ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

InfoDay NCC-ES

Oportunidades de financiación para el desarrollo de capacidades de ciberseguridad

9 de julio de 2025

En breves momentos comenzamos

Cofinanciado por la Unión Europea

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe_

SPANISH NATIONAL CYBERSECURITY INSTITUTE

NCC-ES: Oportunidades de financiación en ciberseguridad Programa Europa Digital

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Conectando el ecosistema

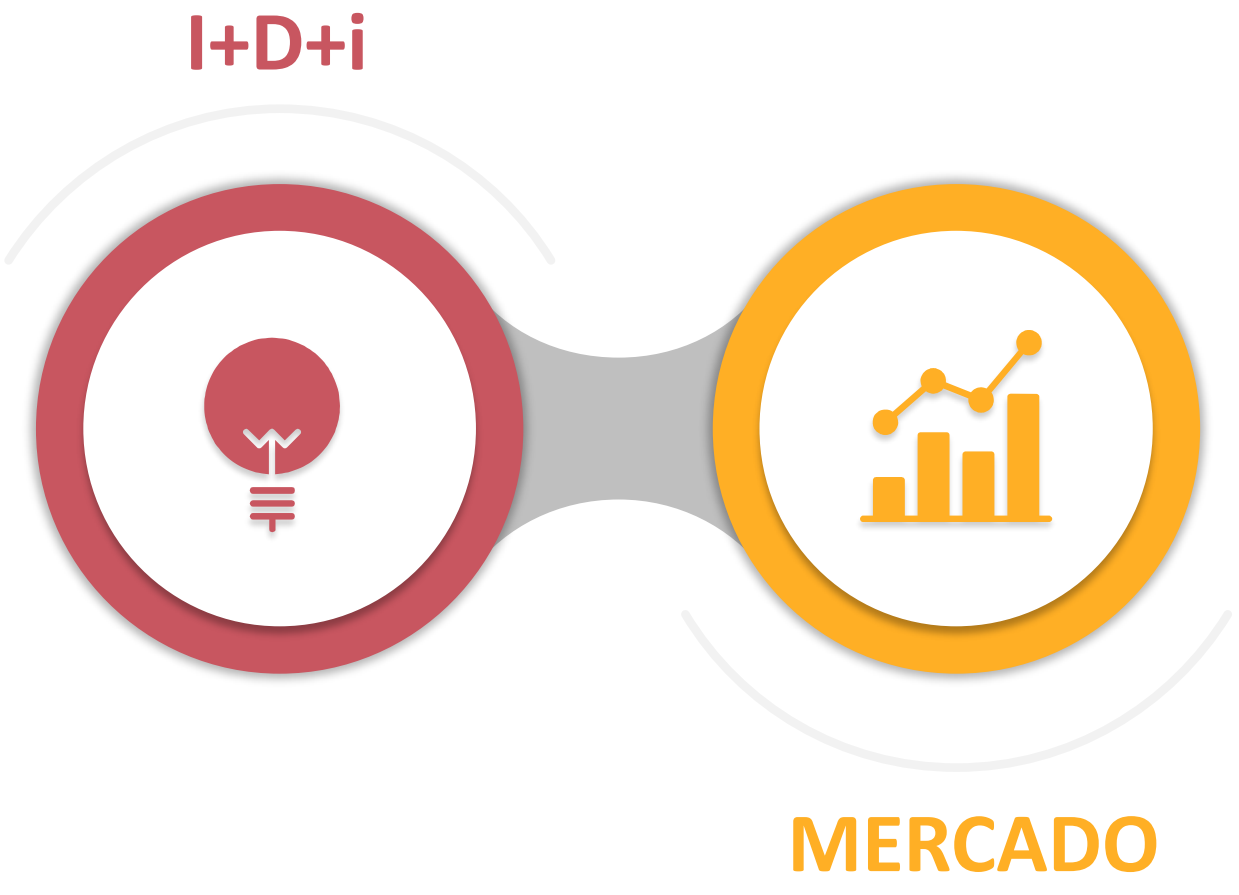
Cerrando la **brecha de innovación** con EE.UU. y China, especialmente en tecnologías avanzadas (e.g. 270.000 millones de dólares en 2021)

Cerrar la brecha: **Investigación - Mercado**

Europa no se coordina donde importa: industria, política, normativa…

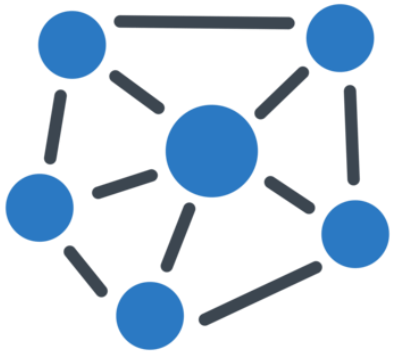
Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Cerrando la brecha



Co-funded by the European Union

Conectando el ecosistema



Entorno de ciberseguridad en Europa

La estructura institucional de la UE funciona como un ecosistema coordinado y distribuido

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Define las prioridades estratégicas de inversión y canaliza la financiación

Proporciona apoyo técnico, impulsa la cooperación operativa y lidera la armonización normativa.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

NCC-ES SPAIN CYBERSECURITY COORDINATION CENTRE

Aplica políticas a escala nacional y conecta a las partes interesadas locales con las prioridades del ECCC

Organización público-privada. Actúa como puente entre la industria y el sector privado con las instituciones públicas.

ECSO EUROPEAN CYBER SECURITY ORGANISATION

Alcance de la iniciativa

Alcance

- **Reforzar las capacidades** europeas en materia de ciberseguridad
- **Proteger** nuestra economía y a la sociedad frente a los **ciberataques**,
- Mantener y promover la **excelencia en la investigación** y reforzar la **competitividad de la industria** de la UE

Septiembre 2017	Cumbre Jefes de Estado Tallín 2017: Mandato de convertir la UE en **líder mundial de ciberseguridad en 2025**
Septiembre 2018	La Comisión presenta la propuesta de Reglamento
Diciembre 2020	Estos Estados miembros **confirman el acuerdo**
Enero 2021	**Adopción formal** por parte del Parlamento Europeo y del Consejo
Junio 2021	**Entrada en vigor** del reglamento
2021-2022	**Puesta en macha** del ECCC y de los NCCs (designación de INCIBE)

Centro Europeo de Competencia: Misión

El Centro Europeo de Competencia en Ciberseguridad (ECCC), con sede en Bucarest, reforzará las **capacidades** de la comunidad tecnológica de la ciberseguridad, protegerá nuestra economía y nuestra sociedad de los **ciberataques**, mantendrá la excelencia en **investigación**, y reforzará la **competitividad** de la industria de la UE en este ámbito

Es la mission del ECCC (art. 3):

- Apoyar la **resiliencia y la fiabilidad de las redes y los sistemas de información**.
- Apoyar las **capacidades, competencias y medios tecnológicos de la Unión en relación con la resistencia y fiabilidad de las infraestructuras de red y los sistemas de información**.
- Aumentar la **competitividad y el liderazgo de la UE** en materia de ciberseguridad.

Debe contribuir:

- La aparición de **soluciones a los retos de ciberseguridad** a los que se enfrentan los sectores público y privado y el apoyo al despliegue efectivo de estas soluciones.
- Tomar **decisiones estratégicas de inversión**, poniendo en común los recursos de la UE, los Estados miembros y la industria.
- Implementar el **apoyo financiero**, en ciberseguridad, de los programas Horizonte Europa y Europa Digital.

ECCC: Agenda Estratégica

Declaraciones de impacto a corto plazo

- Para 2027, el ECCC y la Red de NCCs habrán financiado a las **PYME europeas en el desarrollo y uso de tecnologías, servicios y procesos estratégicos de ciberseguridad** mediante un mecanismo coordinado de financiación en cascada a través de las NCC y la cofinanciación nacional que reduce el umbral de solicitud para las PYMEs.
- Para 2027, el ECCC y la Red de NCCs habrán apoyado y **aumentado la mano de obra profesional en ciberseguridad**, tanto en cantidad como en calidad, mediante la normalización y la certificación de competencias en ciberseguridad e inversiones en educación y formación de profesionales de la ciberseguridad.
- Para 2027, el ECCC y la Red de NCCs habrán **reforzado la experiencia en investigación, desarrollo e innovación y la competitividad** de la comunidad de ciberseguridad de la UE mediante el desarrollo y la aplicación de un plan de acción eficaz y coherente.

Centro de Coordinación Nacional (NCC-ES): Funciones

NCC Funciones

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

- Actuar como punto de contacto y coordinación para apoyar al Centro de Competencia.
- Ejecución de proyectos transfronterizos y acciones conjuntas financiadas a través de la UE
- Aportar conocimientos especializados teniendo en cuenta los retos específicos en materia de ciberseguridad.
- Establecer sinergias con las actividades pertinentes a nivel nacional, regional y local.
- Proporcionar asistencia técnica a los proyectos gestionados por el ECCC
- Promover programas de educación en ciberseguridad
- Evaluar las solicitudes nacionales para formar parte de la Comunidad
- Crear una Comunidad de Competencia público-privada a nivel nacional

ECCC: Una Oportunidad para la I+D+i en ciberseguridad

Impulso Financiero

Mecanismos directos y *financiación en Cascada*

BOE

Real Decreto 204/2023, de 28 de marzo, por el que se modifica el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital.

Financiación para el Objetivo especifico 3 (Ciberseguridad)

158M€ en 2025

118M€ en 2026

114M€ en 2027

1.650M€ (financiación ciberseguridad 2021-2027)

Financiacion Cluster III (destination Ciberseguridad)

90,5M€ en 2025

1.600M€ (financiación Cluster III para 2021-2027)

EUROPEAN UNION
EUROPEAN DEFENCE FUND

8.000 M€
(2021-2027)

Apoyo y Dinamización

- **I+D+i tecnologías emergentes**
- **Pymes e Industria Ciber**
- **Impacto Multisectorial (energía, salud, telco, manufacturero, público, financiero, espacio…)**
- **Soluciones de uso civil y militar**
- **Fomento del Empleo y desarrollo del Talento**
- **Sinergias con Comunidad y órganos europeos**

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DIGITAL EUROPE 8 - Cybersecurity: Cronograma

Apertura de la Convocatoria
Principios de Junio 2025

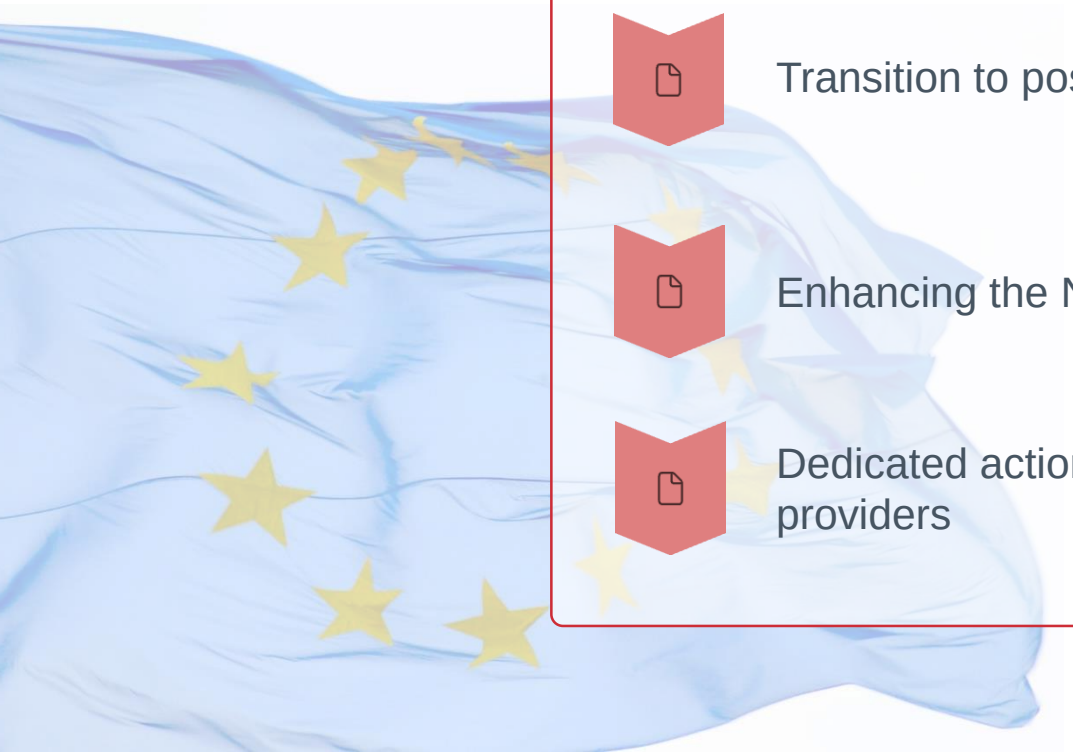
Cierre de la Convocatoria
07/10/2025

Período de Evaluación
03/11/2025 – 12/12/2025

Notificación a los Solicitantes
30/01/2026

Firma del GA
07/07/2026

DIGITAL EUROPE 8 - Acciones



- Transition to post-quantum Public Key Infrastructures
- Enhancing the NCC Network
- Dedicated action to reinforcing hospitals and healthcare providers

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 1: Transition to post-quantum Public Key Infrastructures

Objetivo

- Abordar integración efectiva de los algoritmos PQC en PKIs.
- Ofrecer estrategias de migración eficientes y continuidad negocio.

Alcance

- Diseñar combinadores cripto.
- Realizar pruebas certificados en los protocolos.
- Desarrollar protocolos (gestión/revocación certificados, transparencia), métodos/herramientas gestión claves.

Stakeholder Objetivo

- Todos los actores en la cadena PKI (CAs, CAs intermedias, investigadores, usuarios finales, vendedores).

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 1: Transition to post-quantum Public Key Infrastructures

Indicadores Clave de Rendimiento (KPIs)

- Disponibilidad y rendimiento de combinadores y certificados híbridos.
- Desarrollo de librerías open-source.
- Claridad de procedimientos de gestión de claves.
- Evaluación de alternativas X.509.

Resultado esperado

- Desarrollo de nuevos combinadores, evaluación experimental de certificados híbridos y pruebas de usos alternativos a X.509
- Creación o mejora de librerías open-source y establecimiento de procedimientos claros para la gestión del ciclo de vida de claves.
- Actividades de concienciación y formación para fomentar el conocimiento y la adopción de estas tecnologías.

Presupuesto: 15M€. Financiación: 50%. Simple Grants.

Duración Esperada: 36 meses. **Cuantía estimada de presupuesto por proyecto:** 3-4M€

Call 2: Enhancing the NCC Network

Objetivo

- Apoyar la operación de los Centros Nacionales de Coordinación (NCCs) y fortalecer sus capacidades.
- Fomentar la adopción de soluciones de ciberseguridad (especialmente por PYMEs).
- Impulsar el ecosistema de start-ups/PYMEs de ciberseguridad europeas.
- Aumentar la concienciación sobre ciberseguridad y potenciar el mercado único digital para productos/servicios de ciberseguridad.

Alcance

- Ser puntos de contacto y aportar experiencia al ECCC; creando sinergias nacionales/regionales/locales.
- Apoyo estratégico y técnico para las PYMEs en la participación en proyectos transfronterizos, acciones financiadas (posible FSTP para PYMEs) y la adopción de soluciones y herramientas innovadoras.
- Desarrollo de capacidades y gestión de la comunidad, promoviendo los resultados, gestionando la Comunidad de Competencia y realizando actividades de concienciación, formación y desarrollo de talento (boot camps, desafíos, etc.).

Stakeholder Objetivo

- Centros Nacionales de Coordinación (NCCs) y sus consorcios (incluyendo entidades públicas/privadas, academia, investigación), PYMEs, start-ups, sociedad civil, comunidad académica/investigadora.

Call 2: Enhancing the NCC Network

Resultado esperado / Entregables Clave :

- Impulsar una red de iniciativas, marcos para aceleradoras/incubadoras y una posible plataforma o marketplace europeo para fomentar la adopción de soluciones innovadoras.
- Reforzar el Observatorio y la Comunidad de Competencia, y organizar plataformas/eventos para facilitar el acceso a financiación y al mercado.
- Desarrollar campañas centralizadas de sensibilización, apoyar la enseñanza y el talento (incluyendo embajadores), y promover la adopción de capacidades reforzadas.

Presupuesto: 10M€. Financiación: 50%. / Si se usa FSTP: El NCC recibe el 100% para esa parte, pero el apoyo financiero a terceros cubrirá el 50% de los costes elegibles del tercero. Simple Grants.

Duración Esperada: 36-48 meses. **Cuantía estimada de presupuesto por proyecto:** 2-3M€

Call 3: Dedicated action to reinforcing hospitals and healthcare providers

Objetivo

- Fortalecer la ciberseguridad de hospitales y proveedores sanitarios; mejorando la detección, monitorización y respuesta a ciberamenazas.
- Aumentar la resiliencia del sistema sanitario europeo.
- Contribuir al plan de acción de la UE en ciberseguridad sanitaria

Alcance

- Abordar las necesidades de monitorización, inteligencia y respuesta; definiendo el estado de preparación y necesidades específicas e identificar soluciones como SOCs, SIEM, herramientas y formación.
- Desarrollar planes técnicos adaptados con estimaciones de costes, realizar demos de implementación en hospitales/proveedores y proporcionar formación al personal sanitario.
- Apoyar proyectos piloto con clústeres/asociaciones del sector salud y proveedores de ciberseguridad.
- Difundir buenas prácticas para replicar/escalar, a fin de apoyar y fomentar el cumplimiento de NIS 2

Stakeholder Objetivo

- Entidades públicas y privadas; Clústeres/asociaciones regionales/nacionales de hospitales y proveedores sanitarios (pequeños, medianos, grandes) de al menos 2 Estados Miembros; Proveedores de servicios de ciberseguridad.

Call 3: Dedicated action to reinforcing hospitals and healthcare providers

Resultado esperado / Deliverables Clave :

- Realizar el mapeo de necesidades comunes de ciberseguridad, directrices para autoevaluación de proveedores sanitarios y elaboración de planes técnicos detallados para mejorar la resiliencia.
- Mejorar la capacidades de detección y respuesta (especialmente ante ransomware), implementación de instalaciones piloto monitorizadas con KPIs, y garantía de continuidad operativa ante incidentes.
- Formación del personal sanitario y campañas de difusión para facilitar la replicación y escalado de las soluciones en toda Europa.

Presupuesto: 30M€. Financiación: 50%. Simple Grants.

Duración Esperada: 18-24 meses. **Cuantía estimada de presupuesto por proyecto:** 3-5M€

DIGITAL EUROPE Cybersecurity 9: Cronograma*

Apertura de la Convocatoria
01/09/2025

Cierre de la Convocatoria
22/01/2026

Período de Evaluación
16/03/2026 – 15/05/2026

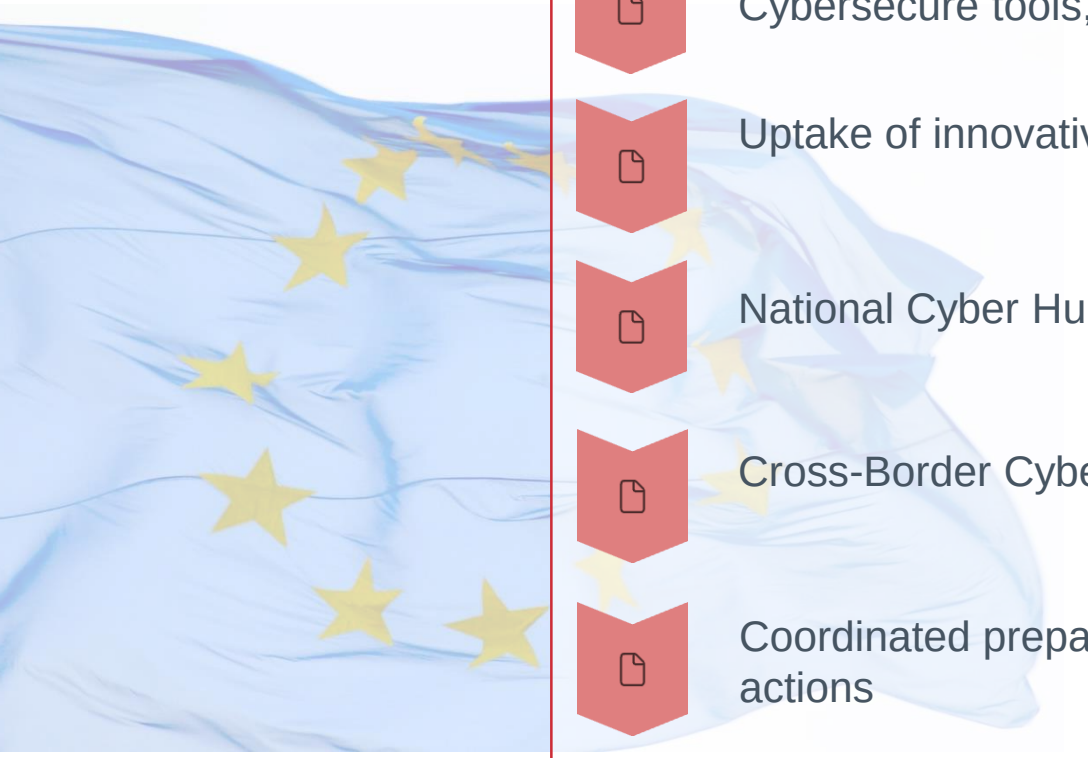
Notificación a los Solicitantes
01/07/2026

Firma del GA
15/07/2026

*Fechas provisionales

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DIGITAL EUROPE 9 - Calls



- Cybersecure tools, technologies and services relying on AI
- Uptake of innovative cybersecurity solutions for SMEs
- National Cyber Hubs
- Cross-Border Cyber Hubs
- Coordinated preparedness testing and other preparedness actions

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 1: Cybersecure tools, technologies and services relying on AI

Objetivo

- Reforzar capacidades de autoridades (Cyber Hubs, CSIRTs, etc.) y entidades NIS 2 con herramientas IA para analizar, detectar, prevenir y responder a ciberamenazas/incidentes.
- Abordar la seguridad de la IA.

Alcance

- Detección avanzada de amenazas y anomalías, respuesta rápida a incidentes, mitigación de malware e identificación de vulnerabilidades.
- Protección de datos sensibles, cumplimiento del Reglamento de Ciberresiliencia (CRA) y certificación de seguridad, especialmente en soluciones basadas en IA.
- Establecimiento de mecanismos seguros para el intercambio de inteligencia sobre amenazas cibernéticas (CTI).

Stakeholder Objetivo

- Proveedores tecnología, operadores Cyber Hubs, investigación/academia, entidades ciberseguridad, sector público, entidades NIS 2, sector privado, otros stakeholders relevantes.

Call 1: Cybersecure tools, technologies and services relying on AI

Indicadores Clave de Rendimiento (KPIs)

- Nivel de despliegue de tecnologías.
- Número de herramientas desarrolladas/desplegadas.
- Disponibilidad de feeds/servicios CTI europeos.
- Contribución a estandarización/certificación.

Resultado esperado

- Despliegue de tecnologías de inteligencia artificial como facilitadoras para Cyber Hubs y CSIRTs, y desarrollo de nuevas herramientas ciber basadas en IA.
- Herramientas de automatización para CTI, mejora del intercambio de información y provisión de feeds y servicios CTI europeos.
- Desarrollo de soluciones de IA seguras para sectores cubiertos por la directiva NIS y contribución a procesos de estandarización y certificación.

Presupuesto: 15M€. Financiación: 50%. Simple Grants.

Duración Esperada: 36 meses. **Cuantía estimada de presupuesto por proyecto:** No especificado.

Call 2: Uptake of innovative cybersecurity solutions for SMEs

Objetivo

- Apoyar la entrada al mercado y diseminación de soluciones en ciber e IA para PYMEs.
- Apoyar actividades de formación, sensibilización y mejora de la seguridad en soluciones open-source, incluyendo programas de recompensas por errores (bug bounty).

Alcance

- Apoyo a la adopción de herramientas y servicios de ciberseguridad listos para el mercado, especialmente desarrollados por PYMEs o en proyectos financiados por la UE.
- Mejora de la preparación, protección y respuesta ante amenazas mediante servicios de protección, auditoría, pruebas de seguridad, respuesta a incidentes y herramientas de investigación.
- Impulso a plataformas de interacción entre proveedores y usuarios, formación, campañas de sensibilización, hackathons y mejora de software open-source

Stakeholder Objetivo

- PYMEs, start-ups, investigación/academia, sector público, entidades NIS 2, otros actores industriales y stakeholders relacionados.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 2: Uptake of innovative cybersecurity solutions for SMEs

Indicadores Clave de Rendimiento (KPIs)

- Nivel de adopción de herramientas IA por PYMEs.
- Disponibilidad y usabilidad de toolkits.
- Mejora en la resiliencia cibernética de las PYMEs participantes.

Resultado esperado

- Adopción soluciones ciber IA innovadoras.
- Herramientas/servicios IA actualizados para PYMEs.
- Integración IA en procesos ciberseguridad.
- Despliegue herramientas IA ciberseguras y conformes a legislación UE.

Presupuesto: 15M€. Financiación: 50%/75% (PYMES). Simple Grants.

Duración Esperada: 36 meses. **Cuantía estimada de presupuesto por proyecto:** No especificado.

Call 3: National Cyber Hubs

Objetivo

- Establecer y consolidar centros nacionales que actúen como puntos de referencia para la implementación de políticas, iniciativas y capacidades en ciberseguridad.
- Crear/fortalecer Hubs nacionales para monitorizar, entender y gestionar ciberamenazas en colaboración con CSIRTs/ISACs.

Alcance

- Formación en herramientas, análisis, CTI, estándares (ECSF) y participación en hubs transfronterizos para fortalecer capacidades humanas y técnicas. Capacitación (equipos, herramientas, feeds CTI, análisis, interconexión).
- Uso de inteligencia artificial, automatización, hardware seguro y estándares para mejorar la eficiencia y la seguridad en ciberdefensa.
- Vigilancia de infraestructuras clave como cables submarinos y mejora del intercambio seguro de información.

Stakeholder Objetivo

- Organismos públicos actuando como Cyber Hubs Nacionales (identificados por EMs).

Call 3: National Cyber Hubs

Indicadores Clave de Rendimiento (KPIs)

- Niveles madurez SOC antes/después.
- Número de entidades beneficiadas.
- Nivel intercambio información.
- Servicios CTI desarrollados.

Resultado esperado

- Creación y consolidación de Hubs Nacionales de primer nivel.
- Desarrollar capacidades CTI y conciencia situacional.
- Realizar cursos de formación específicos.
- Implementación de aplicaciones de notificación automatizada.

Presupuesto: 20M€. Financiación: Joint Procurement (50%) + Simple Grant (50%).

Duración Esperada: 36 meses. **Cuantía estimada de presupuesto por proyecto:** No especificado.

Call 4: Cross-Border Cyber Hubs

Objetivo

- Crear nuevos Cross-Border Cyber Hubs sobre SOCs existentes para agregar datos ciberamenazas entre varios EMs.
- Fomentar la adquisición y/o adoptación de herramientas comunes (de automatización).

Alcance

- Prevención, detección y análisis de amenazas, con monitorización de infraestructuras críticas como cables submarinos.
- Adopción de herramientas, procesos e infraestructuras comunes para CTI, aplicando estándares como MISP y CSAF, junto con analítica avanzada y agrupación de datos.
- Refuerzo de la colaboración en la CSIRTs Network, y mejora del flujo de información sobre incidentes de gran escala hacia EU-CYCLONe y otros actores clave.

Stakeholder Objetivo

- Organismos públicos actuando como Cyber Hubs Nacionales (identificados por EMs) participando en el Hub Transfronterizo.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 4: Cross-Border Cyber Hubs

Indicadores Clave de Rendimiento (KPIs)

- Niveles madurez SOC antes/después.
- Número de entidades beneficiadas.
- Nivel intercambio información.
- Servicios CTI desarrollados.

Resultado esperado

- Hubs transfronterizos de primer nivel.
- Intercambio CTI entre Hubs Nacionales.
- Acuerdos intercambio información.

Presupuesto: 20M€. Financiación: Joint Procurement (75%) + Simple Grant (50%).

Duración Esperada: 36 meses. **Cuantía estimada de presupuesto por proyecto:** No especificado.

Call 5: Coordinated preparedness testing and other preparedness actions

Objetivo

- Complementar esfuerzos de la EMs/UE para aumentar protección/resiliencia (esp. infraestructuras críticas).
- Asistir a la EMs en preparación.

Alcance

- Realizar pruebas de vulnerabilidades (pen testing);
- Despliegue de herramientas/infraestructuras (cyber-ranges);
- Evaluación de las capacidades, cadena suministro, amenazas/riesgos.
- Monitoreo de los riesgos: apoyo en la divulgación/gestión de vulnerabilidades; ejercicios/formación.

Stakeholder Objetivo

- Autoridades competentes, CSIRTs. Adicionalmente: SOCs/Hubs, entidades sectores críticos/muy críticos, industria (ISACs); Proveedores servicios ciberseguridad confiables.

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Call 5: Coordinated preparedness testing and other preparedness actions

Indicadores Clave de Rendimiento (KPIs)

- Número de pruebas desarrolladas, entidades apoyadas, acciones transfronterizas.
- Número de usuarios cubiertos;
- Número y naturaleza de vulnerabilidades descubiertas;
- Número de evaluaciones amenazas/análisis

Resultado esperado

- Cooperación/preparación/resiliencia mejorada.
- Servicios apoyo preparación, evaluación amenazas/riesgos y monitoreo de riesgos.
- Mejor cumplimiento, divulgación/monitoreo coordinado vulnerabilidades.
- Habilidades mejoradas vía ejercicios/formación.

Presupuesto: 5M€. Financiación: 50%. Simple Grants.

Duración Esperada: 36 meses. **Cuantía estimada de presupuesto por proyecto:** No especificado.

Proyectos Europeos: Oportunidades Financiación Cascada

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Proyectos CYSSDE y SECURE

CYSSDE
CYBERSECURITY DEPLOYMENT SUPPORT
Preparedness Support, Capacity & Capabilities

- Financiación total: 4M€ (2M€ ya repartidos)
- Ayuda: 200.000€
- Tasa financiación: 50%
- Público objetivo: Proveedores de pentest, pymes
- Apertura siguiente convocatoria: T1 2026

- Despliegue de pruebas de pentest y monitoreo de riesgos en entidades NIS2 y CER, también pymes

SECURE
Cyber Resilience for SMEs

- Financiación total: 16,5M€
- Ayuda: 30.000€
- Tasa financiación: 50%
- Público objetivo: Pymes
- Apertura primera convocatoria: Sept 2025

- Adecuación de fabricantes de productos con componentes digitales, proveedores de herramientas y soluciones para el cumplimiento de la CRA, otras categorías bien justificadas en línea con la CRA

Co-funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

INSTITUTO NACIONAL DE CIBERSEGURIDAD

¡Gracias!

www.incibe.es

nccspain@incibe.es

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

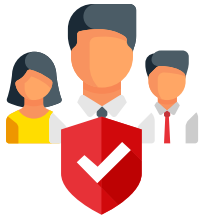
SPAIN
Land of cybersecurity

El programa DIANA y las oportunidades de financiación del uso dual

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Cofinanciado por la Unión Europea
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI INNOVACIÓN

El mandato del NCC-ES en el desarrollo de la industria de uso dual

Reglamento (UE) 2021/887 *del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.*



Contribuir al amplio despliegue de la tecnología avanzada, en particular mediante la gestión o el apoyo a la adquisición de productos y soluciones

Facilitar la cooperación entre los sectores **civil y de defensa en relación con las tecnologías y aplicaciones de doble uso**, y potenciar las sinergias entre la defensa civil y el Fondo Europeo de Defensa.

8.6.2021 ES Diario Oficial de la Unión Europea L 202/1

I

(Actos legislativos)

REGLAMENTOS

REGLAMENTO (UE) 2021/887 DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 20 de mayo de 2021

por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 173, apartado 3, y su artículo 188, párrafo primero,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo (1),

De conformidad con el procedimiento legislativo ordinario (2),

Considerando lo siguiente:

(1) La mayor parte de la población de la Unión está conectada a internet. La vida cotidiana de las personas y la economía se están volviendo cada vez más dependientes de las tecnologías digitales. Los ciudadanos y las empresas están cada vez más expuestos a incidentes ciberseguridad graves y numerosas empresas en la Unión sufren al menos un incidente de ciberseguridad cada año. Ello pone de manifiesto la necesidad de resiliencia, de mejorar la

Principales características en el ámbito del uso dual

Especialmente en los marcos internacionales, implican lagunas en la aplicación de tecnologías duales.

Es necesario abordar tecnologías en rápida evolución, con medidas proactivas, dinámicas y con visión de futuro. Estas tecnologías evolucionan mucho más rápido que los marcos regulatorios tradicionales, lo que exige una transición hacia una gobernanza flexible y anticipatoria.

Panorama de financiación fragmentado para la I+D de doble uso. La financiación actualmente es dispersa y descoordinada, lo que limita su impacto.

Herramientas financieras: incentivos fiscales, subvenciones y préstamos a bajo interés aplicados de manera inconsistente e infrautilizados.

Dificultades para atraer inversión privada en tecnologías de alto riesgo y alta rentabilidad.

Construir un ecosistema tecnológico resiliente y soberano, haciendo frente a la fragmentación de su infraestructura digital y tecnológica transfronteriza.

Se requiere aspirar a un mercado unificado que pueda incentivar la producción local y reducir la dependencia de proveedores externos.

Reglamento (UE) 2021/821, → infraestructura tecnológica regulatoria y de pruebas transfronterizas.

El objetivo final no debe ser sólo fortalecer la seguridad mutua, sino también establecer un estándar mundial para la innovación responsable en tecnologías de doble uso.

Desarrollar un enfoque cooperativo para el establecimiento de normas globales.

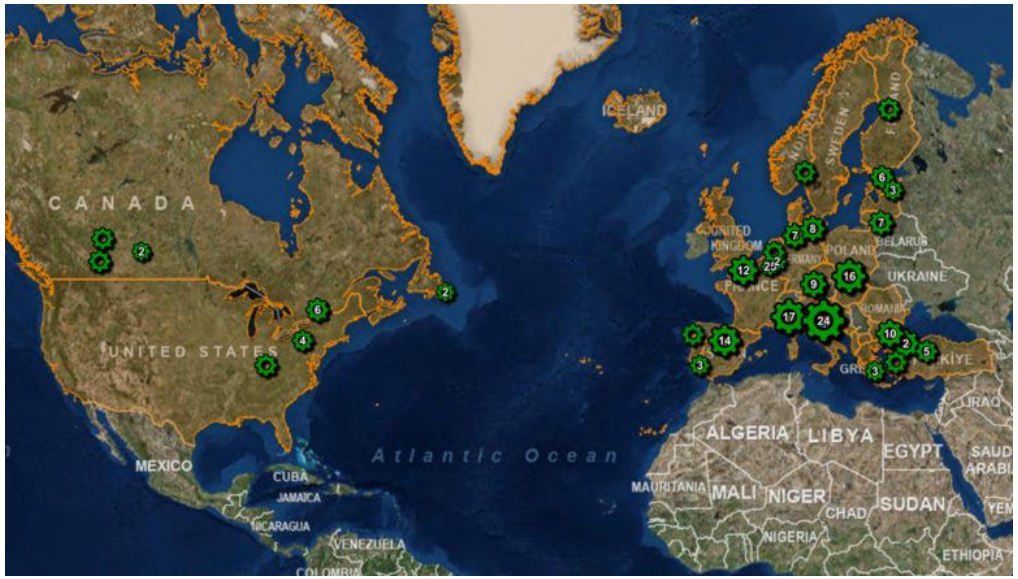
Desarrollo de sistemas integrados que armonicen las prioridades regulatorias y tecnológicas de los Estados miembros.

Extraído de *Dual-use technology – cross-sector cooperation in the cyber security sector. policy brief.* Cybersec Expo-Forum

DIANA de la OTAN

DIANA es la Aceleradora de Innovación en Defensa para el Atlántico Norte, una organización de la OTAN cuya misión es encontrar y acelerar la innovación de **doble uso**.

DIANA presenta anualmente convocatorias en las que plantea retos relacionados con la defensa. Cada año selecciona a innovadores que participan en un **programa de aceleración para el desarrollo de su tecnología**, recibiendo soporte económico, de conocimiento y entrando a formar parte de la red completa de la DIANA

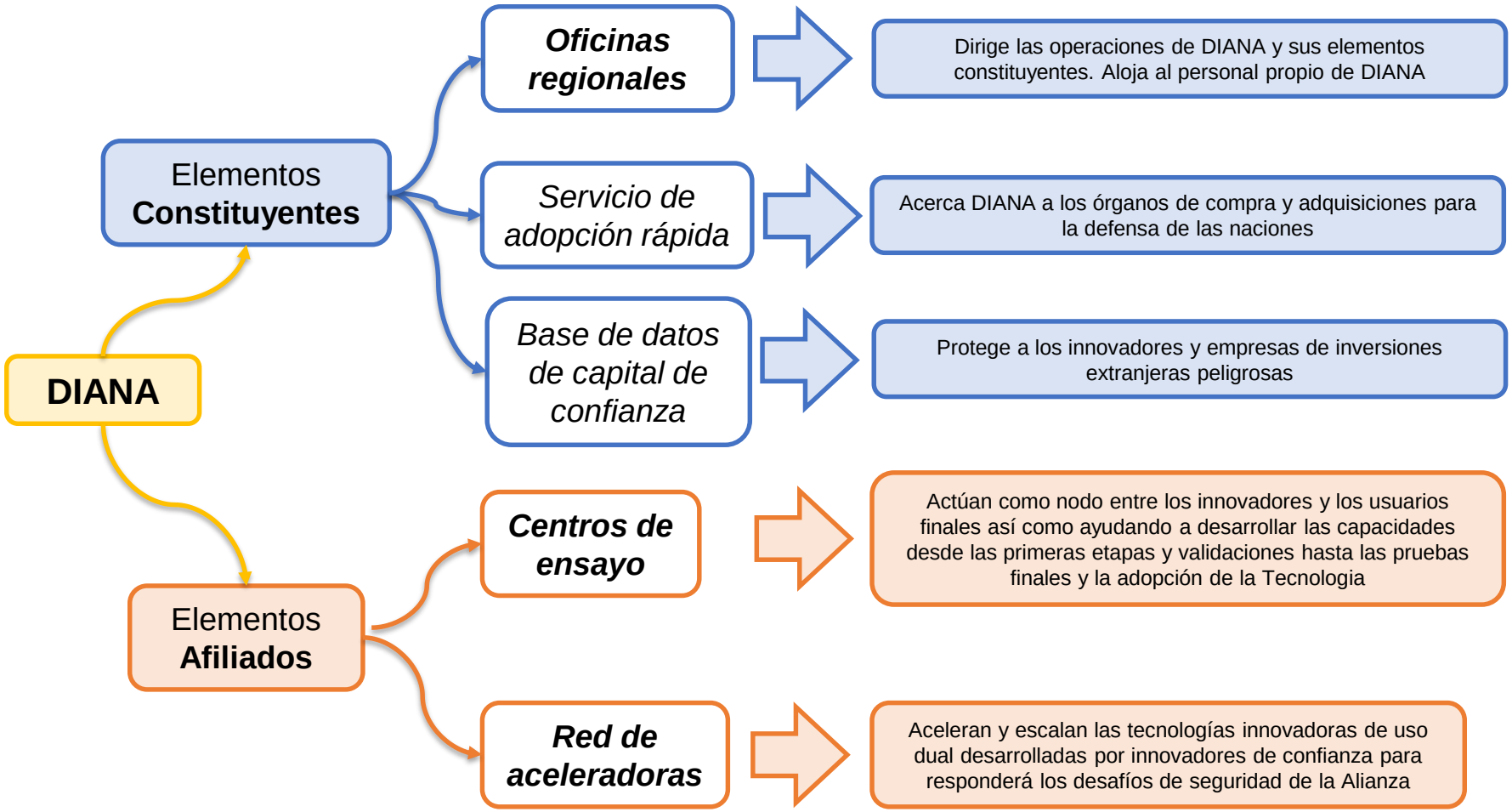


- Innovadores
- Aceleradoras
- Test Centres
- Usuarios finales
- Inversores
- Industria

The DIANA Accelerator Programme is designed to equip businesses with the skills and knowledge to navigate the world of deep tech, dual-use innovation.

Emerging and disruptive technologies are changing the way the Alliance operates in times of peace, crisis, and conflict.

Estructura

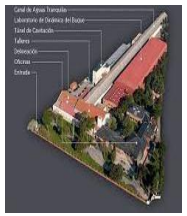

DIANA
Elementos Constituyentes
Elementos Afiliados
Oficinas regionales
Servicio de adopción rápida
Base de datos de capital de confianza
Centros de ensayo
Red de aceleradoras
Dirige las operaciones de DIANA y sus elementos constituyentes. Aloja al personal propio de DIANA
Acerca DIANA a los órganos de compra y adquisiciones para la defensa de las naciones
Protege a los innovadores y empresas de inversiones extranjeras peligrosas
Actúan como nodo entre los innovadores y los usuarios finales así como ayudando a desarrollar las capacidades desde las primeras etapas y validaciones hasta las pruebas finales y la adopción de la Tecnologia
Aceleran y escalan las tecnologías innovadoras de uso dual desarrolladas por innovadores de confianza para responderá los desafíos de seguridad de la Alianza

Requisitos y beneficios para la empresa

- Tener la sede en un estado miembro de la OTAN (independientemente de la nacionalidad)
- Tener un número DUNS (Data Universal Numbering System)
- Desarrollar tecnologías a partir de TRL4. Se estudiarán los casos con TRL más bajos.
- No ser una universidad ni una entidad sin ánimo de lucro. En el futuro se explorarán estas posibilidades
- Dedicar un tiempo mínimo del 20% al programa.
- Pueden ser de cualquier tamaño, a pesar de que el programa será más beneficioso para start-ups y empresas pequeñas

- Financiación
- Mentoría de científicos, ingenieros, usuarios finales, empresarios y expertos gubernamentales, asesoría jurídica…
- Acceso a red de inversores y participación en Demo-days
- Feedback de usuarios finales
- Oportunidad de presentar su tecnología en ambientes operacionales
- Acercamiento al mercado

Centros de ensayo



CEHIPAR
Canal de Experiencias Hidrodinámicas El Pardo

CIMA
Centro de Instrucción de Medicina Aeroespacial

CLAEX
Centro Logístico de Armamento y Experimentación

NEUROTECNOLOGÍA e IA
(CTB, UPM)

COMUNICACIONES CUÁNTICAS
(CCS, UPM)

Centros adicionales TICS

Nueve (9) nuevos centros de ensayo. (MadQCi, Dev. Centre & Lab-I, Dev. Centre & Lab-II, TCCT-León, TCCT-Málaga, TCCT-Vigo, TCCT-Madrid, Thinx BCN, Thinx MAD)

Programa piloto 2023

Energy Resilience

Secure Information Sharing

Sensing and Surveillance

Se recibieron **1.675** solicitudes y se seleccionaron 44 empresas.

España presentó 44 solicitudes (10º posición)

Fueron seleccionadas dos entidades españolas:

- Zelestium (reto Energy Resilience)
- G2-Zero (reto Secure Information Sharing)

Spanish Accelerator site

INCIBE, como **NCC-ES designado** trabaja para el desarrollo de las capacidades de uso dual ofreciendo iniciativas que fomenten el ecosistema de esta industria.

En colaboración con la UPM Universidad Politécnica de Madrid, conforman la aceleradora nacional del programa DIANA (Spanish Accelerator Site UPM-INCIBE), coordinada por el Ministerio de Defensa, que contribuye al desarrollo del ecosistema de la industria del uso dual en España.

PART OF THE DIANA NETWORK

- DIANA cuenta con una red de aceleradoras en la que los innovadores seleccionados en cada edición realizan una estancia de 6 meses.
- La aceleradora nacional (INCIBE-UPM) se ha acreditado recientemente para recibir los primeros proyectos a acelerar en 2026.

Convocatoria 2026 – plazo abierto

Ya está abierto hasta el próximo 11 de julio el plazo de presentación de propuestas para la convocatoria 2026 de DIANA (Defence Innovation Accelerator for the North Atlantic) de la OTAN. Además, junto con la convocatoria ya se han presentado los nuevos 10 retos para el año 2026

Retos 2026

energy & power

sensing & surveillance

human health & performance

data & information security

critical infrastructure & logistics

Proceso de evaluación

Revisión de la documentación → Evaluación quad chart → Evaluación proposal form → Presentación entrevista

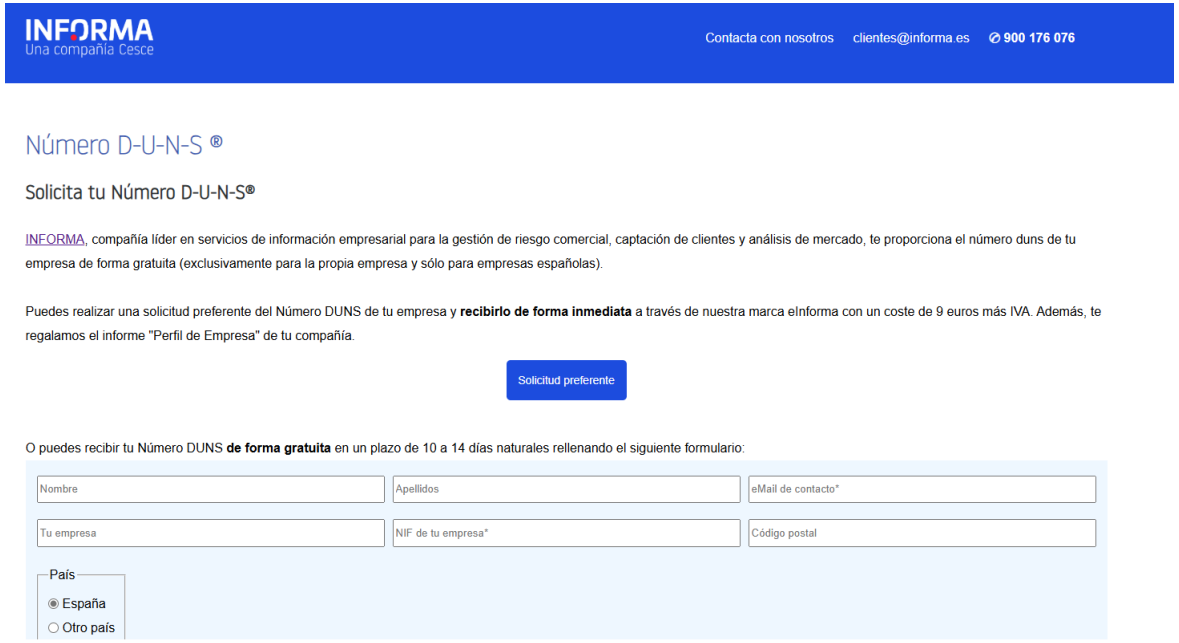
Alignment to challenge	**Technical Approach**
Roadmap with Risks, Mitigation and Maturation Plan	**Dual-use Business Case**

Part 1 Abstract
Part 2 Alignment to the challenge statement
Part 3 Techinal Solution
Part 4 Dual use potential
Part 5 Commercial analysis
Part 6 Development Roadmap with risks and mitigations
Part 7 Use of challenge funding

*Importante: número DUNS

D-U-N-S® (Data Universal Numbering System)

Es un identificador numérico de nueve dígitos, que proporciona identidad única a nivel global a cada negocio o empresa.



NCC-ES INCIBE
Edificio INCIBE. Av. José Aguado 41.
24005 León. España
Tel: +34 987 877 189
nccspain@incibe.es

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPAIN
Land of cybersecurity

Digital Europe Programme

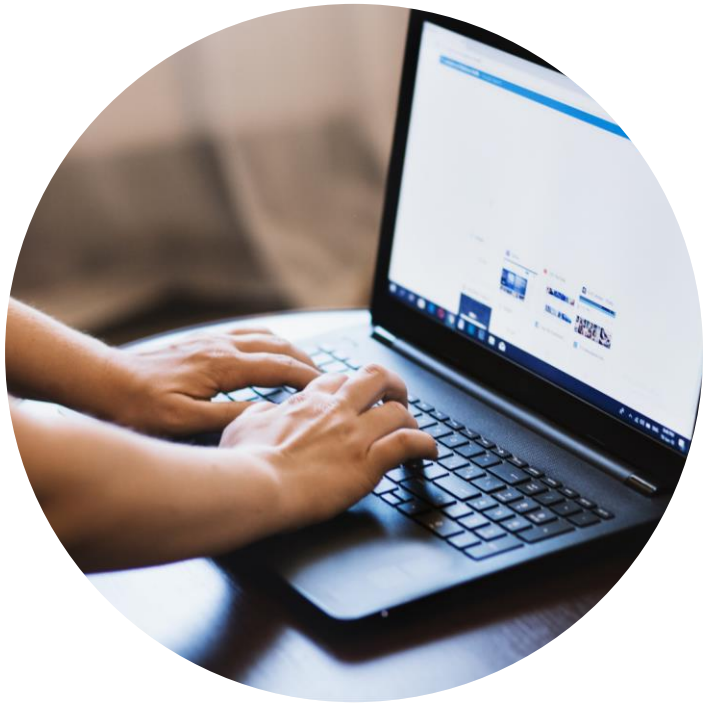
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cofinanciado por la Unión Europea

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Índice

- ¿Qué es el Programa Europa Digital?
- Objetivos Específicos
- Programas de Trabajo
- Tipos de Financiación
- Costes Subvencionables
- Ejecución del Programa
- ¿Cómo participar?
- Evaluación de la Propuesta
- Convocatorias Abiertas
- Próximas convocatorias
- Resumen de Resultados España 2021-2025
- Actividad den la SGSDla SEDIA



¿Qué es el Programa Europa Digital?

Programa de financiación de la UE centrado en acercar la tecnología digital a las empresas, los ciudadanos y las administraciones públicas.

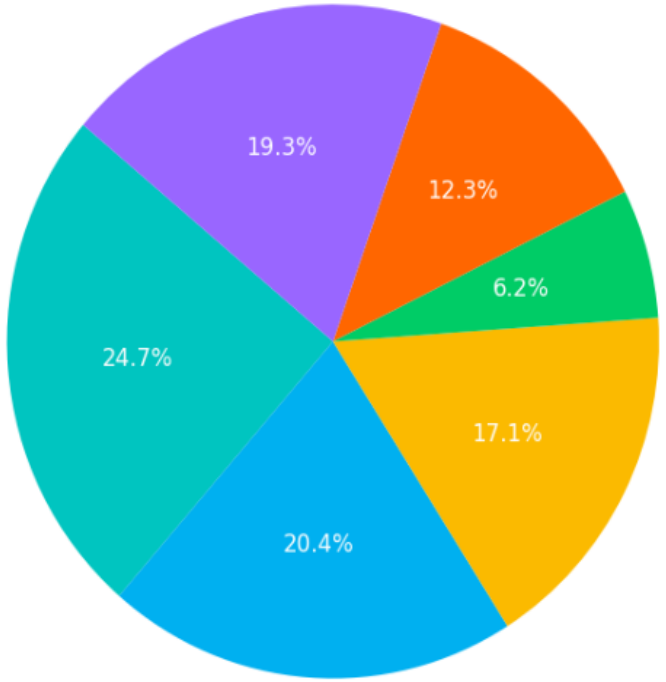
Proporciona financiación apoyando proyectos en ámbitos como: supercomputación, inteligencia artificial, ciberseguridad, capacidades digitales avanzadas y garantía de un amplio uso de las tecnologías digitales en toda la economía y la sociedad.

Objetivos Específicos

8.168.000.000 € distribuidos entre 2021 y 2027

1. Informática de alto rendimiento 2.019.914.000 €
2. Inteligencia Artificial 1.663.956.000 €
3. Ciberseguridad y confianza 1.399.566.000 €
4. Habilidades digitales avanzadas 507.347.000 €
5. Despliegue de la capacidad digital 1.002.217.000 €
6. Semiconductores 1.575.000.000 €

Distribución del presupuesto por actuación



Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021

Reglamento (UE) 2023/1781 del Parlamento Europeo y del Consejo de 13 de septiembre de 2023

Programas de Trabajo

	Gestión de fondos
Programa de trabajo principal	Comisión Europea
Programa de trabajo de Computación de Alto Rendimiento	EuroHPC JU[1]
Programa de trabajo de Centros Europeos de Innovación Digital	Comisión Europea
Programa de trabajo de Ciberseguridad	ECCC[2] y NCC[3]
Programa de trabajo de Semiconductores	Chips JU

[1]Joint Undertaking
[2]Centro Europeo de Competencia en Ciberseguridad (ECCC)
[3]Centro de Coordinación Nacional (NCC)

Tipos de Financiación

Subvenciones Simples	Actuaciones de apoyo a las PYMEs	Actuaciones coordinación y apoyo	Adquisición de capacidades avanzadas	Adquisición	Subvenciones de apoyo financiero	Subvenciones a tanto alzado
• Cubren la mayoría de las actividades • Actividades con terceros posibles pero limitadas. • **50% del total de los costes subvencionables para todos los beneficiarios.**	• Apoyo a PYMEs en la creación y despliegue de capacidades digitales. • **50% del total de los costes subvencionables. PYMEs un porcentaje del 75%.**	• Difusión, creación de redes, servicios de coordinación o apoyo, diálogos políticos, ejercicios y estudios, etc • **100% de los costes subvencionables**	• Compra de bienes y servicios digitales innovadores (tecnologías que aún no están ampliamente disponibles). • **Porcentaje de financiación: 50% del total de los costes subvencionables.**	•Compra de bienes y servicios y subcontr. de tareas. •**Porcentaje de financiación: 50% del total de los costes para todos los beneficiarios.**	•Normas específicas: conflictos de intereses, principios de transparencia, no discriminación, etc. •**100% costes para el consorcio, cofinanciación del 50% del total de los costes para el tercero.**	•Importe a tanto alzado se fija ex ante. •Cubre los costes directos e indirectos. •Si la acción no se ejecuta correctamente, sólo se abonará una parte a tanto alzado. •**50% del total de los costes.**

Costes Subvencionables

A. Costes de personal

- Empleado fijo
- Empleado temporal
- Autónomos
- Propietarios de PYMEs y personas físicas beneficiarias

B. Costes de subcontratación

C. Costes de adquisición

- Viajes y dietas
- Equipamiento
- Otros bienes, obras y servicios

D. Otros costes

- Apoyo financiero a terceros
- Bienes y servicios facturados internamente

E. Costes indirectos

- Para el cálculo de los costes indirectos se aplicará un 7% de los costes directos

Ejecución del Programa

Programa de trabajo » **Convocatoria** » **Topic**

Dos tipos de documentos a considerar

PT

- Prioridades y antecedentes, vínculos con otros programas.
- Subvenciones, contrataciones, instrumentos financieros, acuerdos de contribución, otras actuaciones.
- Ejecución, anexos.

CONV.

- Detalles específicos del topic (presupuesto, descripción, condiciones específicas, tipo de actuaciones, admisibilidad, elegibilidad, evaluación, anexos obligatorios).

Modalidades de financiación

Contratación pública

- Licitaciones.
- Contratos marco.

Subvenciones

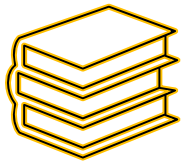
Criterios

- Cumplir con el plazo de presentación.
- Presentar toda la documentación requerida.
- Cumplir requisitos de acceso.
- No tener criterios de exclusión.
- Capacidad financiera y operativa.
- Superar proceso de evaluación.

¿Cómo participar?

Artículo 18 del Reglamento Programa Europa Digital: **Entidades Jurídicas admisibles**

- Aquellas establecidas en un **estado miembro** o país o territorio de ultramar que dependa de un estado miembro.
- **Tercer país asociado al programa** de acuerdo con los artículos 10 y 12 del Reglamento y terceros países **no asociados** al programa **cuya participación sea necesaria** para la consecución de los **objetivos** del Programa.
- **Personas Físicas NO ADMISIBLES.**



Cada convocatoria puede contener condiciones específicas

Prevé la participación de PYMEs

Cofinanciado por la Unión Europea

¿Cómo participar?

Encuentra la convocatoria

Subvenciones del Programa Europa Digital

Licitaciones publicadas por la COM

Búsqueda de socios

Puedes utilizar la **función de búsqueda de socios del Portal**.

Esta función permite:

- Buscar organizaciones que hayan recibido financiación en el pasado,
- Crear y comprobar solicitudes de búsqueda de socios por convocatoria/topic.

Registra la organización

Antes de presentar una solicitud, todos los participantes implicados en la propuesta deben estar registrados en el Registro de participantes y disponer de su Código de Identificación del Participante (número PIC) de 9 dígitos.

Sube tu propuesta

- ☑ Inicia sesión en el Portal y selecciona tu topic.
- ☑ Crea un borrador.
- ☑ Gestiona los participantes.
- ☑ Edita el borrador y el formulario de propuesta (Parte A) y completa toda la información requerida.
- ☑ Sube las plantillas específicas de la convocatoria (Parte B) y el resto de los archivos anexos y presenta tu propuesta.
- ☑ Enviar.

Evaluación de la propuesta

Criterios de adjudicación:

- **Relevancia**
  - Alineación objetivos DEP y contribución
  - Reforzar y asegurar cadena suministros UE
  - Superación obstáculos financieros
- **Ejecución:**
  - Madurez del Proyecto
  - Solidez ejecución y uso eficiente de recursos
  - Capacidad para llevar a cabo el trabajo
- **Impacto**
  - Consecución de resultados y productos esperados
  - Reforzar competitividad, medioambiente, difusión..

Evaluación de la propuesta

2. Comité de evaluación (expertos externos independientes):

- **Condiciones de admisibilidad: Cumplimentar**
  - ☑ Plazos: Fecha límite
  - ☑ Documentación
  - ⊘ Incompletas: Inadmisibles

- **Criterios de elegibilidad:**
  - ☑ Capacidad Financiera y operativa
  - ☑ Depende de la convocatoria

- **Criterios de exclusión:**
  - ⊘ Sanciones administrativas UE
  - ⊘ Según la convocatoria específica.

- **Criterios de adjudicación:**
  - ☑ Relevancia
  - ☑ Ejecución
  - ☑ Impacto

Convocatorias abiertas

Convocatoria	Topic	Apertura indicativa	Presupuesto indicativo
AI/Cloud-to-edge	Apoyo a la secretaría de la Alianza sobre Procesadores y Tecnologías de Semiconductores	T2 – 2025	1 M€
AI/Data para fabricación de IA	Centros de soporte de Data Spaces	T2 – 2025	10 M€
	Soluciones digitales para el cumplimiento normativo a través de los datos	T2 – 2025	8 M€
	Proyecto Multipaís en Agroalimentación	T2 – 2025	15 M€
Aplicar la implementación de la estrategia de IA	GenAI para la administración pública: subvenciones para la contratación pública	T2 – 2025	21 M€
IA/Centros Europeos de Innovación Digital	Consolidación de la Red de Centros Europeos de Innovación Digital (AI EDIHs)	T2 – 2025	170 M€
	Consolidación de la Red de Centros Europeos de Innovación Digital (EDIHs con enfoque reforzado en IA) – países recientemente asociados	T2 – 2025	9 M€
	Finalización de la red inicial de Centros Europeos de Innovación Digital (EDIH)	T2 – 2025	2 M€
Competencias digitales avanzadas	Academias sectoriales de competencias digitales	T2 – 2025	27 M€
Safer internet	Red de Centros de Internet más seguro (SICs)	T2 - 2025	42 M€
	Red Europea de verificadores de datos	T2 - 2025	5 M€

Primer set de convocatorias

Deadline: T2 - 2025

Evaluación: T4 - 2025

Firma: T1- 2026

Próximas convocatorias

Convocatoria	Topic	Apertura Indicativa	Presupuesto Indicativo
Datos para fábricas de IA	Espacio de datos para la fabricación/industria	T4 – 2025	10 MILL
	Espacio de datos para la salud: capacidades de ingesta de datos y servicios de datos para los datos genómicos europeos	T4 – 2025	25 MILL
implementación estrategia IA	Pruebas de la aplicación de GENAI4EU a escala y condiciones reales	T4 – 2025	16 MILL
	Aplicación de la IA: Gen AI para la administración pública- CSA	T4 – 2025	2 MILL
	Implementación de soluciones multimodales de vanguardia basadas en IA en cáncer e imágenes médicas	T4 – 2025	16 MILL
	Bancos de prueba de la UAL World	T4 – 2025	20 MILL
AI/Centros europeos de innovación	Consolidación de la Red de Centros Europeos de Innovación Digital	T4 – 2025	80 MILL
Competencias digitales avanzadas	Academias sectoriales de competencias digitales	T4 – 2025	7 MILL
	ELEVATE: Liga Europea de Academias de Habilidades Digitales Avanzadas	T4 – 2025	8 MILL

Segundo set de convocatorias

Deadline: T4 - 2025

Evaluación: T1 - 2026

Firma: T3- 2026

Actividad en la SGSD en la SEDIA

GOBERNANZA DEL PROGRAMA

Representación de España en el Comité del Programa

- ✓ Representar los intereses de España en las decisiones estratégicas del Programa.
- ✓ **Negociación de los Programas de Trabajo**, asegurando que las prioridades nacionales se queden reflejadas.
- ✓ Colaboración internacional.

Punto de Contacto Nacional en España

- ✓ Intermediario entre la Comisión Europea y los actores nacionales.
- ✓ Información y asistencia sobre el Programa a nivel nacional:
  - **Difusión** de información sobre el Programa.
  - **Asesoramiento y apoyo** a potenciales beneficiarios.

LinkedIn del PCN del Programa Europa Digital

Información sobre los elementos principales del Programa Europa Digital.

Convocatorias: Anuncios, explicaciones y recordatorios sobre las convocatorias del Programa.

Recursos de interés como novedades y encuestas de la Comisión Europea.

Infodays: Invitaciones a participar en infodays y otros eventos sobre el Programa.

Enlaces de Interés

1. Página oficial del Programa
2. Programas de trabajo
3. Reglamento original por el que se establece el Programa Europa Digital (Reglamento DEP)
4. Otros Reglamentos que consultar
   - *Modificación del Reglamento DEP, última versión* (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02021R0694-20230921)
   - Reglamento de chips, por el que se modifica el Reglamento DEP original (https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81291)
5. Manuales de ayuda del Portal de Financiación Licitaciones

NCC-ES INCIBE
Edificio INCIBE. Av. José Aguado 41.
24005 León. España
Tel: +34 987 877 189
nccspain@incibe.es

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPAIN
Land of cybersecurity

AGENDA

- El Fondo Europeo de Defensa
- ¿Por qué es interesante?
- ¿Cómo identificar oportunidades?
- ¿Cuáles serían los próximos pasos?
- ¿Dónde puedo obtener más información?
- Preguntas y respuestas

- **El Fondo Europeo de Defensa**

Objetivos

Plan de Acción Europeo de Defensa (EDAP): *Marco que integra las iniciativas de la UE para el desarrollo de capacidades y el apoyo al sector industrial europeo de la defensa.*

FONDO EUROPEO DE DEFENSA (EDF)

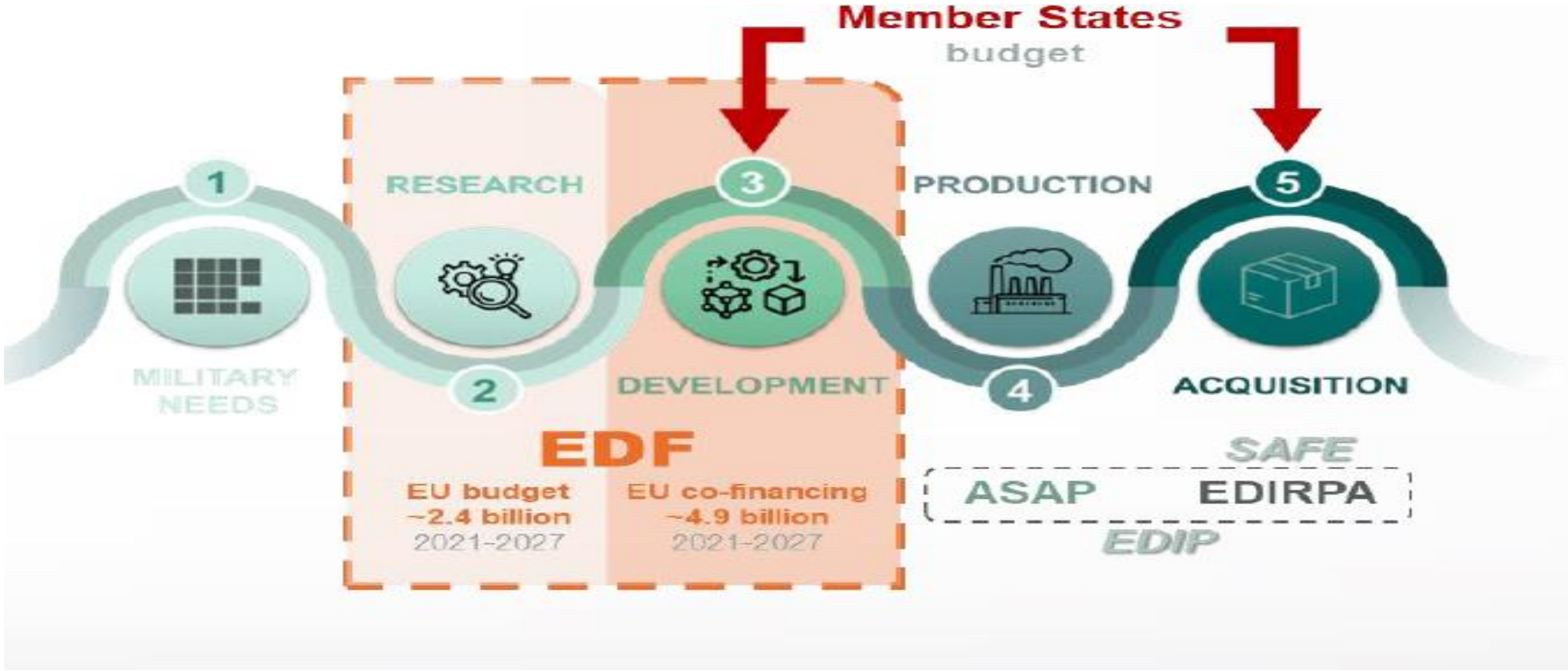
Objetivos EDF :

1. Fomentar la competitividad, eficiencia y capacidad de **innovación** de la **base tecnológica e industrial de la defensa (BTID) europea.**

2. Potenciar la **cooperación transfronteriza.**

1. Fomento de la innovación de la BTID

- Dentro del proceso de desarrollo de capacidades de defensa, el EDF se centra las acciones colaborativas de Investigación y Desarrollo.

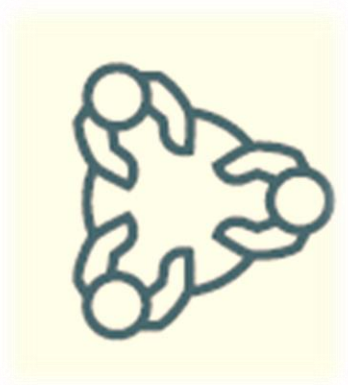


Fuente: https://eur-lex.europa.eu/ES/legal-content/summary/european-defence-fund-2021-2027.html

2. Cooperación transfronteriza

Requisito de cooperación transfronteriza:

- Consorcios de, al menos, tres entidades (públicas o privadas).
- Establecidas en tres Estados miembros distintos o Noruega.
- Excepción: convocatoria de tecnologías disruptivas (dos entidades establecidas en al menos dos Estados miembros o Noruega).



3+3

¿Por qué es interesante?

Financiación del EDF

- El Fondo Europeo de Defensa tiene un presupuesto total de 7.9 mil millones de euros para el periodo 2021-2027.

- El presupuesto está dividido en:
  - Investigación: 2.6 mil millones de euros.
  - Desarrollo: 5.3 mil millones de euros.

2021-2027

EDF
(7.9 M€)

Investigación
(33% - 2.651 M€)

Desarrollo de capacidades
(66% - 5.302 M€)

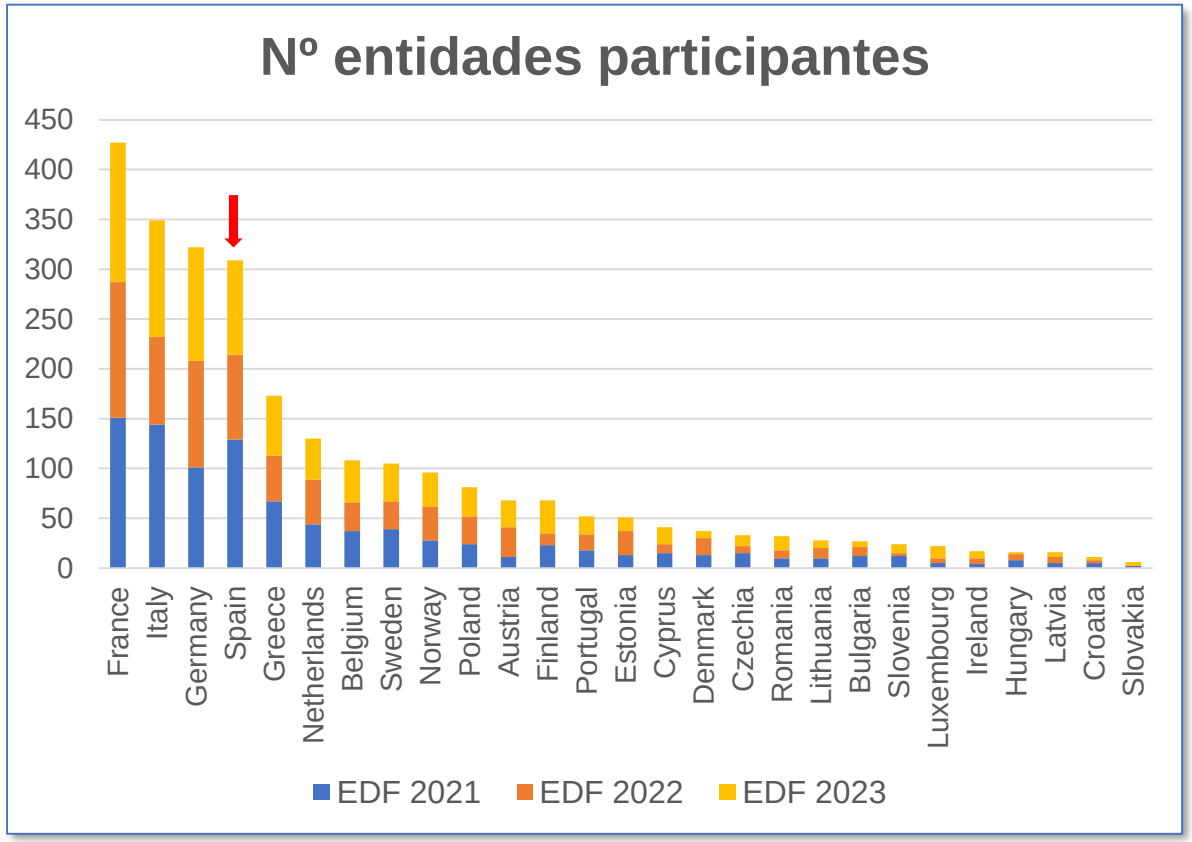
Financiación de la I&D en Defensa

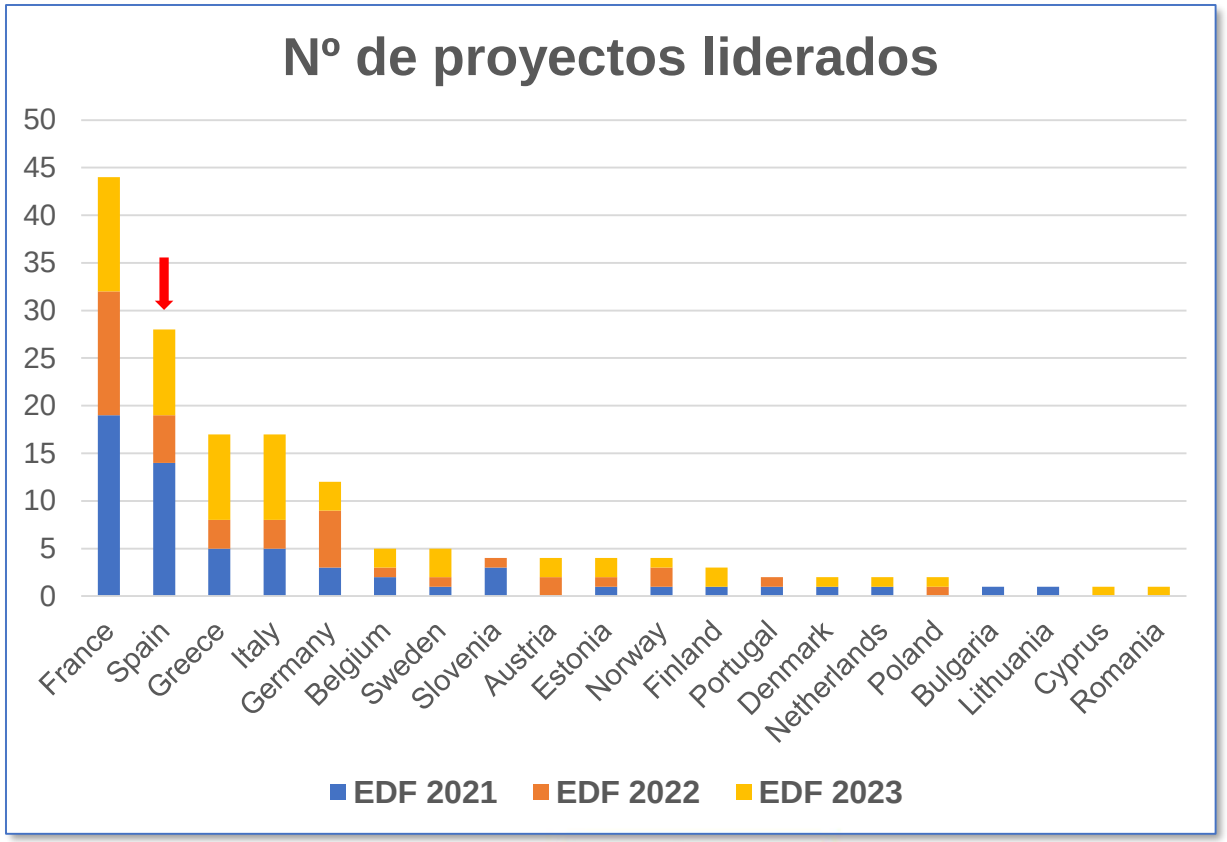
- El presupuesto y número de proyectos financiados ha aumentado.
- Se prevé continuidad en la financiación para la Investigación y Desarrollo en Defensa.

			€ millones	# Proyectos
EDF 2021-2027	€ 8.000 millones	2026	*En preparación. Publicación prevista: diciembre 2025*	
		2025	1.065	Plazo propuestas **16 Oct 2025**
		2024	1.065	*Resultados en mayo 2025*
		2023	1.119	61
		2022	831	41
		2021	1.165	60
EDIDP		2019-20	500	44
PADR		2017-19	90	18

Participación por Estado miembro

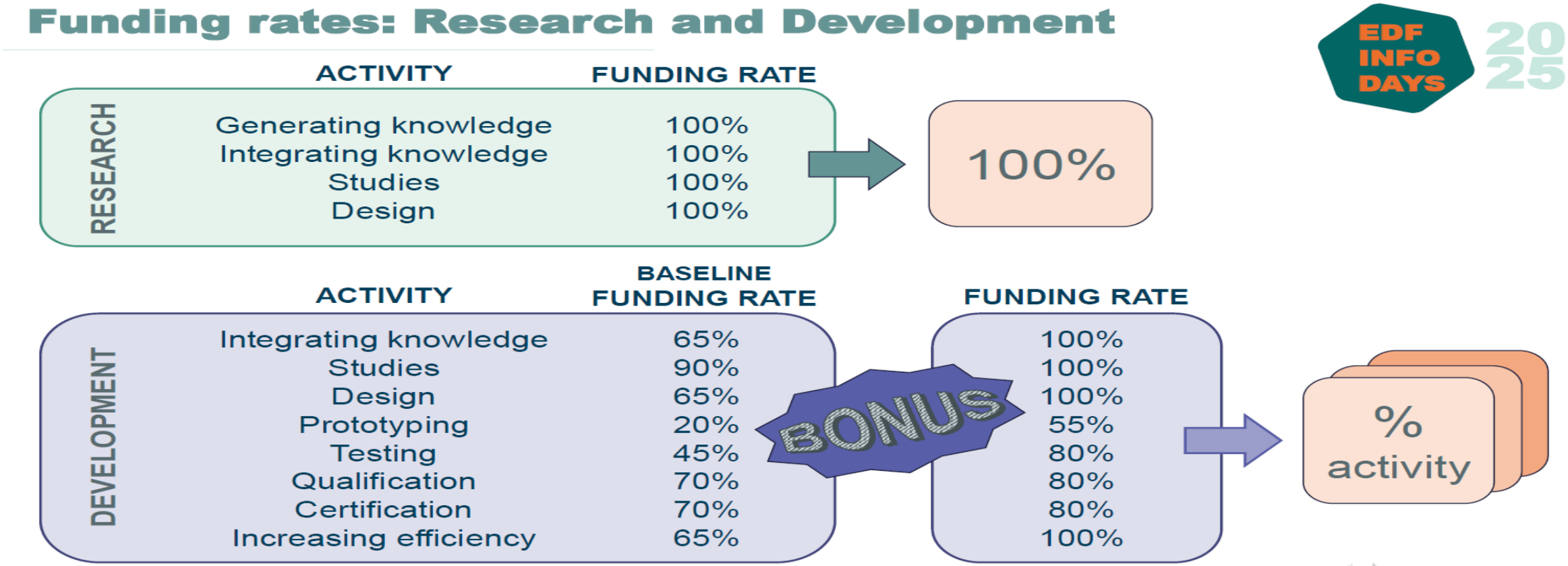
- España es pionera tanto en número de entidades participantes como en número de proyectos liderados.





Financiación de la Comisión

- La financiación de la propuesta dependerá del tipo de convocatoria y de las actividades que cubra.



Fuente: European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission

Bonificaciones

- La Comisión ofrece bonificaciones para incentivar la participación de pymes, pymes transfronterizas, midcaps y vinculación con proyectos PESCO.

The bonus system: development actions

INFO DAYS 2024

CONDITION FOR APPLICATION	VALUE OF THE BONUS
PESCO Bonus	
Action developed in context of the Permanent Structured Cooperation (PESCO)	+10% for **all activities** in the action
'Mid-cap' bonus	
% eligible costs allocated to 'Midcaps' established in the EU (or NO) ≥ 15%	+10% **for the activity**
SME Bonus	
% eligible costs allocated to 'SMEs' established in the EU (or NO) ≥ 10%	% of eligible costs allocated to '**non cross-border SMEs**' established in the EU or NO (maximum 5%) + 2 x % of eligible costs allocated to '**cross-border SMEs**' established in the EU or NO

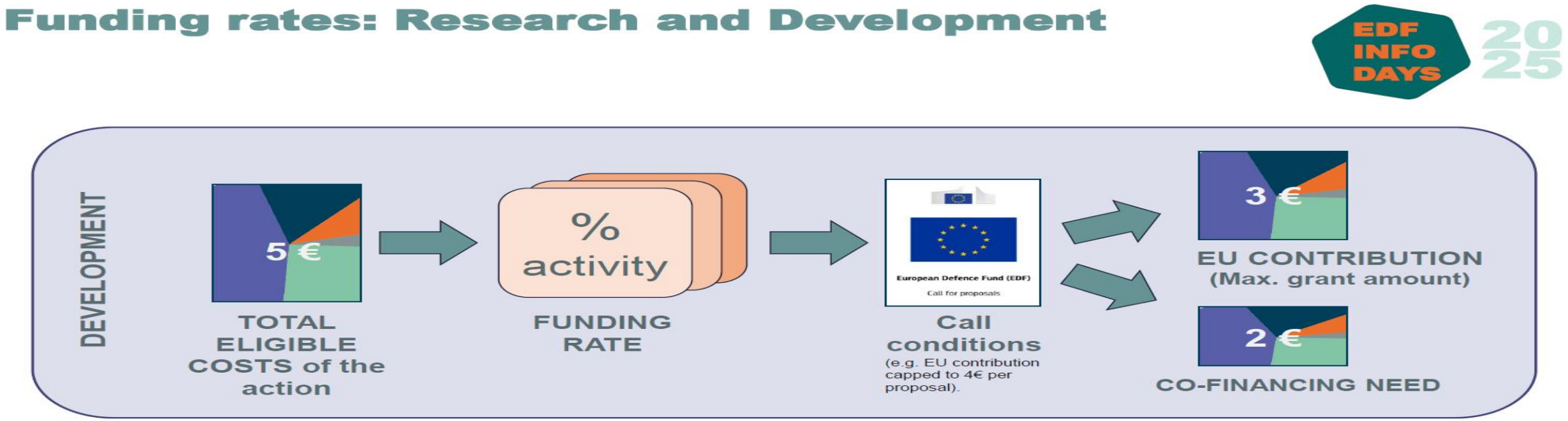
#EUDefenceIndustry

Fuente: European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Cofinanciado por la Unión Europea

Financiación del EDF

- Los costes elegibles que no sean cubiertos por la Comisión deberán ser cubiertos por co-financiación de sus gobiernos y/o las empresas del consorcio.
  - La propuesta tiene que demostrar que el 100% de los costes elegibles están cubiertos.



Fuente: European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission

¿Cómo identificar oportunidades?

Programa de Trabajo - Estructura

- Cada propuesta será enviada para un tipo de convocatoria y un tema específico.

Ejemplos EDF2025

		Tipo de convocatoria		Categoría/temática			
Fund	**Year**	**Type of Grant**	**Research vs. Development**	**Category**	**Topic**	**Other**	**Name**
EDF	2025	**-** (Actual Cost)	**RA** (Research)	ENEREN V	PSR	-	EDF-2025-**RA**-ENERENV-PSR: **P**ropulsion **s**ystem for next generation **r**otorcrafts
EDF	2025	**LS** (Lump Sum)	RA (Research)	ENEREN V	NH2PS	**STEP**	EDF-2025-**LS**-RA-SI-ENERENV-NH2PS-STEP: **N**aval **h**ybrid propulsion and **p**ower **s**ystems
EDF	2025	**-** (Actual Cost)	**DA** (Development)	ENEREN V	APEM	-	EDF-2025-**DA**-ENERENV-APEM: **A**ircraft **p**ropulsion and **e**nergy **m**anagement systems

Programa de Trabajo - Convocatorias

- El EDF25 tiene 8 convocatorias.

★Es importante entender los requisitos, financiación, actividades que cubren, etc. de cada convocatoria.

EDF 2025 Call structure

Type of Action and Type of Model Grant Agreement as central elements in Work Programme structuring (*e-grants*)

Type of Action	○ EDF-RA: European Defence Fund - **Research Action** ○ EDF-LSRA: European Defence Fund - **Lump Sum-Research Action** ○ EDF-DA: European Defence Fund - **Development Action** ○ EDF-LSDA: European Defence Fund - **Lump sum-Development Action** ○ EDF-RA-SGA: European Defence Fund - **Specific Grant Agreement***
Type of Model Grant Agreement	○ EDF-AG: European Defence Fund - **Action Grant** ○ EDF-AG-LS: European Defence Fund - **Action Grant-Lump Sum**
Legibility	○ Policy objectives pursued ○ Set of homogenous eligibility conditions

8 competitive R&D calls

EDF-2025-RA
EDF-2025-LS-RA-SI
EDF-2025-LS-RA-CHALLENGE
EDF-2025-LS-RA-DIS
EDF-2025-LS-RA-SMERO
EDF-2025-DA
EDF-2025-DA-SI
EDF-2025-LS-DA-SME

*SGA awarded without call for proposals in relation to a Framework Partnership Agreement (FPA)

Fuente: European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission

Programa de Trabajo - Categorías

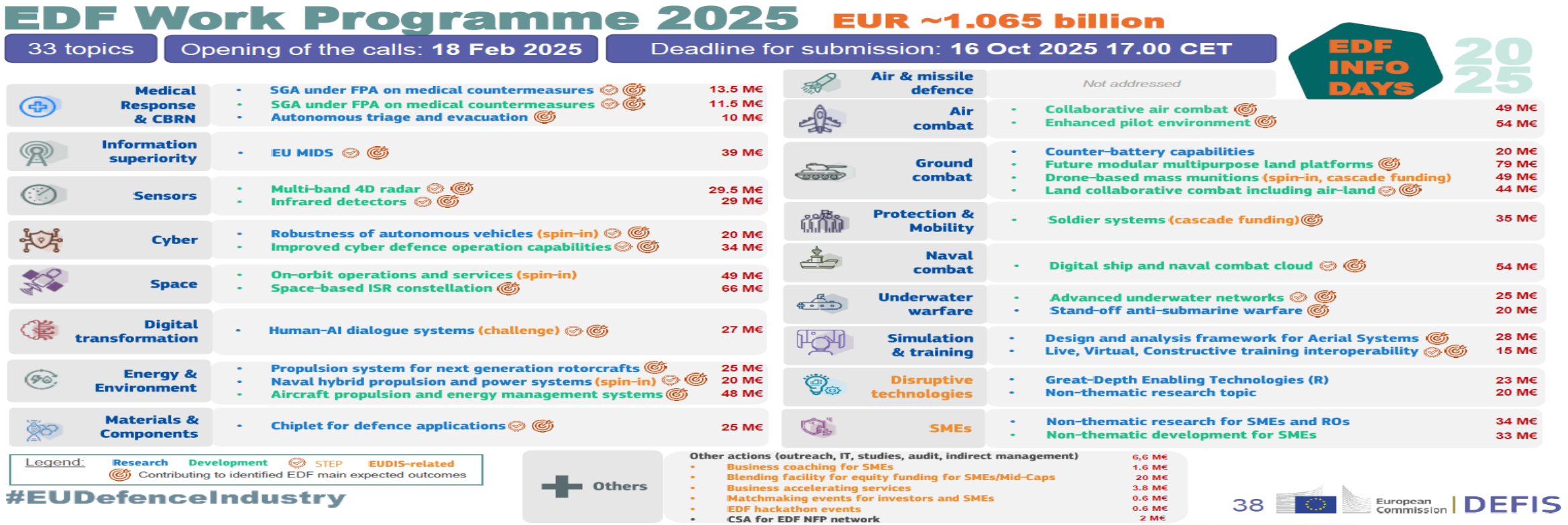
- El Programa de Trabajo se divide en Categorías.

Fuente: [European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission]

Programa de Trabajo - Temáticas

- Cada propuesta se remite para cada uno de estos temas (“topics”) dentro de las categorías.

★ Identificar áreas en las que la entidad puede aportar valor.

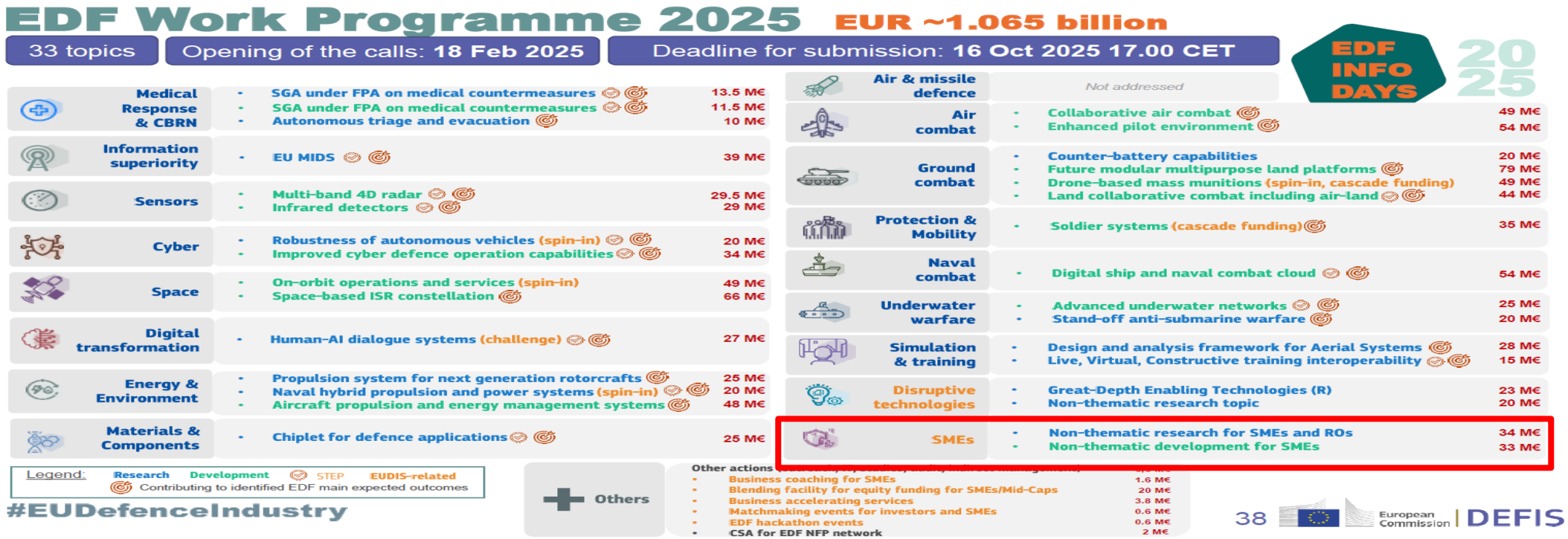


Fuente: [European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission]

Programa de Trabajo - PYMES

- Dentro de la categoría de SMEs, hay dos "no temáticas" para pymes.

★Tener en cuenta alta competencia.



Fuente: [European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission]

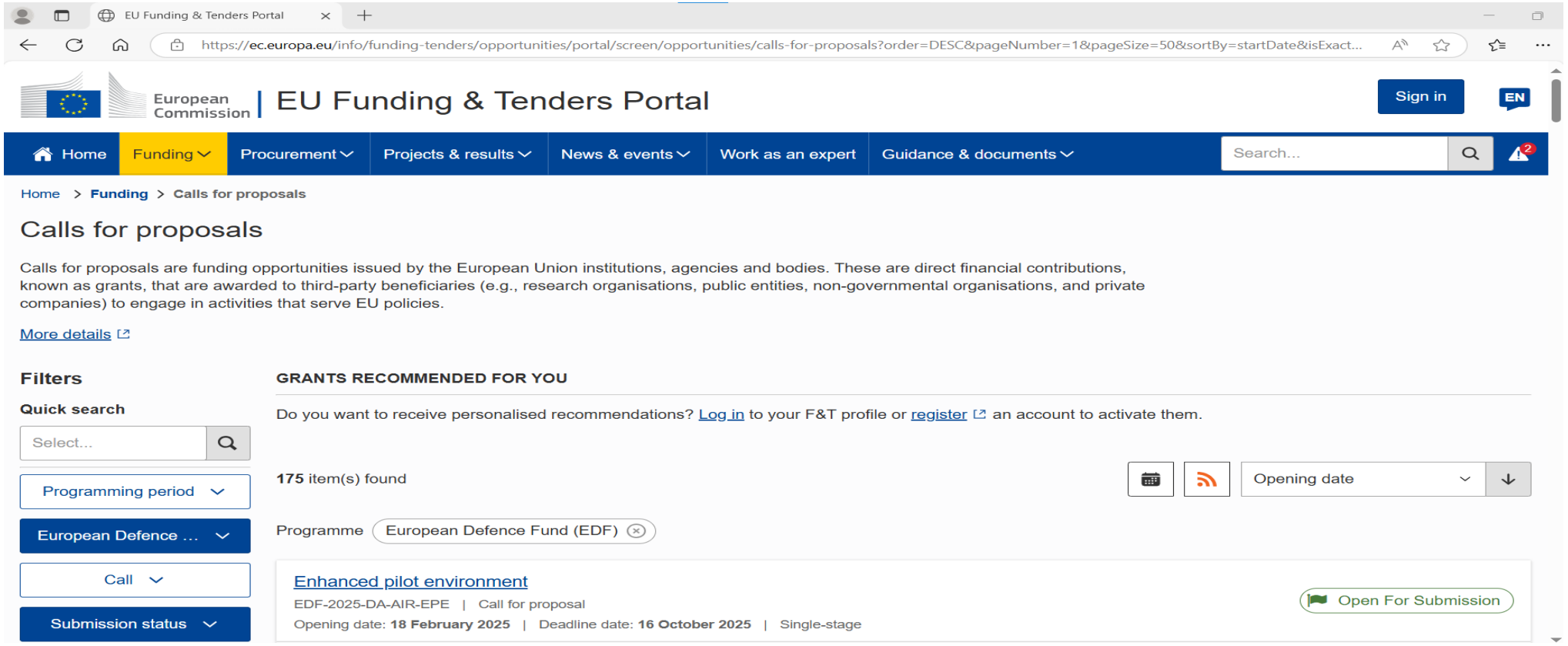
¿Cuáles son los próximos pasos?

Calendario y fechas clave EDF25

- La fecha límite para envío de propuestas de la Comisión es el 16 de octubre

Convocatorias y remisión de propuesta

- La información de las convocatorias y la remisión de las propuestas se hace a través de la página EU Funding & Tenders Portal de la Comisión.



Fuente: EU Funding & Tenders Portal

Call for proposals

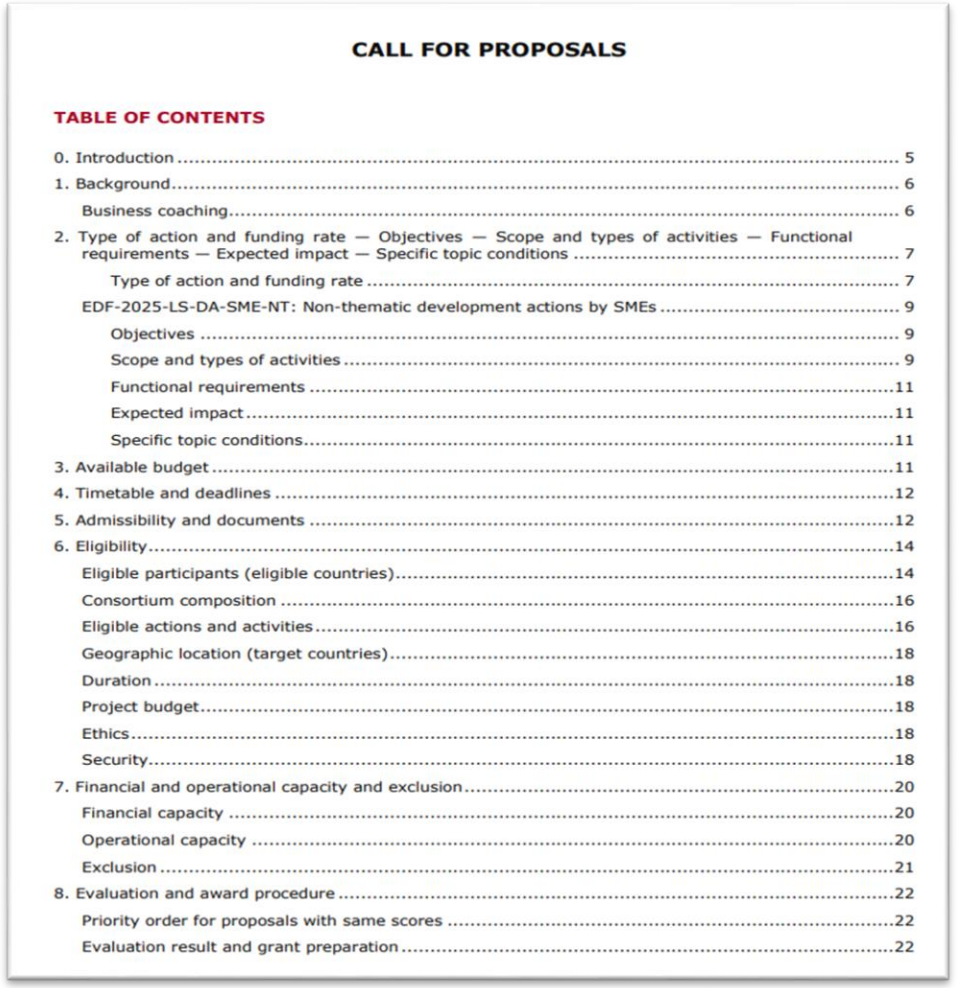
EJEMPLO CONVOCATORIA 2025

European Defence Fund (EDF)

Call for proposals

EDF-2025-LS-DA-SME

Call for EDF development actions, dedicated to **SMEs**, implemented through lump sum grants



CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction 5
1. Background 6
Business coaching 6
2. Type of action and funding rate — Objectives — Scope and types of activities — Functional requirements — Expected impact — Specific topic conditions 7
Type of action and funding rate 7
EDF-2025-LS-DA-SME-NT: Non-thematic development actions by SMEs 9
Objectives 9
Scope and types of activities 9
Functional requirements 11
Expected impact 11
Specific topic conditions 11
3. Available budget 11
4. Timetable and deadlines 12
5. Admissibility and documents 12
6. Eligibility 14
Eligible participants (eligible countries) 14
Consortium composition 16
Eligible actions and activities 16
Geographic location (target countries) 18
Duration 18
Project budget 18
Ethics 18
Security 18
7. Financial and operational capacity and exclusion 20
Financial capacity 20
Operational capacity 20
Exclusion 21
8. Evaluation and award procedure 22
Priority order for proposals with same scores 22
Evaluation result and grant preparation 22

Funding and Tenders Portal: Call document for the "Call for EDF development actions, dedicated to SMEs, implemented through lump sum grants"

Cofinanciado por la Unión Europea

¿Dónde puedo obtener más información?

Recursos de DG DEFIS

Grabaciones de los Info Days

EDF Info Days 2025

The European Commission is pleased to announce that the upcoming edition of the EDF Info Days will took place on 2 - 3 April 2025 in Brussels and online.

The **EDF Info Days 2025** gathered more than **5000 participants** from all around the EU, Norway and beyond both on-site and online.

It was a unique opportunity to learn all what is needed to apply to EU Funding & Tenders Portal for proposals and to discover and network with potential partners in future EDF projects.

The slides of Day 1 (plenary info session) are now **available here.**

Watch the recording of the info sessions of day 1:

- EDF25 - Gold Hall - Welcome & Introduction
- EDF25 - Gold Hall - Overview of the 2025 calls, including Q&A
- EDF25 - Gold Hall - EDF evaluation process and best practices
- EDF25 - Gold Hall - Financial aspects, supportive actions and concluding remarks

Tutoriales

EDF tutorials

Learn more about some of the European Defence Fund specific features via our set of tutorials.

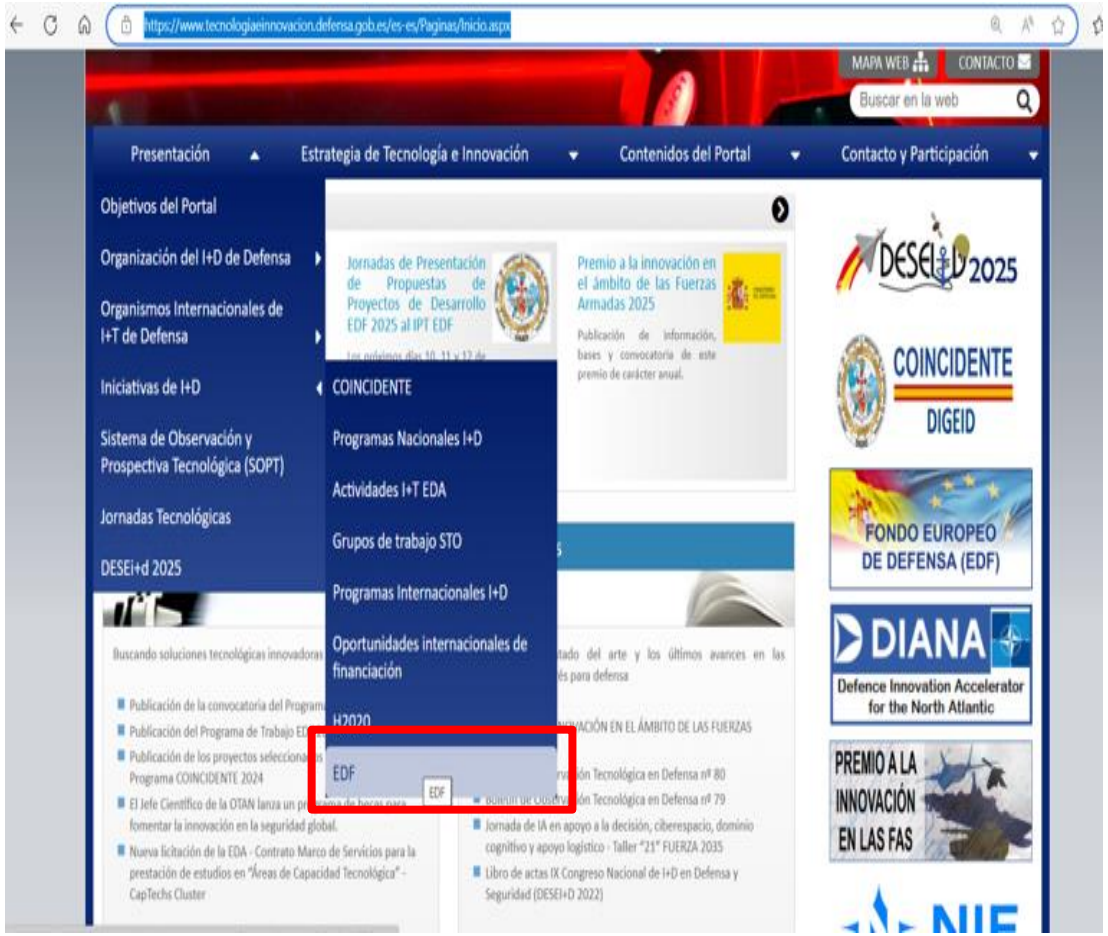
Financial aspects

- Funding rates (video, slides)
- Co-financing declaration (video, slides)
- Co-financing in Detailed budget tables (video)
- Type of grants: Form of Funding (video, slides)
- Costs categories and eligible costs (video, slides)
- Actual indirect costs (video, slides)
- Detailed budget tables (video, slides)
- Payment scheme (video, slides)

Fuente: European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission

Recursos del Ministerio de Defensa

Sección dedicada al EDF dentro del Portal



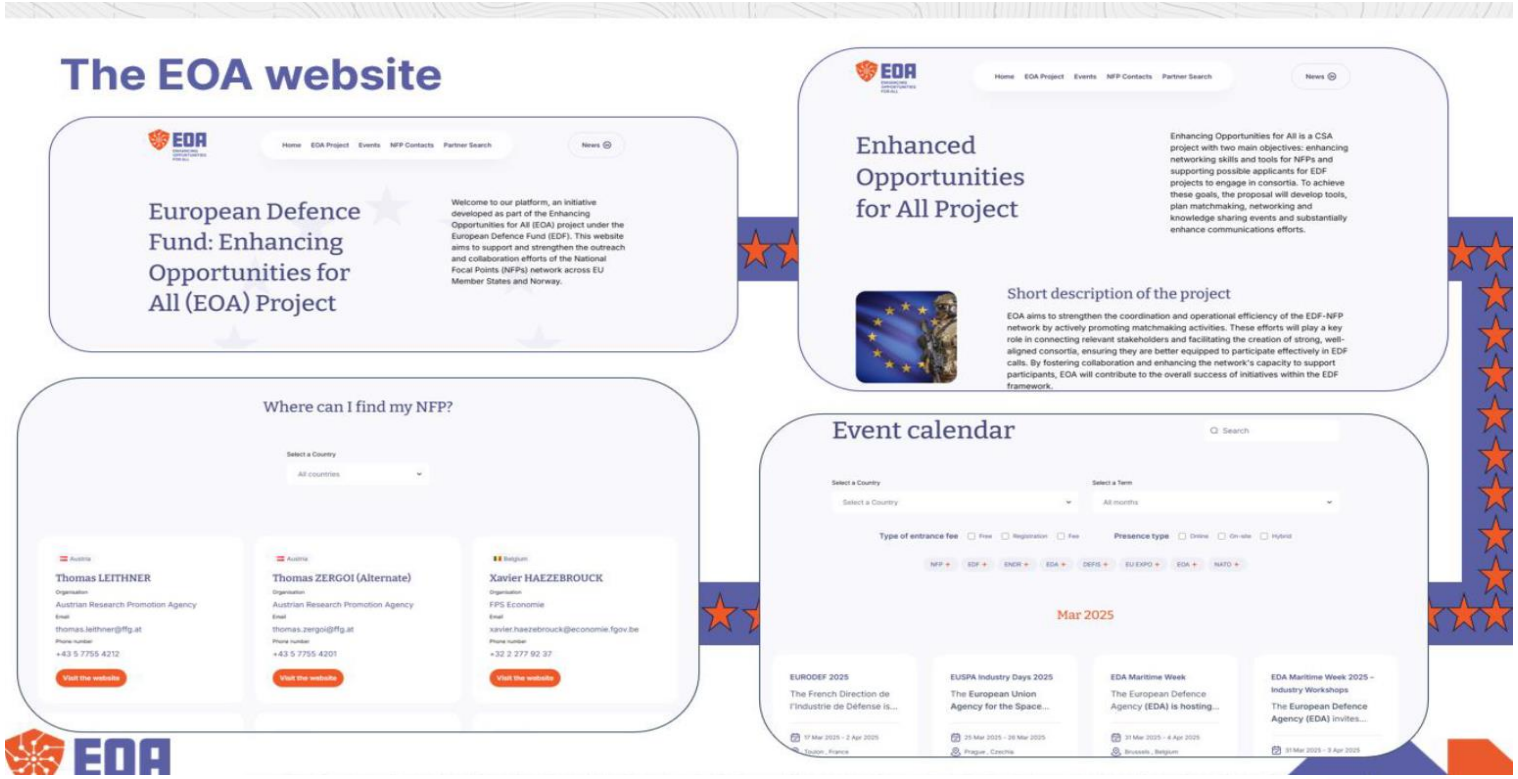
Grabación de la sesión dentro del apartado de Noticias

Fuente: https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Paginas/Inicio.aspx

Otros recursos – EOA website

- La red de National Focal Points facilita información través de la página del proyecto "Enhancing Opportunities for All" (EOA).

EOA website

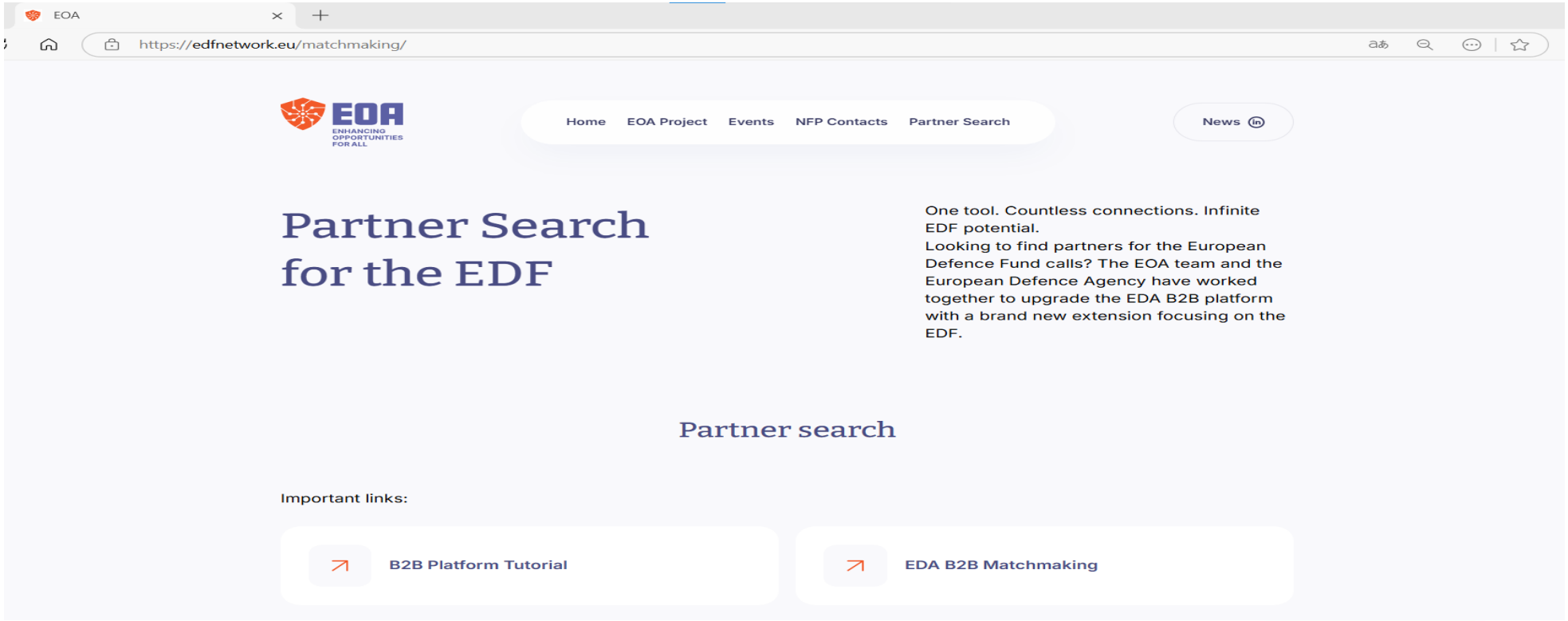


Fuente: https://edfnetwork.eu/eoa-projects/

Otros recursos – EOA Partner Search

- La red de National Focal Points, a través del proyecto EOA y en colaboración con la EDA, ha creado una herramienta de búsqueda de socios específica para EDF.

EOA Partner Search



Fuente: https://edfnetwork.eu/eoa-projects/

Otros recursos – EOA LinkedIn

- Seguir la página de LinkedIn para estar actualizado de todas las novedades: https://www.linkedin.com/company/eoa-enhancing-opportunities-for-all/

Página de LinkedIn del EOA

Enlaces de interés

Qué es EDF y cómo funciona

Página web oficial de la Comisión sobre EDF:
https://ec.europa.eu/defence-industry-space/eu-defence-industry/european-defence-fund-edf_en

NOTA: de especial interés en esta página son las presentaciones y vídeos de los **Info Days** de la Comisión Europea sobre cada convocatoria anual EDF

Convocatorias EDF y otras oportunidades de financiación

Portal "Funding & Tender opportunities" de la Comisión:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/edf

Información genérica sobre financiación y subvenciones en defensa y espacio:
https://ec.europa.eu/defence-industry-space/funding-and-grants_en

Web oficial de la dirección DEFIS de la Comisión Europea:
https://ec.europa.eu/info/departments/defence-industry-and-space_es

Eventos y búsqueda de socios

Eventos que organiza la Comisión Europea:
https://ec.europa.eu/defence-industry-space/events-0_en

Plataforma B2B de la EDA:
https://b2bplatform.eda.europa.eu

NOTA: las entidades también pueden buscar socios o indicar su intención de participar en el propio portal "Funding & Tender" de la Comisión, dentro de cada uno de los *topics* de las convocatorias.

Gestión de la participación nacional en EDF

Información en el Portal de Tecnología e Innovación del Ministerio de Defensa:
https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/ImasD/Paginas/EDF.aspx

Procedimiento Nacional para Participar en el EDF:
https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/ImasD/Documents/Procedimiento%20Gesti%C3%B3n%20de%20la%20Participaci%C3%B3n%20Nacional%20EDF.pdf

Requisitos nacionales para poder participar

1- Alta en el registro de las empresas y organismos de la DGAM (MINISDEF)
https://www.defensa.gob.es/portalservicios/servicios/industriadefensa/registroempresas
Emails: registroempresas@oc.mde.es / soporte.industria@oc.mde.es

2- Disponer de Habilitación de Seguridad
https://www.cni.es/oficina-nacional-de-seguridad
Email: seguridad_industrial@oc.mde.es

3- Obtener licencias de exportación
Registro Especial de Operadores de Comercio Exterior (REOCE):
https://comercio.gob.es/ImportacionExportacion/Regimenes/Paginas/FAQS/reoce.aspx

E-mails de contacto en el MINISDEF

Para resolver cualquier duda, presentar una propuesta o solicitar una cita:
- Proyectos de desarrollo: iniciativasedf@mde.es
- Proyectos de investigación: cooperacionid@mde.es

Para proyectos liderados por consorcios de otras naciones
La nación líder debe ponerlo en conocimiento del MINISDEF:
Email: ES.UE.MULTI@mde.es

E-mails de contacto en el MINISDEF

- Para resolver dudas o presentar una propuesta:
  - Proyectos de Desarrollo: iniciativasedf@mde.es
  - Proyectos de Investigación: cooperacionid@mde.es
  - Preguntas generales EDF: ES.UE.MULTI@mde.es

Preguntas y respuestas

NCC-ES INCIBE
Edificio INCIBE. Av. José Aguado 41.
24005 León. España
Tel: +34 987 877 189
nccspain@incibe.es

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPAIN
Land of cybersecurity

Oportunidades de financiación en Ciberseguridad en Horizonte Europa- Clúster 3 – Convocatoria 2025

Maite Boyero Egido

Representante y NCP Clúster 3

Maite.boyero@cdti.es

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Cofinanciado por la Unión Europea
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PUBLICA
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI INNOVACIÓN

HOME

CNECT

International affairs

Issues related to security and migration have an international dimension. That is why, the EU works together with countries across the globe and international organisations on different topics, such as: border management, migration and mobility, fighting terrorism and migrant smuggling.

Law enforcement cooperation

To combat cross-border crime and terrorism, law enforcement authorities of EU countries cooperate and exchange information, such as passenger information collected by airlines (PNR). The agency Europol supports countries in this information sharing.

Internal security

From combatting terrorism to fighting trafficking in human beings and organised crime – by harmonising security related rules across EU countries the EU becomes a safer place. Latest focus is also on combatting cybercrime and preventing cyberattacks.

Digital Economy and Society

Research and Innovation

PILAR 1 – CIENCIA EXCELENTE	25.011
ERC - Consejo Europeo de Investigación	16.004
MSCA - Acciones Marie Skłodowska-Curie	6.602
Infraestructuras de investigación	2.406

PILAR 2 - RETOS MUNDIALES Y COMPETITIVIDAD INDUSTRIAL EUROPEA	53.516
Clúster 1 - Salud	8.246
Clúster 2 - Cultura, creatividad y sociedad inclusiva	2.280
Clúster 3 – Seguridad civil	1.596
Clúster 4 - Digital, industria y espacio	15.349
Clúster 5 - Clima, energía y movilidad	15.123
Clúster 6 - Alimentación, bioec. recursos naturales, agricultura y MA	8.952
JRC – Centro Común de Investigación	1.970

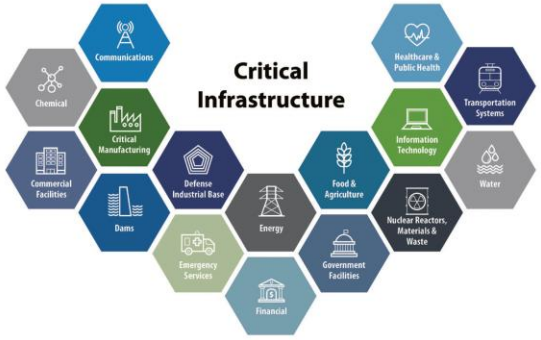
PILAR 3 – INNOVACIÓN ABIERTA	13.597
EIC- Consejo Europeo de Innovación	10.105
Ecosistemas de innovación europea	527
EIT - Instituto Europeo de Innovación y Tecnología	2.965

Ampliar la Participación y Fortalecer el Espacio Europeo de Investigación	3.393
Ampliar la participación y difundir la excelencia	2.955
Reformar y mejorar el sistema europeo de la I+i	438

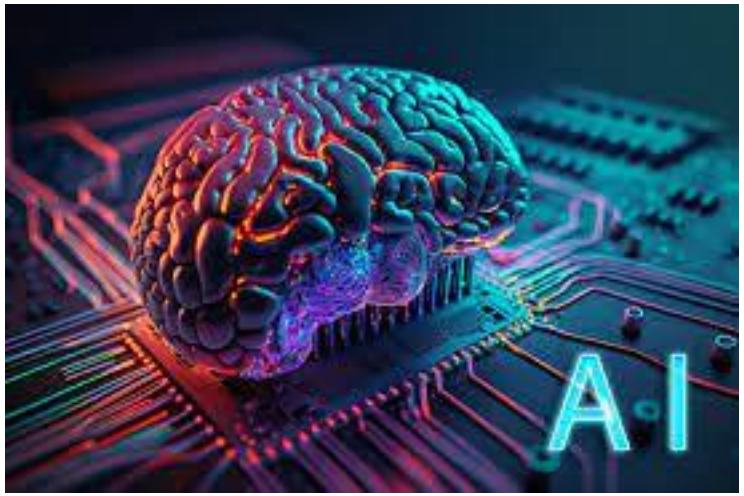
Presupuesto en precios corrientes.

Retos de Seguridad

- ✓La investigación en seguridad como respuesta a retos **geo-políticos, económicos y de seguridad**
- ✓Sinergias / Dual-use research

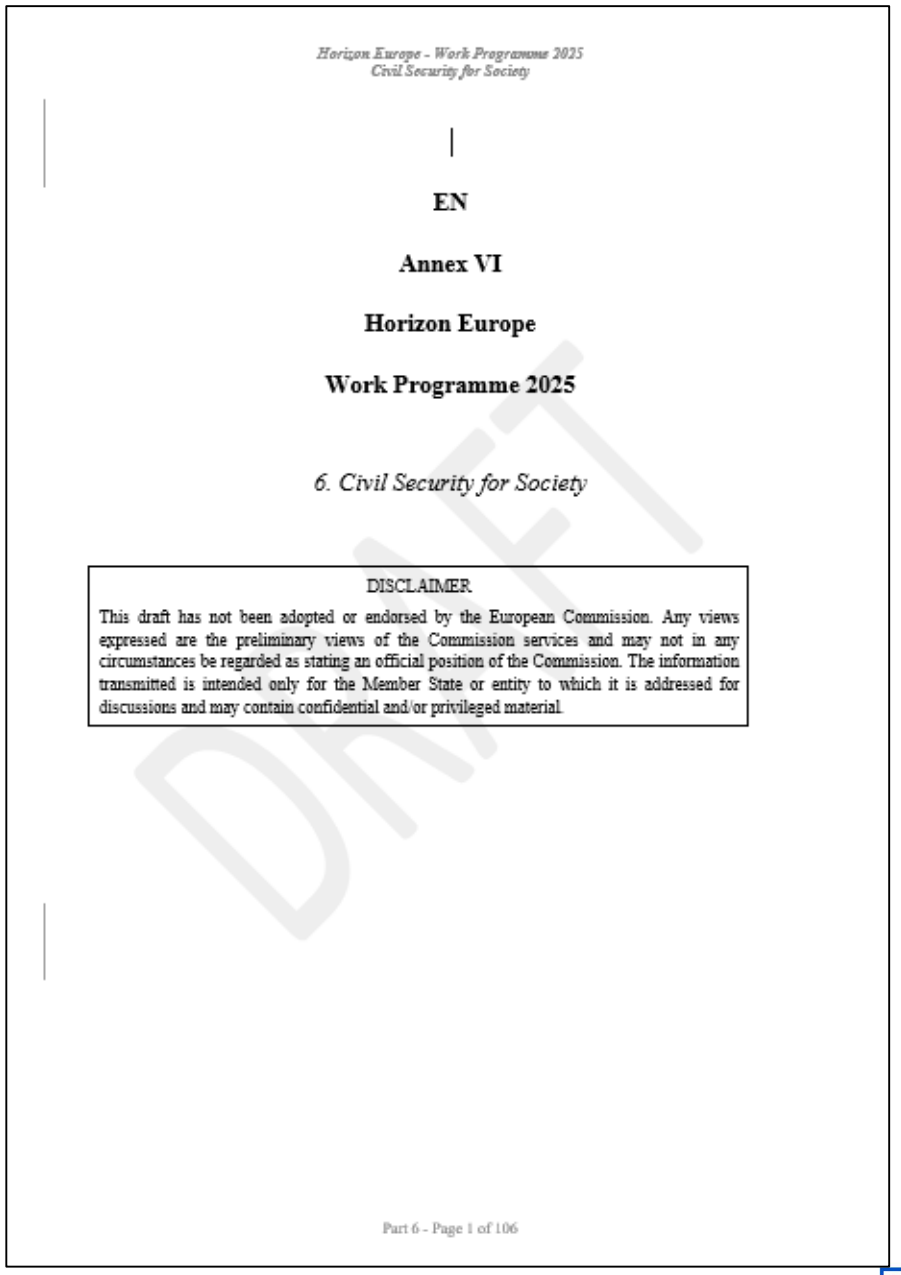


Tendencias tecnológicas y tecnologías críticas



Horizon Europe

- *Horizon Europe is the EU's flagship research and innovation program.*
- *Budget of nearly €100 billion.*
- *Horizon Europe addresses societal challenges and promotes scientific excellence*
- ***Cybersecurity topics part of "Civil Security for Society" WP in Cluster 3***
- ***Horizon Europe calls for cyber focus on Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures & Cryptography, Privacy, Post-quantum cryptography, AI for Cybersecurity, etc.***



Horizon Europe - Work Programme 2025
Civil Security for Society

EN

Annex VI

Horizon Europe

Work Programme 2025

6. Civil Security for Society

DISCLAIMER

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and may contain confidential and/or privileged material.

DRAFT

Part 6 - Page 1 of 106

Convocatoria 2025:

- Documento aprobado: wp-6-civil-security-for-society_horizon-2025_en.pdf
- Abrió el 12 de Junio de 2025
- **Cierra: 12 Noviembre de 2025*** 5pm CET

Algunos detalles:

- Principalmente: **"Open Topics"**
- Se financiará + de 1 propuesta por topic
- Total presupuesto convocatoria: ~ 200 M€, y sólo en CS: 90M€
- Rol de los Usuarios finales es fundamental

Destination “Increased cybersecurity”

- Apoyar las **capacidades tecnológicas de la UE** invirtiendo en investigación e innovación en ciberseguridad para reforzar aún más su liderazgo, autonomía estratégica, soberanía digital y resiliencia;
- Ayudar a proteger sus infraestructuras y mejorar su capacidad para **prevenir, protegerse contra, responder, resistir, mitigar y recuperarse de incidentes cibernéticos e híbridos**, especialmente dada la actual situación de cambio geopolítico;
- Apoyar **la competitividad europea en ciberseguridad y la autonomía estratégica europea, protegiendo los productos de la UE y las cadenas de suministro digitales,** así como los servicios e infraestructuras críticas de la UE (tanto físicas como digitales) para asegurar su solidez y continuidad ante severas interrupciones;

Y además…

- Fomentar el desarrollo de la Comunidad del Centro de Competencia Europeo en Ciberseguridad (ECCC)
- Se prestará especial atención a las pequeñas y medianas empresas (PYMEs), que juegan un papel crucial en el ecosistema de ciberseguridad y en la competitividad general del mercado único digital de la UE, promoviendo la seguridad y la privacidad 'desde el diseño' *(Cybersecurity-by-design)* en tecnologías existentes y emergentes.

Topics – call 2025	EUR (M€) Per topic	EUR (M€) per grant	ToA / TRL	Eligibility Conditions	Observations
HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications	40	12-14	RIA	Only **legal entities established in MS and AC**, and **not directly or indirectly controlled by a non-eligible country** or entity from a non-eligible country.	Proposals should address AT LEAST ONE of the next expected outcomes: a. Developing, training and testing of Generative AI models for monitoring, detection, response and self-healing capabilities in **digital processes, and systems against cyberattacks**, including adversarial AI attacks. b. Development of Generative AI tools and technologies **for continuous monitoring, compliance and automated remediation.** Participation of SMEs is encouraged.
HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity	23,55	4,5-6 	IA / 4-7		Participation of start-ups and SMEs with an active role in the implementation would be considered an asset.
HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies	11	3-4 	RIA	Avoid the participation of the so called “high-risk supplier entities”.	Engagement of SMEs is encouraged**.**

HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications

- Las propuestas deben abordar al menos uno de los siguientes resultados esperados:
  - a. Desarrollo, formación y prueba de modelos de IA Generativa para la monitorización, detección, respuesta y capacidades de recuperación en procesos y sistemas digitales contra ciberataques, incluyendo ataques de IA adversaria.
    - i. Detección y análisis de amenazas y anomalías avanzadas
    - ii. Medidas de seguridad adaptativas
    - iii. Autenticación y control de acceso
  - b. Desarrollo de herramientas y tecnologías de IA Generativa para la monitorización continua, el cumplimiento de normativa de forma automatizada. Éstas deben considerar aspectos legales de la regulación de la UE y nacional, así como aspectos éticos y de privacidad.
    - i. Aplicación de reglamentos nacional y de la UE en sistemas digitales
    - ii. Adaptación a un entorno dinámico

HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity

- Las propuestas deben abordar al menos dos de los siguientes resultados esperados:
  - Conciencia situacional mejorada a través de marcos, herramientas y servicios avanzados de inteligencia sobre amenazas cibernéticas, así como evaluaciones de riesgo de ciberseguridad de cadenas de suministro críticas realizadas en la UE,
  - Marcos, herramientas y servicios para la preparación contra amenazas cibernéticas y híbridas en tecnología de la información y comunicación (TIC) y tecnología operativa (OT), incluidos ejercicios de ciberseguridad,
  - Ampliación de la funcionalidad del Centro de Operaciones de Seguridad/Equipo de Respuesta a Incidentes de Seguridad Informática (SOC/CSIRT) a través de herramientas y servicios avanzados para la detección, análisis, manejo de incidentes, incluyendo respuesta e informes,
  - Desarrollo de instalaciones de pruebas y experimentación para herramientas y procesos avanzados de ciberseguridad operativa, incluida la creación de gemelos digitales para infraestructuras críticas y entidades esenciales e importantes según lo definido en NIS2,
  - Desarrollo e implementación piloto, servicios y herramientas de gestión de crisis cibernéticas transversales y/o transfronterizas, frameworks, servicios y herramientas dirigidos a mecanismos y procesos para una cooperación operativa mejorada entre entidades del sector público (red CSIRT, EU-CyCLONe). Incorporación de servicios / entidades críticas son bienvenidas

HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies (1/2)

- Los proyectos deben abordar uno o varios de los siguientes aspectos:
  - Desarrollo de tecnologías robustas, escalables y confiables para mantener la privacidad dentro de marcos de intercambio de datos federados y seguros, así como en el procesamiento de datos personales e industriales, integrados en sistemas de entornos reales.
  - Desarrollos que preserven la privacidad para soluciones de intercambio de datos, incluyendo el intercambio de información sobre ciberamenazas que preserva la privacidad, y en entornos colaborativos donde se intercambien datos sensibles.
  - Integración de la privacidad desde el diseño en el núcleo de los procesos de desarrollo de software y protocolos, asegurando que las herramientas criptográficas y firmas digitales mejoran la privacidad y que los esquemas de autenticación de usuarios sean ágiles y modulares, para facilitar una transición hacia algoritmos criptográficos post-cuánticos.
  - Desarrollo de tecnologías que mejoran la privacidad para los usuarios de dispositivos restringidos.

HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies (2/2)

- Contribución a los espacios de datos europeos conformes con la GDPR para servicios digitales e investigación, como los relacionados con datos de salud, alineándose con los topics de Clúster 4
- Desarrollo de tecnologías y soluciones que mejoren la privacidad, para beneficiar los requisitos de los ciudadanos y las empresas, incluyendo a las PYMES.
- Desarrollo de tecnologías que mejoren la privacidad y estén basadas en blockchain y descentralizadas, para preservar la confidencialidad, integridad y autenticidad de las transacciones y activos digitales.
- Investigación de la usabilidad y experiencia del usuario de las tecnologías que mejoran la privacidad y exploración de formas de diseñar sistemas que sean seguros y amigables para el usuario.

Topics – call 2025	EUR (M€) Per topic	EUR (M€) per grant	ToA	Eligibility Conditions	To take into account…
HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives	4	2-3 	RIA	Only **legal entities established in MS and AC**, and **not directly or indirectly controlled by a non-eligible country** or entity from a non-eligible country.	Eventually, combination with AI, or on solely AI-based approaches, are welcome.
HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms	6				
HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	6				Consortia including RTOs, relevant public entities & industry to ensure that solutions meet real-world are also welcome.

HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives

- **Los proyectos deben contribuir a uno o varios de los siguientes resultados esperados:**
  - Avances en la comprensión de la robustez cuántica de diversos algoritmos que actualmente sustentan la seguridad de los sistemas criptográficos actuales y futuros post-cuánticos;
  - Nuevos algoritmos cuánticos con una potencialidad cuántica significativa para problemas matemáticos basados en redes, y códigos
  - Soliciones basadas en IA para ayudar a descubrir vulnerabilidades de problemas matemáticos basados en redes u otras clases de problemas matemáticos;
  - Criptoanálisis
  - Parámetros para crear un conjunto de blockchain criptográfico para la ciberseguridad post-cuántica y el diseño de sistemas criptográficos post-cuánticos con una seguridad mejorada contra ataques cuánticos o basados en IA.

HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms

- **Los proyectos deben contribuir a uno o varios de los siguientes resultados esperados:**
  - Diseño e implementación de algoritmos de criptografía post-cuántica (PQC) que sean resistentes a ataques de canal lateral y fault attacks;
  - Medidas de contraataque optimizadas teniendo en cuenta un equilibrio adecuado entre seguridad, rendimiento y costes;
  - Recomendaciones sobre la implementación de contramedidas para una amplia gama de ataques, identificando también el hardware disponible y necesario;
  - Análisis de nuevos ataques o combinaciones de ataques, que eventualmente también pueden ser mejorados por IA, aplicables a condiciones y escenarios reales
  - Diseño de evaluaciones de seguridad automatizadas para implementaciones de PQC.

HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

Los proyectos deben contribuir a uno o varios de los siguientes resultados esperados:

- Diseño e implementaciones de, al menos, un protocolo de criptografía post-cuántica de alto nivel junto con un análisis de seguridad que demuestre que no se pierde seguridad en comparación con las tecnologías blockchain utilizadas
- Presentación de estos protocolos de alto nivel integrando PQC a organismos de estandarización y/o presentación de la especificación e implementación a los respectivos proyectos de código abierto;
- Análisis de requisitos para el desarrollo de soluciones PQC que garanticen la migración hacia entornos PQC.

Eventos de búsqueda de socios

SMI2G
Security Mission Information & Innovation Group
2025 Brokerage Event
6 & 7 May

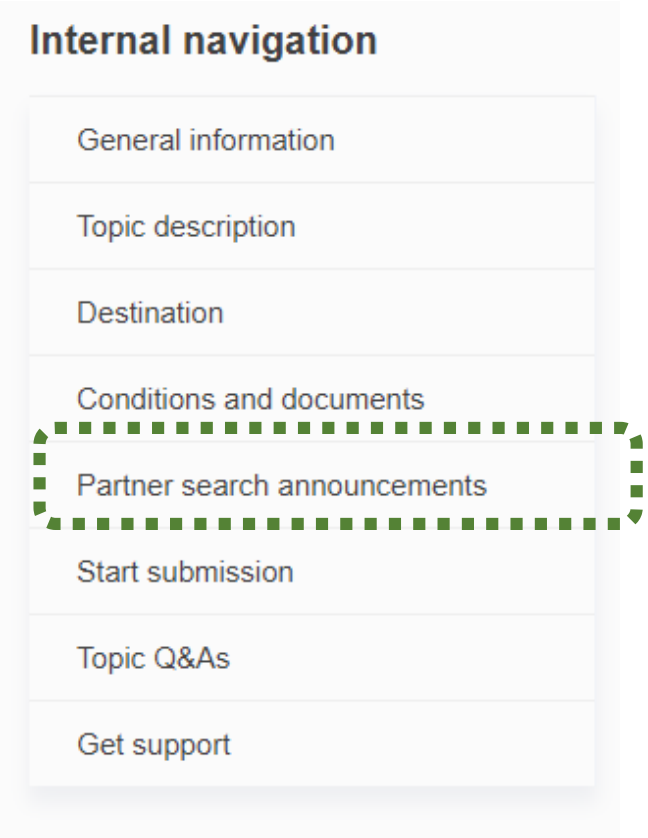
this link.

12th June Home | Cluster 3 Infoday and Brokerage Event 2025

Herramientas para la búsqueda de socios

Funding and Tenders Portal

[EU Funding & Tenders Portal]



SeReMa – Security Research Map

https://security-research-map.b2match.io/

maite.boyero@cdti.es

marina.cdti@sost.be

ripaca@inta.es

Group: Horizonte Europa Clúster 3 “Seguridad civil para la sociedad”

www.horizonteeuropa.es

Canal de Telegram “Horizonte Europa”

NCC-ES INCIBE
Edificio INCIBE. Av. José Aguado 41.
24005 León. España
Tel: +34 987 877 189
nccspain@incibe.es

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPAIN
Land of cybersecurity

#innovacion
#ayudascdti
#asesoramiento
#internacionalizacion

HORIZONTE EUROPA
@HorizonteEuropa

Horizonte Europa C4-Digital

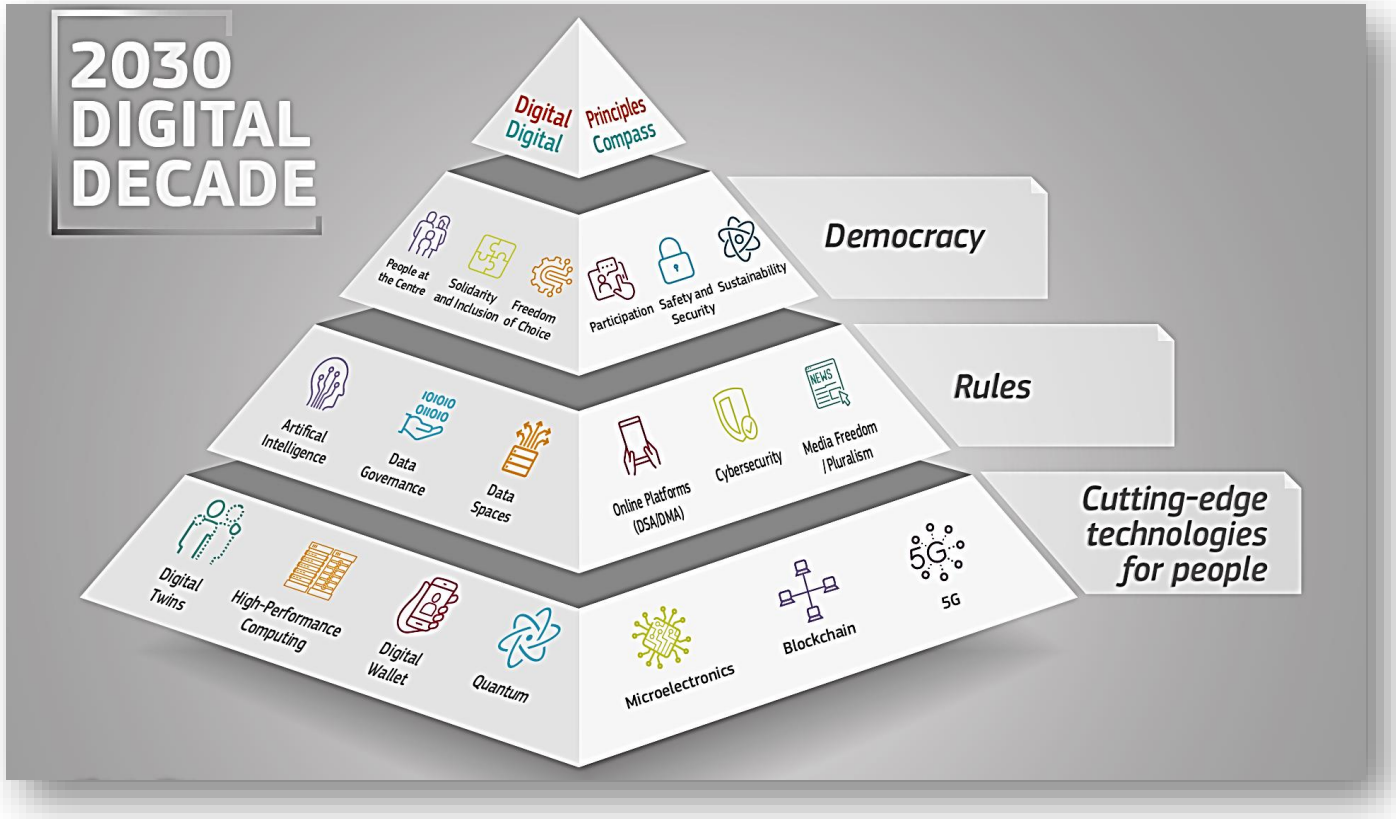
WP2025

León, 9 julio 2025

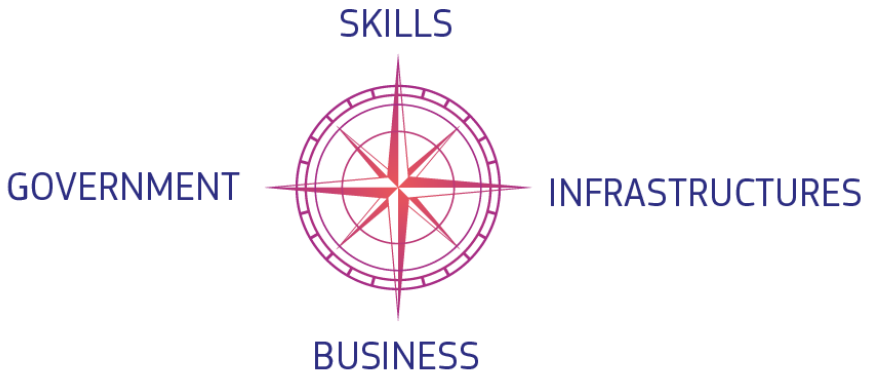
Fernando Martín Galende
fernando.martin@cdti.es

1. El contexto político en el desarrollo de tecnologías digitales (DGCONNECT)
2. Horizonte Europa – Clúster 4 – Digital
3. Destinations y Áreas de Interés
4. Convocatorias y Topics
5. Puntos Nacionales de Contacto y Apoyo a los Participantes
6. Conclusiones

Estrategia Política: Digital (DGCONNECT)

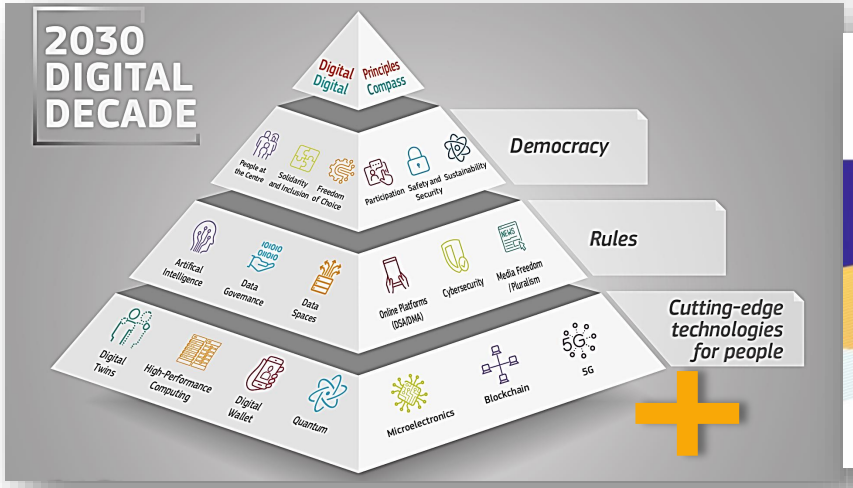


Brújula Digital



Estrategia Política: Digital (DGCONNECT)

https://digital-strategy.ec.europa.eu/en/policies



Estrategia Política: Programas Digitales (DGCONNECT)

Horizonte Europa: Clúster 4 - Digital

Horizonte Europa: Clúster 4 – Digital - Partenariados

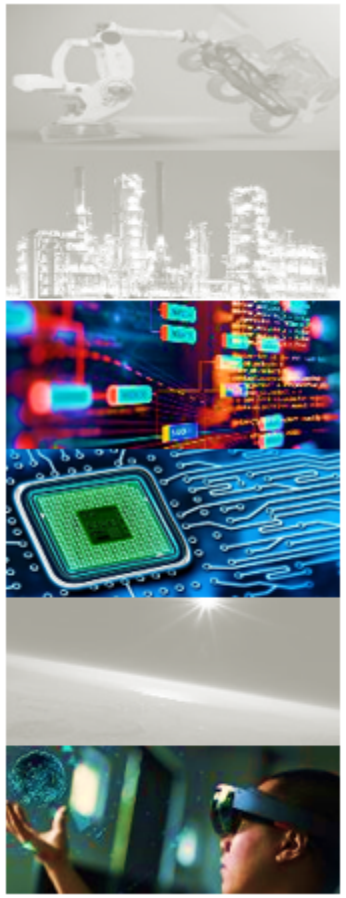
Institucionalizados

- Chips (**Chips JU**)
- High Performance Computing (**EuroHPC JU**)
- Smart Networks and Services (**SNS JU**)

Co-programdaos

- AI / Data / Robotics (**ADRA**)
- Photonics (**Photonics21**)
- Virtual Worlds **NUEVO**

Horizonte Europa: Clúster 4 – Digital – Destinations



CLIMATE NEUTRAL, CIRCULAR AND DIGITISED **PRODUCTION**

INCREASED AUTONOMY IN KEY STRATEGIC VALUE CHAINS FOR **RESILIENT** INDUSTRY

WORLD LEADING **DATA** AND COMPUTING TECHNOLOGIES

DIGITAL AND **EMERGING** TECHNOLOGIES FOR COMPETITIVENESS AND FIT FOR THE GREEN DEAL

OPEN STRATEGIC AUTONOMY IN DEVELOPING, DEPLOYING AND USING GLOBAL **SPACE-BASED** INFRASTRUCTURES, SERVICES, APPLICATIONS AND DATA

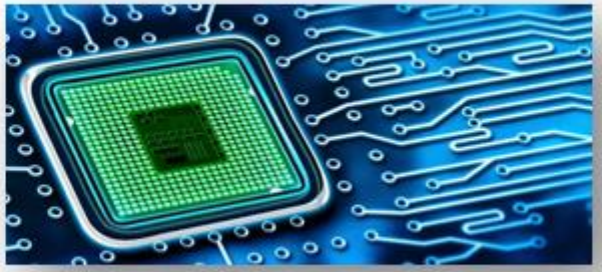
A **HUMAN-CENTRED** AND ETHICAL DEVELOPMENT OF DIGITAL AND INDUSTRIAL TECHNOLOGIES

Horizonte Europa: Clúster 4 – Digital – Destinations

D3 - DATA

- Data
- 3C Networks

D4 - EMERGING



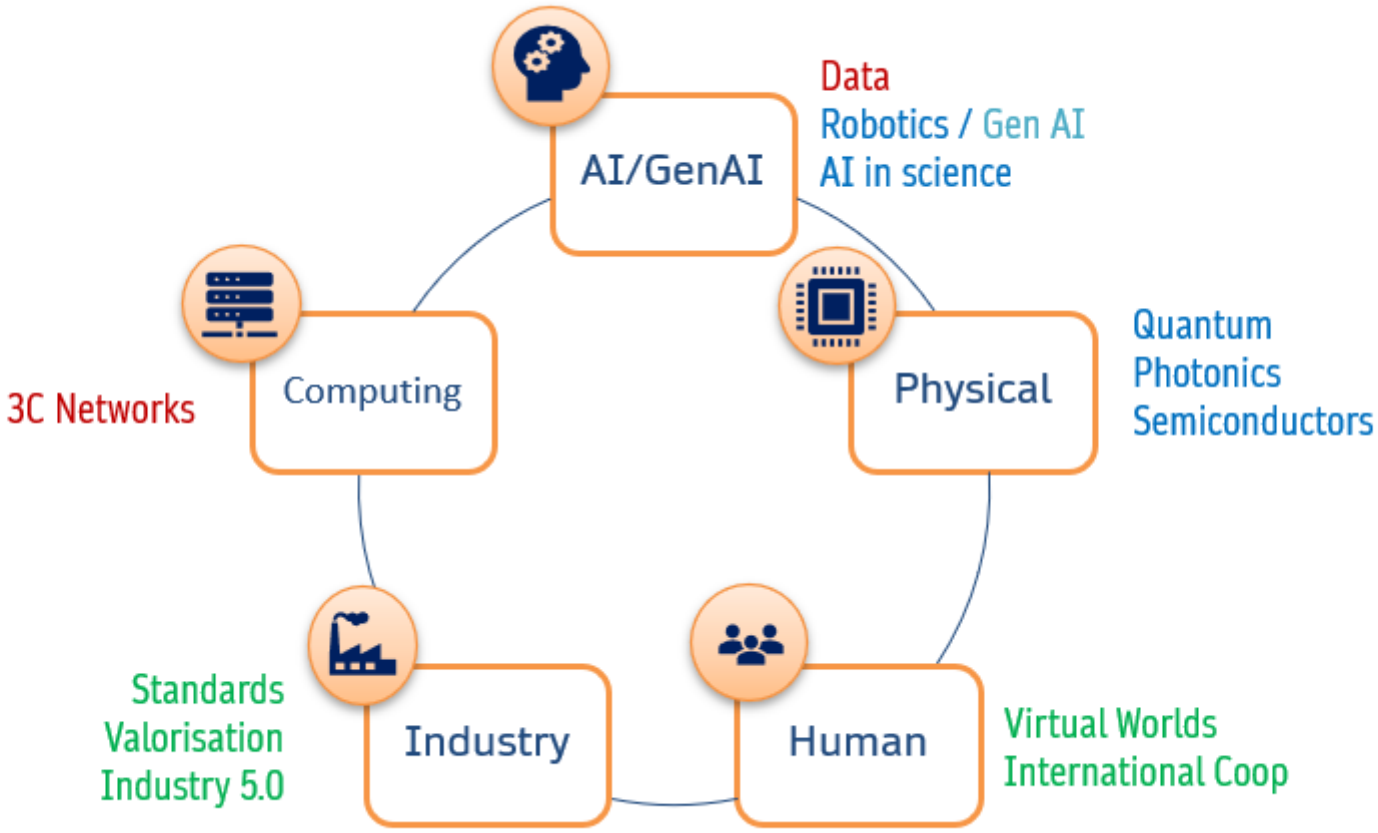
- Quantum
- Photonics
- Robotics / Gen AI
- AI in science

D6 - HUMAN

- Gen AI
- Virtual Worlds
- Standards & valorisation
- International cooperation

Horizonte Europa: Clúster 4 – Digital – Áreas de Interés

D3 - DATA
D4 - EMERGING
D6 - HUMAN



Horizon-C4: 3C Networks

Topic	Title	Inst.	M€ Project	M€ Topic	TRLs
2025-03-DATA-08	**Large-scale pilots** for supply end-to-end infrastructures integrating device, network computing and communication capabilities for Telco Edge Cloud deployments, as a basis for Connected Collaborative Computing Networks (3C networks) (RIA)	RIA	75	75	3 to 7
2025-03-DATA-09	**Alignment of stakeholders** towards the supply-side large-scale pilot of end-to-end infrastructures integrating device, network computing and communication capabilities (CSA)	CSA	2,5	2,5	-
2025-03-DATA-10	**Roadmap** for next generation computing technologies from IoT device level to edge to cloud to HPC (CSA)	CSA	2,5	2,5	-
2025-03-DATA-11	Open Internet Stack: development of technological commons/open-source **3C building blocks** (RIA)	RIA	10	10	SW, dev/ops
2025-03-DATA-12	Preparing the Advancement of the state of the art of **submarine cable infrastructures** (CSA)	CSA	2,1	2,1	-

Cierre: 02/10/2025

Horizon-C4: GenAI / Data / Robotics

Topic	Title	Inst.	M€ Project	M€ Topic	TRLs
2025-03-DATA-13	Fostering Innovative and **Compliant Data** Ecosystems (IA) (ADRA)	IA	7-9	45	6-7 to 8
2025-04-DATA-02	Empowering AI/GenAI along the Cognitive **Computing continuum** (RIA) (ADRA)	RIA	6-8	30	3 to 6-7
2025-04-DATA-03	**Software Engineering** for AI and Generative AI (RIA) (ADRA)	RIA	4-6	15	4 to 6
2025-04-DIGITAL-EMERGING-05	**Soft Robotics** for Advanced physical capabilities (IA) (ADRA)	IA	10	20	4 to 7
2025-03-DIGITAL-EMERGING-07	Robust and trustworthy GenerativeAI for **Robotics and industrial automation** (RIA) (ADRA & Made in Europe Partnerships)	RIA	40-45	85	2 to 6
2025-04-DIGITAL-EMERGING-04	**Assessment methodologies for General Purpose AI** capabilities and risks (RIA) (ADRA)	RIA	3-4	7	2 to 5
2025-04-DIGITAL-EMERGING-07	Enhanced Learning Strategies for **General Purpose AI**: Advancing GenAI4EU (RIA) (ADRA)	RIA	15	30	2 to 5
2025-04-DIGITAL-EMERGING-09	**Challenge-Driven** GenAI4EU Booster (RIA) (ADRA)	RIA	15	45	3 to 6
INDUSTRY-2025-01-DIGITAL-61	AI **Foundation models** in science (GenAI4EU) (RIA)	RIA	5	30	1 to 4
INDUSTRY-2025-01-DIGITAL-62	Facilitated **cooperation** for AI in Science (CSA)	CSA	3	3	-
2025-03-HUMAN-18	GenAI4EU **central Hub** (CSA) (ADRA)	CSA	3	3	-

Cierre: 23/09/2025

Cierre: 02/10/2025

Horizon-C4: Photonics / Quantum / Semiconductors

Topic	Title	Inst.	M€ Project	M€ Topic	TRLs
2025-04-DIGITAL-EMERGING-01	Advanced sensor technologies and **multimodal sensor integration** for multiple application domains (IA) (Photonics Partnership)	IA	4-6	25	3-4 to 7
2025-03-DIGITAL-EMERGING-01	Continuation of the **Quantum Technologies** Flagship (CSA)	CSA	4,5	4,5	-
-	Quantum Internet Framework Partnerships Agreement– launching the second **Specific Grant Agreement** (SGA2)	SGA	47,5	47,5	4-5 to 6-7
2025-03-DIGITAL-EMERGING-02	Quantum Computing – complementing the quantum computing FPAs with the development of a technology agnostic **software stack** (RIA)	RIA	5	10	3-4 to 5-6
2025-03-DIGITAL-EMERGING-03	**Supporting Digital Partnerships** in Quantum technologies (RIA)	RIA	2,5-2,7	8	2-3 to 3-5
2025-03-DIGITAL-EMERGING-04	Post-exascale **HPC** (CSA)	CSA	2,5	2,5	-
2025-03-DIGITAL-EMERGING-08	Strengthening the **fabless Start-up and SME ecosystem** in Europe (CSA)	CSA	1	1	-

Cierre: 02/10/2025

Horizon-C4: Virtual Worlds / International Cooperation

Topic	Title	Inst.	M€ Project	M€ Topic	TRLs
2025-03-HUMAN-14	**Core technologies** for virtual worlds (RIA) (Virtual Worlds and Photonics Partnerships)	RIA	5-6	43	3 to 5
2025-03-HUMAN-15	**Generative AI** for Virtual Worlds: Advanced technologies for better performance and hyper personalised and immersive experience (IA) (AI/Data/Robotics & Virtual Worlds Partnerships)	IA	4-5	20	4 to 6
2025-03-HUMAN-16	Drive the evolution of the internet towards open and interoperable **Web 4.0** and Virtual Worlds : building blocks in priority areas (RIA) (Virtual Worlds Partnership)	RIA	1-3	14,5	SW, dev/ops
2025-03-HUMAN-17	Specific **support** for the Virtual Worlds Partnership and the Web 4.0 initiative (CSA) (Virtual Worlds Partnership)	CSA	2,5	2,5	-
2025-03-HUMAN-19	International cooperation in **semiconductors** (CSA)	CSA	3	3	-
2025-04-HUMAN-08	GenAI for Africa	RIA	1-2	5	4 to 6
-	AI for Public Good 1: Innovative AI-powered **cancer imaging solutions** for breast and prostate diagnosis	PP	?	2,4	-
-	AI for Public Good 2: Innovative AI-powered **solutions for emergency** response and crisis management	PP	?	2	-
-	AI for Public Good 3: Innovative AI-powered **solutions for urban** reconstruction	PP	?	2	-
-	AI for Public Good 4: Innovative AI-powered **solutions for electric grid** optimisation	PP	?	3	-

Cierre: 02/10/2025

Horizon-C4: Otras Iniciativas Relacionadas (Industry)

STD

Topic	Title	Inst.	M€ Project	M€ Topic	TRLs
INDUSTRY-2025-01-HUMAN-60	Horizon Standardisation **Booster** (CSA)	CSA	1,5	1,5	-
INDUSTRY-2025-01-HUMAN-61	Standardisation landscape analyses **tool** (CSA)	CSA	1	1	-
INDUSTRY-2025-01-HUMAN-62	**Artificial Intelligence** for knowledge valorisation (CSA)	CSA	2	2	-
INDUSTRY-2025-01-HUMAN-63	Value **creation pilots** for scaling up innovative solutions (CSA)	CSA	2	2	-
INDUSTRY-2025-01-HUMAN-64	Pilot initiatives on Technology **Infrastructures** (CSA)	CSA	0,5 - 1	5	-
INDUSTRY-2025-01-HUMAN-65	**System innovation** experimentation for Industry 5.0 (IA)	IA	3	3	??
INDUSTRY-2025-01-HUMAN-66	Assessment of Technology Infrastructure needs in **Ukraine** (CSA)	CSA	1 - 1,5	1,5	-

Cierre: 23/09/2025

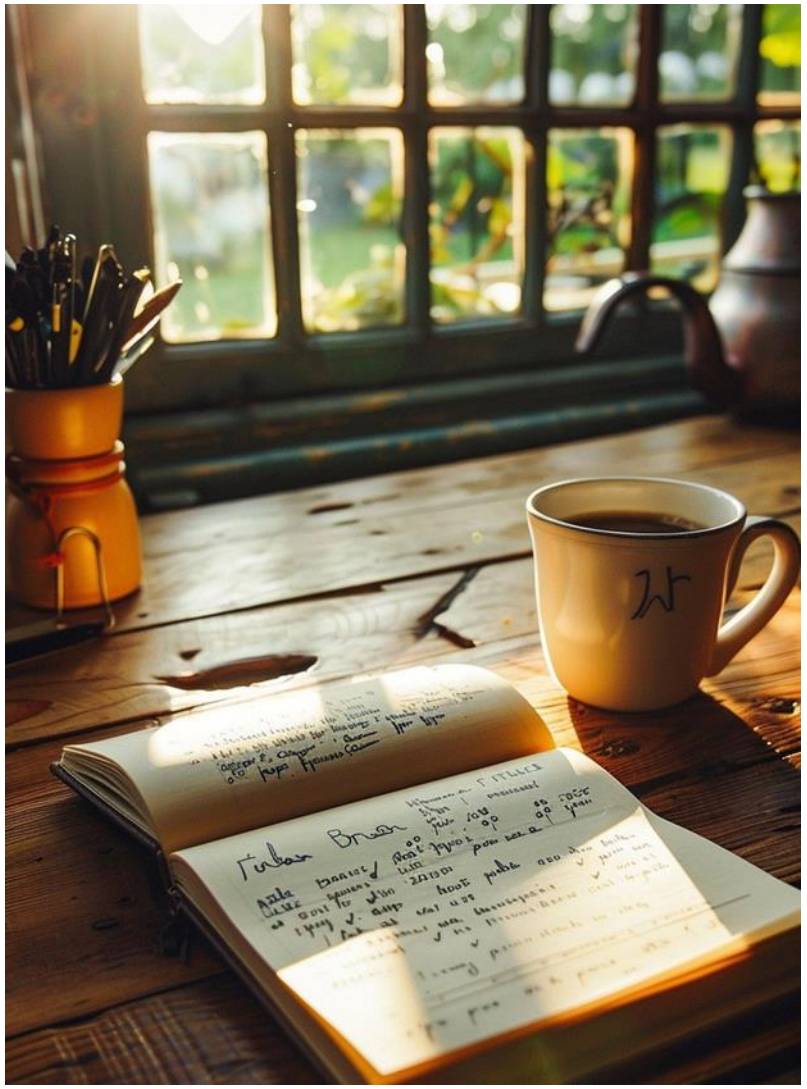
Horizonte Europa: Clúster 4 – Digital – Puntos de Contacto

enrique.pelayo@cdti.es

fernando.rico@cdti.es

fernando.martin@cdti.es

Conclusiones



- Hay cambios en HE, algunos de ellos relevantes, como las **restricciones a la participación** (Artículos 22.5 y 22.6).
- La parte digital del cluster 4 se centra en **Desarrollo** de tecnologías.
- Hay mucho peso de los **Partenariados.**
- Desde el **CDTI damos soporte** en todo momento al participante.

NCC-ES INCIBE
Edificio INCIBE. Av. José Aguado 41.
24005 León. España
Tel: +34 987 877 189
nccspain@incibe.es

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NCC-ES
SPAIN CYBERSECURITY COORDINATION CENTRE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

InfoDay NCC-ES

Oportunidades de financiación para el desarrollo de capacidades de ciberseguridad

¡GRACIAS!

Cofinanciado por la Unión Europea

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD