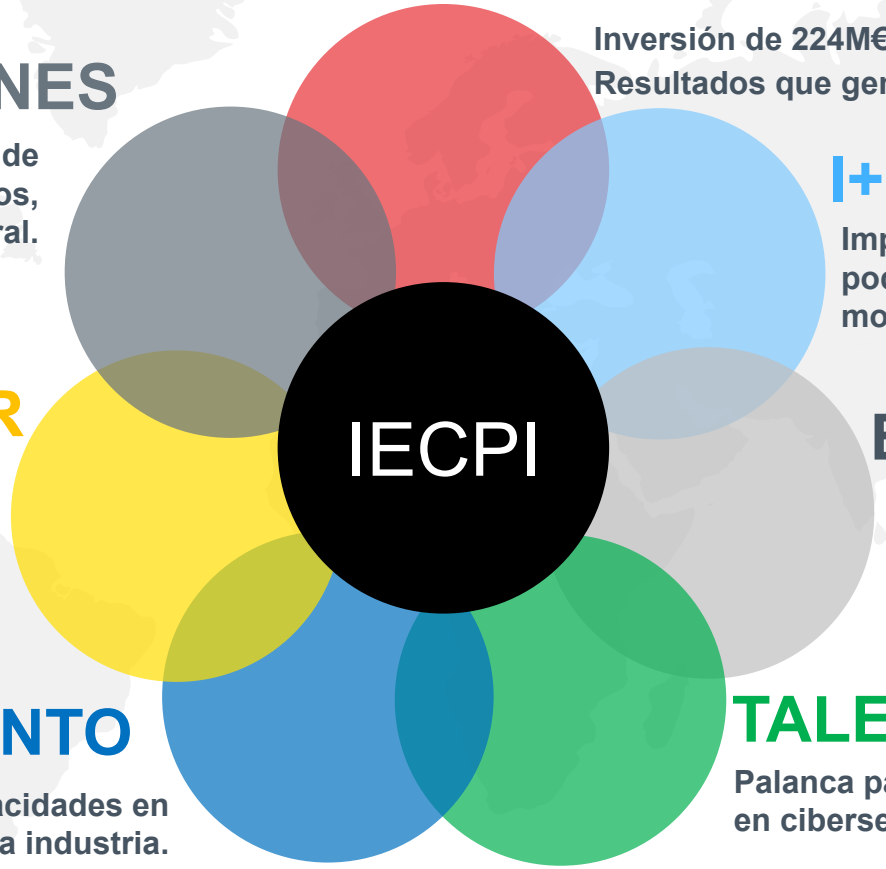
Inversión de 224M€ públicos y movilización de capital privado.
Resultados que generen efectos e impactos económicos y sociales.

SOLUCIONES

Generación de soluciones competitivas de ciberseguridad para usuarios finales, tanto públicos, privados como la ciudadanía en general.

I+D+i

Impulsar la innovación y la competitividad desde los poderes públicos con enfoque multi-proyecto para movilizar el mayor número de agentes.



CADENA DE VALOR

Dinamizar y traccionar toda la cadena de valor de la innovación.
Participación de todos los agentes del ecosistema.

EMPRENDIMIENTO

Promover la participación de empredadores, *start-ups*, pymes y organismos de investigación.

FORTALECIMIENTO

Política de innovación dirigida a fortalecer las capacidades en ciberseguridad de la industria.

TALENTO

Palanca para la generación de empleo y el desarrollo del talento en ciberseguridad.

La IECPI de INCIBE es la mayor iniciativa de Compra Pública de Innovación en ciberseguridad con una inversión pública de 224 millones de €.

Características generales
Compra Pública Precomercial CPP001/23

Documento Regulador

Esta iniciativa de Compra Pública de Innovación esta regulada por el **documento regulador** disponible en la Plataforma de Contratación del Sector Público.

Órgano de Contratación: Dirección General del Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE)
Expediente: CPP001/23

Contexto

Contratación Proyectos I+D

Proyectos independientes de I+D que den respuesta a los retos planteados, que contribuyen a las Actuaciones 1, 2, 3, 4, 5 y 7.

Compartir riesgos/beneficios

Contratación de servicios de I+D a varios operadores económicos (o agrupaciones) en un marco en el que el comprador y el prestador del servicio comparten riesgos y beneficios.

Presupuesto

96M€ para contratos entre 0,3 y 1,5 M€* +IVA.
Etapa 1 OK=25.000€ vs. NOK=3.000€

(*) o la mitad del presupuesto del reto, si Reto<3M€

Plazo

Fecha fin: 30 de junio de 2026.
Sin prórrogas.
Incluidos cierre administrativo y justificación PRTR.
Post-proyecto: Compromisos DPII contraídos.

Competencia

Al menos 2 contratistas independientes entre sí abordando cada reto.

Resultados

Generación de soluciones (productos, servicios materiales) que no estén disponibles actualmente en el mercado validados por usuarios finales.

Innovación

Situación de partida: TRL menores que 6.
Situación de llegada: TRL 7-8.
Comercialización (TRL9) y adquisición excluida.

Usuarios finales

Implicados en la generación y especialmente en las pruebas y validación. Al menos uno de ellos deberá ser aportado por el licitador.

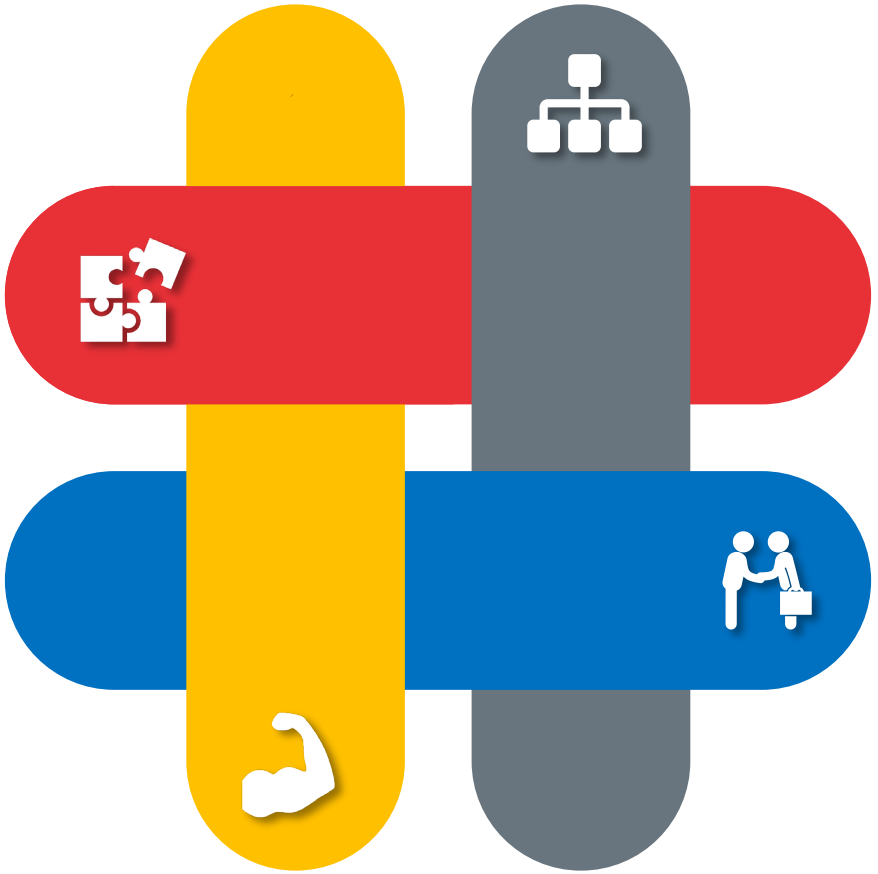
Participantes

QUIÉNES

Operadores económicos **individualmente** o en **agrupación.**

SOLVENCIAS

Económica o Financiera1
Técnica o Profesional2



GRUPOS

Empresas pertenecientes a un mismo grupo empresarial.*

(*) No pueden presentar ofertas diferentes para un mismo reto

SUBCONTRATACIÓN

Subcontratación permitida sin límite.*

(*) es el licitador quien tiene el compromiso y responsabilidad.
El licitador podrá basarse en solvencias de subcontratas

Etapas de ejecución de los contratos

Claves del Documento Regulador (DR)

PLAZO DE EJECUCIÓN. DR 1.4

- Los proyectos se ejecutarán completamente antes del 30 de Junio de 2026.

TRL ADMITIDOS. DR 1.4

- TRL mide el grado de madurez de las tecnologías.
- TRL de partida < TRL6 (demo de prototipo en entorno representativo).
- TRL final = 7/8 (demo de prototipo en entorno representativo / sistema completo y certificado).

RESULTADO O SOLUCIÓN ESPERADA. DR 2.1

- 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.

Claves del Documento Regulador (DR)

USUARIOS FINALES. DR 2.3

- Al menos 1 aportado por el licitador, salvo que en un reto se mencione un número superior.

NÚMERO DE CONTRATISTAS POR RETO. DR 2.3

- Al menos 2 contratistas por reto.
- No hay un número máximo preestablecido, el límite es el presupuesto del reto (Anexo 6).

PRESUPUESTO DE LOS RETOS Y DE CADA CONTRATO. DR 2.5.2

- El Anexo 6 marca el presupuesto máximo por reto.
- En cuanto los contratos, el mínimo 300.000€ y máximo 1.500.000€.

NÚMERO DE OFERTAS QUE UN LICITADOR PUEDE PRESENTAR. DR 3

- Cada licitador puede concurrir máximo a 3 retos y solo puede presentar 1 oferta por reto.

Claves del Documento Regulador (DR)

¿QUÉ SE HACE CON EL DINERO SI HAY REMANENTE DE RETOS QUE NO SE HAN CUBIERTO?. DR 3.5

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 haya ofertas válidas pero insuficiencia de presupuesto para cubrirlas, hasta alcanzar los 96 millones de €.

¿SE PUEDE MODIFICAR EL PROYECTO UNA VEZ INICIADO EL CONTRATO? 4.2.3 DR:

- Sí, a petición de cualquiera de las partes, siguiendo el procedimiento de gestión de cambios y con un límite de aumento del valor económico del un 20% sobre el precio adjudicado, y siempre que haya presupuesto.

TITULARIDAD DPI. DR 4.8.2.1

- La titularidad de los derechos de propiedad intelectual nacidos bajo el ámbito del presente contrato pertenecerá al contratista, a no ser que se aplique la cláusula *call-back* regulada en el apartado 4.8.2.1, en cuyo caso la titularidad pasará a ser de la entidad contratante.
- El contratista concederá una licencia gratuita a INCIBE.
- 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.

Catálogo de retos

R1

Sistemas para la protección frente a ataques contra el espectro electromagnético.

R2

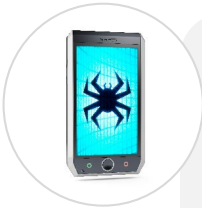
Ciberseguridad en el vehículo conectado.

R3

Detección y análisis del comportamiento de redes *botnets* y servidores de comando y control a través de técnicas innovadoras.

R4

Seguimiento de transacciones vinculadas con *ransomware* y otras campañas.



R5

Sistema de detección de estafas y fraudes en dispositivos móviles.

R6

Diferentes SOC para sectores críticos y esenciales.

R7

Ciberseguridad para proveedores de servicios digitales e infraestructuras digitales.

CPP3-R3. DETECCIÓN Y ANÁLISIS DEL COMPORTAMIENTO DE REDES BOTNETS Y SERVIDORES DE COMANDO Y CONTROL A TRAVÉS DE TÉCNICAS INNOVADORAS.

CPP3-R3 Motivación

- Millones de ciudadanos forman parte de una *botnet* de manera inconsciente.
- Existen *botnets* centralizadas y descentralizadas.
- 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.

CPP3-R3 Objeto

Detección y análisis del comportamiento de redes *botnets* y servidores de comando y control a través de técnicas innovadoras.

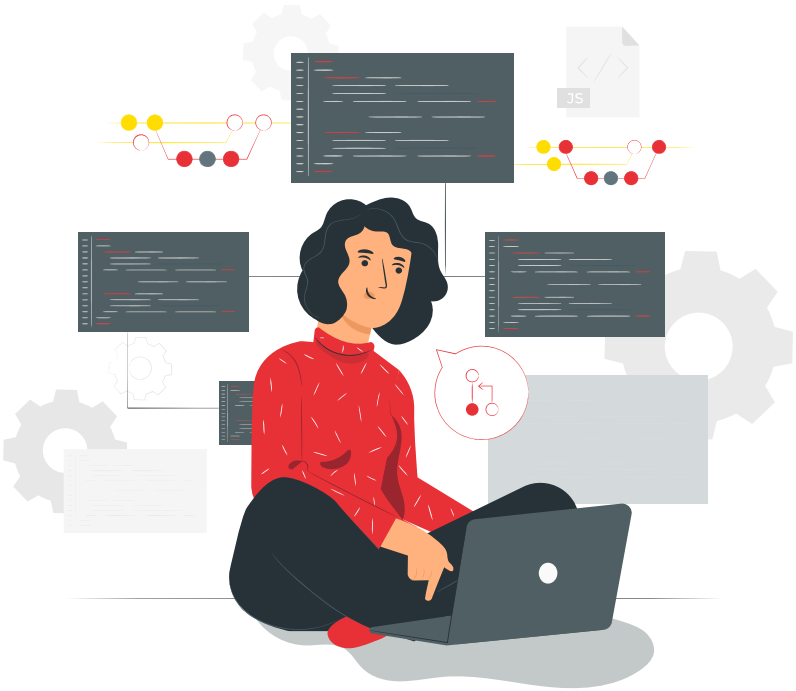
PROBLEMA A RESOLVER

- Desarrollo de servicios de investigación de técnicas avanzadas para la detección de *bots* y, opcionalmente, servidores de comando y control.
- Desarrollo de un sistema que permita a un operador interactuar con la *botnet*, engañando a la red y simulando ser así un *bot* infectado.
- 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 comando y control (C&C) se podría alertar a las FCSE para tratar de ubicarlos y proceder a su desmantelamiento y con ello terminar con la *botnet*.

CPP3-R3 Objeto

Funcionalidades

- 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.
- Identificación de la IP de la víctima y su fiabilidad.
- Identificación de la IP del servidor de C&C y fiabilidad.
- Análisis del comportamiento de la red y detección de cambios en el mismo en tiempo real.
- 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.



CPP3-R3 Alcance

- Entorno operativo: para cumplir con un TRL7-8 se espera una prueba del sistema desplegado en un entorno operativo donde se pueda demostrar sus funcionalidades.
- Duración mínima suficiente para abarcar las tipologías de operaciones habituales.
- Volumen y tipología de datos, similares al entorno real.
- 1 usuario final.

Innovadora,

o que se trate de mejoras sustancialmente significativas de los productos, procesos o servicios ya existentes.

UNE 166000:2006

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.

¿SOLUCIÓN ESPERADA?

Actuación 1. Soluciones de alto impacto estratégico

Actuación 2. Soluciones para pymes

Actuación 3. Soluciones para sectores estratégicos

Actuación 4. Soluciones para el sector público

Actuación 5. Soluciones para INCIBE

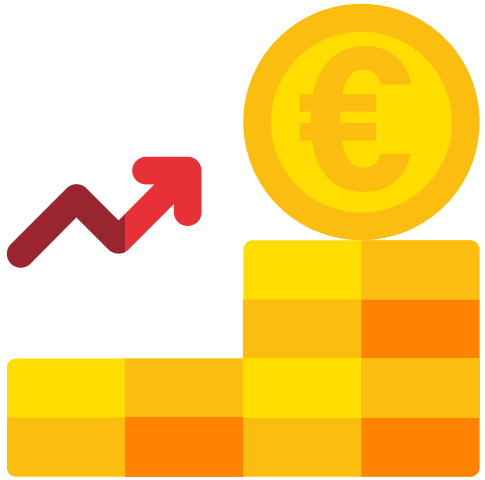
Actuación 7. Pequeños proyectos altamente innovadores

CPP3-R3 Casos de uso

- Organismos nacionales e internacionales con competencias en la protección de ciudadanos y empresas.
  - La detección de víctimas y paneles de C&C y la posterior gestión de estos incidentes de ciberseguridad. Estos incidentes podrían ser reportados a: Proveedores de servicios y a FCSE.
  - Elaboración de contenidos de concienciación para ciudadanía y empresas.
- Fuerzas y Cuerpos de Seguridad nacionales e internacionales. El sistema podrá ser utilizado para el desmantelamiento de los servidores de C&C terminando con ello con la *botnet*.
  - Empresas de ciberseguridad que dentro de sus servicios ofrezcan:
  - Venta de *feeds* de información de inteligencia.
  - Servicios de detección y protección a ciudadanos y empresas.
- 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.

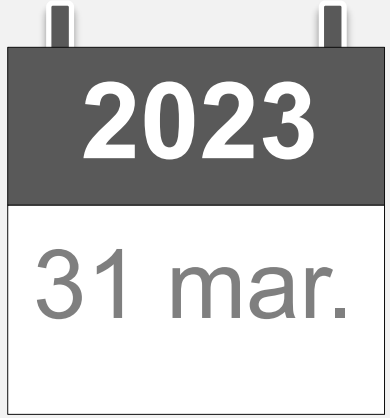
CPP3-R3 Presupuesto

	Reto	Por cada contrato	
	Máxima	**Mínima**	**Máxima**
Aportación de INCIBE	7.500.000 €	300.000 €	1.500.000 €



Mínima coinversión = 6%
Mínimo % de *royalties* (esto no se incluye en el presupuesto) = 1%

Recordatorios importantes



Publicación en la plataforma

Fecha en la que se ha enviado al Diario Oficial de la Unión Europea para la publicación en la Plataforma de Contratación del Sector Público.

Presentación de ofertas

Fecha y hora de cierre de presentación de ofertas a través de la Plataforma de Contratación del Sector Público.

Ejecución del proyecto

Fecha en la que todos los proyectos han de estar completamente ejecutados.

La tramitación completa así como la resolución de dudas se realizará únicamente a través de la Plataforma de Contratación del Sector Público.