European Commission

Ciberseguridad

Fondos europeos para ciberseguridad (Junio 2023)

Fidel Santiago
Junio 2023

“La transición digital se está acelerando, pero solo podrá tener éxito si las personas y las empresas pueden confiar en la seguridad de los productos y servicios conectados, de los que dependen.”

Margrethe Vestager

Vicepresidenta Ejecutiva para Una Europa Adaptada a la Era Digital

European Commission

Estrategia de Ciberseguridad de la UE

RESILIENCIA, SOBERANÍA TECNOLÓGICA Y LIDERAZGO

Infraestructura resiliente y servicios críticos

Construir un escudo cibernético europeo

Una infraestructura de comunicación ultrasegura

Protección de la próxima generación de redes móviles de banda ancha

Una internet de las cosas seguras

Mayor seguridad mundial en internet

Una presencia reforzada en la cadena de suministro de tecnología

Una población activa cibercualificada de la UE

DESARROLLO DE LA CAPACIDAD OPERATIVA PARA PREVENIR, DISUADIR Y CONTRARRESTAR

Una unidad informática conjunta

Lucha contra la ciberdelincuencia

Conjunto de instrumentos de ciberdiplomacia de la UE

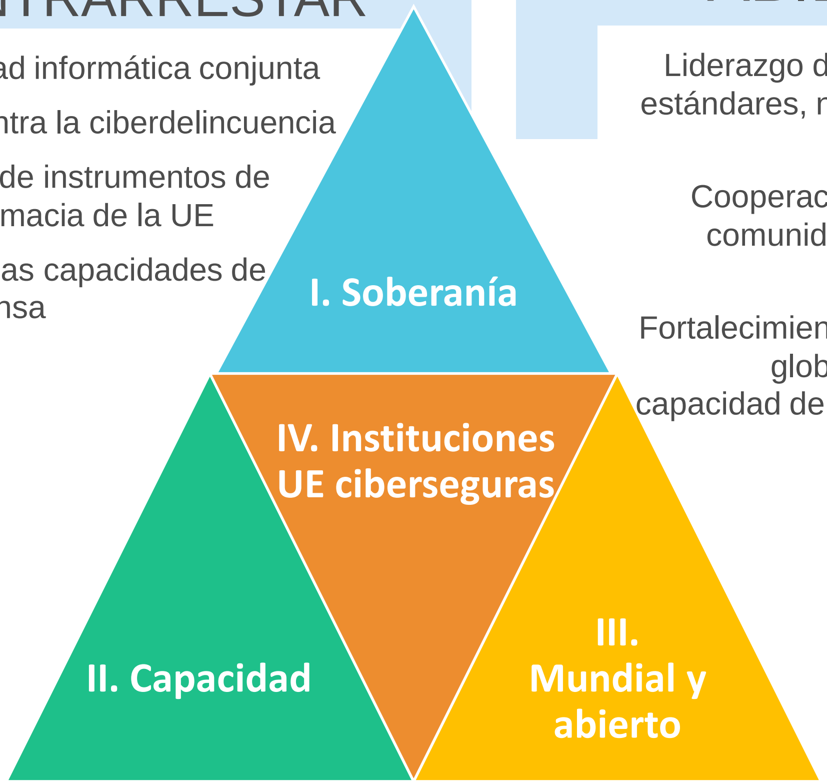
Impulsar las capacidades de ciberdefensa

FOMENTAR UN CIBERESPACIO MUNDIAL Y ABIERTO

Liderazgo de la UE en materia de estándares, normas y marcos en el ciberespacio

Cooperación con los socios y la comunidad de múltiples partes interesadas

Fortalecimiento de las capacidades globales para aumentar la capacidad de recuperación mundial



I. Soberanía

IV. Instituciones UE ciberseguras

II. Capacidad

III. Mundial y abierto

Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad

Centro Europeo de Competencia

- Apoya la inversión conjunta por parte de la UE, de los Estados Miembros y de la industria.
- Apoya el despliegue de productos y soluciones.
- Facilita y ayuda a coordinar la Red y la Comunidad.
- Gestiona los fondos de ciberseguridad en DIGITAL y Horizonte Europa.

Red de Centros Nacionales de Coordinación

- Objetivo: crear capacidad nacional y conectar con iniciativas existentes.
- Punto nacional de contacto.
- Pueden recibir fondos de la UE y traspasar apoyo financiero.

Comunidad de competencias

- Un grupo amplio, abierto y diverso de partes interesadas en ciberseguridad; desde la investigación hasta los sectores privado y público, incluyendo los sectores civil y militar.

Red de Centros Nacionales de Coordinación

- Un NCC por Estado miembro
- Puede recibir y repercutir financiación de la UE
- Fomento de la capacidad nacional y vinculación con las iniciativas existentes
- Promueve la participación en proyectos transfronterizos y en acciones de ciberseguridad
- Coordina los niveles nacional, regional y local
- Promueve programas educativos en materia de ciberseguridad
- Aboga por la participación de las entidades pertinentes

Comunidad de competencias

Un grupo amplio, abierto y diverso de partes interesadas procedentes de

- la investigación
- los sectores público y privado, incluidos los sectores civil y de defensa.

Intercambios con el Centro sobre la evolución de la ciberseguridad

Contribuye a las actividades del Centro, al programa de trabajo plurianual y al programa de trabajo anual

Se divide en grupos de trabajo para un diálogo regular

Horizonte Europa

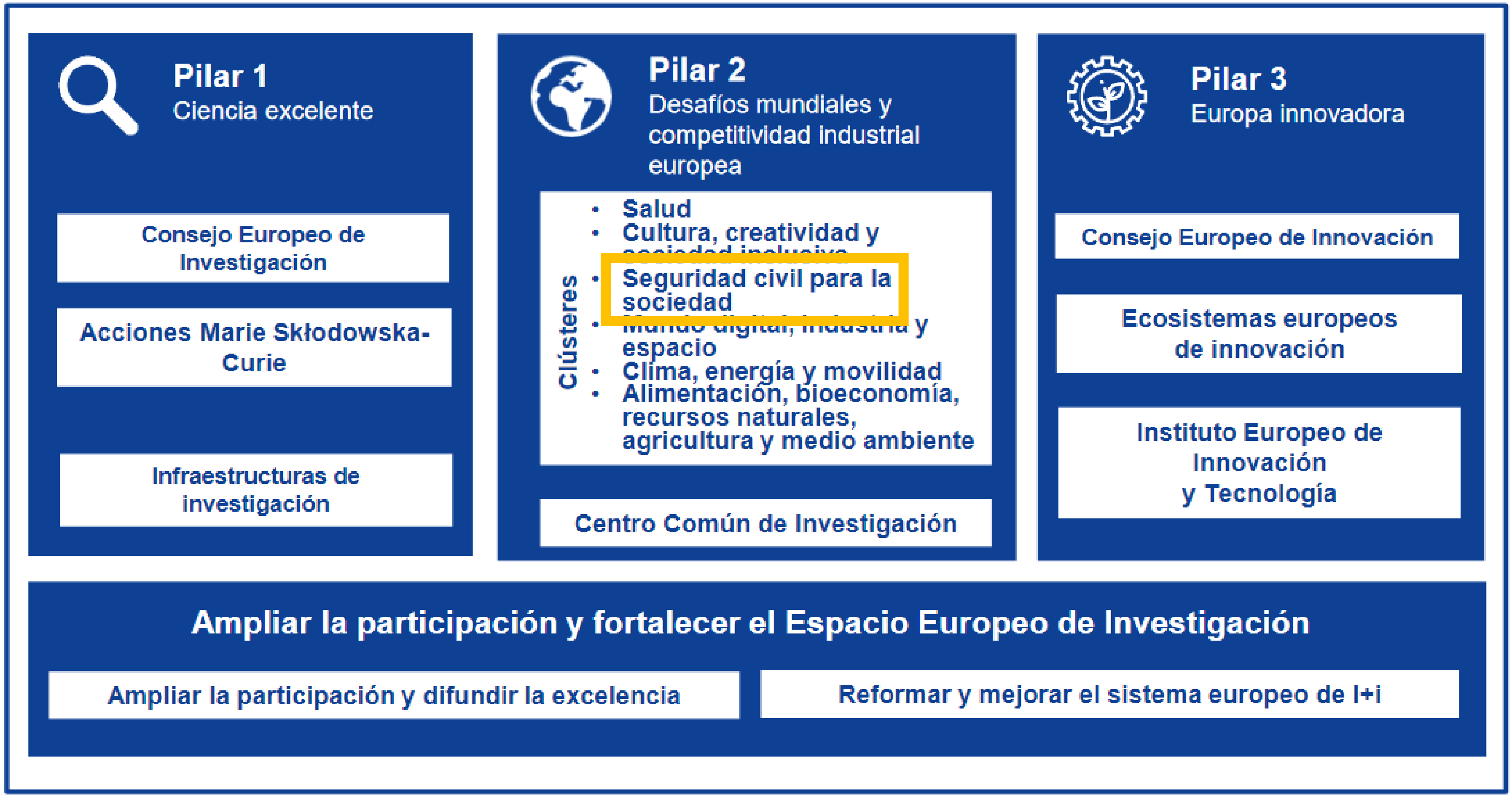
Programa Marco de Investigación e Innovación de la UE (2021-2027)

para reforzar las bases científicas y tecnológicas de la UE y el Espacio Europeo de Investigación (EEI),

para impulsar la capacidad de innovación, la competitividad y el empleo de Europa,

para cumplir con las prioridades de los ciudadanos, así como sostener nuestros valores y modelo socio económico.

Horizonte Europa - Estructura



Pilar 1
Ciencia excelente

- Consejo Europeo de Investigación
- Acciones Marie Skłodowska-Curie
- Infraestructuras de investigación

Pilar 2
Desafíos mundiales y competitividad industrial europea

Clústeres

- Salud
- Cultura, creatividad y sociedad inclusiva
- Seguridad civil para la sociedad
- Mundo digital, industria y espacio
- Clima, energía y movilidad
- Alimentación, bioeconomía, recursos naturales, agricultura y medio ambiente

Centro Común de Investigación

Pilar 3
Europa innovadora

- Consejo Europeo de Innovación
- Ecosistemas europeos de innovación
- Instituto Europeo de Innovación y Tecnología

Ampliar la participación y fortalecer el Espacio Europeo de Investigación

- Ampliar la participación y difundir la excelencia
- Reformar y mejorar el sistema europeo de I+i

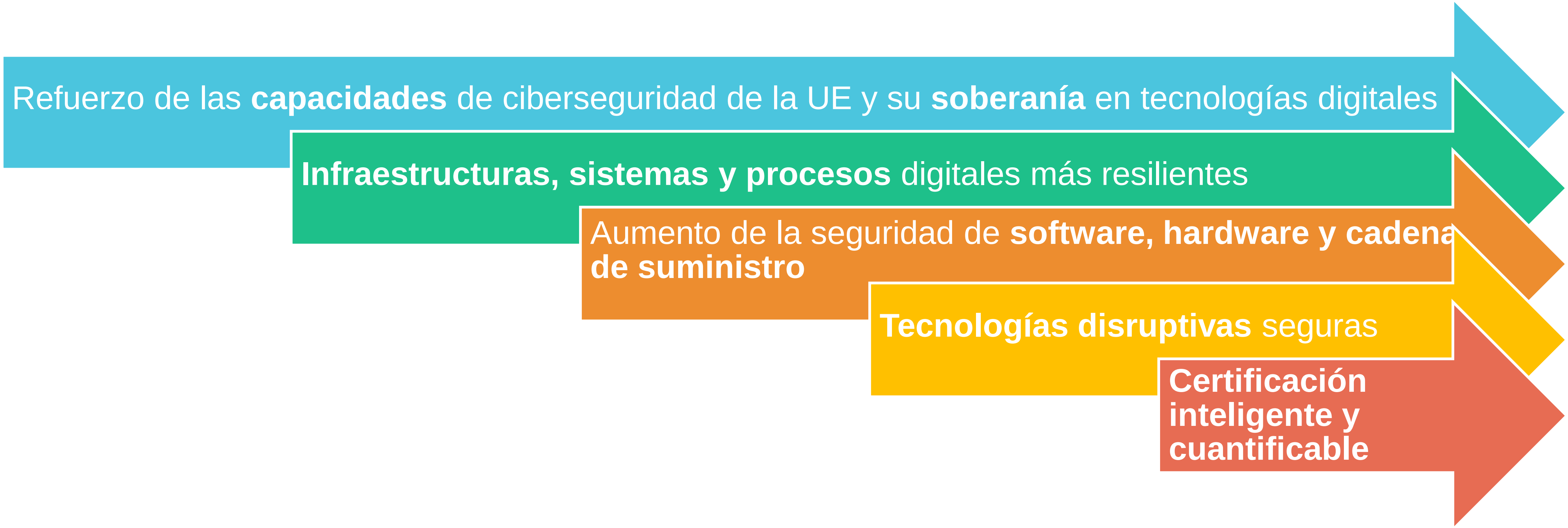
HE Ciberseguridad

Destino *Increased Cybersecurity* (23-24)

*«****Aumento de la ciberseguridad*** *y un* ***entorno en línea más seguro mediante el desarrollo y la utilización eficaz de las capacidades*** *de la UE y los Estados miembros en las tecnologías digitales que apoyan la protección de los datos y las redes que aspiran a la* ***soberanía tecnológica*** *en este ámbito, respetando al mismo tiempo la privacidad y otros derechos fundamentales; esto debe contribuir a la seguridad de los* ***servicios, procesos y productos,*** *así como a* ***infraestructuras digitales*** *sólidas capaces de resistir y* ***contrarrestar los ciberataques y las amenazas híbridas****».*

Plan Estratégico 2021-2024

Destino *Increased Cybersecurity* (23-24)



Refuerzo de las **capacidades** de ciberseguridad de la UE y su **soberanía** en tecnologías digitales

Infraestructuras, sistemas y procesos digitales más resilientes

Aumento de la seguridad de **software, hardware y cadena de suministro**

Tecnologías disruptivas seguras

Certificación inteligente y cuantificable

Convocatoria HE Ciberseguridad 2023*

Del 29.6 al 23.11.2023

	Tipo de acción	Presupuesto (EUR M)	Estimado por acción (EUR M)
Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces) *HORIZON-CL3-2023-CS-01-01*	IA	28	4 – 6
Privacy-preserving and identity management technologies *HORIZON-CL3-2023-CS-01-02*	IA	15.70	2 – 4
Security of robust AI systems *HORIZON-CL3-2023-CS-01-03*	RIA	15	4 – 6

*HORIZON-CL3-2023-CS-01

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces) *HORIZON-CL3-2023-CS-01-01*

Expected outcomes

- **Tools** to support cybersecurity resilience, preparedness, awareness, and detection **within critical infrastructures and across supply chains**
- **Cloud** infrastructures vulnerabilities mitigation
- **Secure integration** of untrusted IoT in trusted environments
- Use of **Zero-Trust** architectures
- Trust & Security for **massive connected IoT** ecosystems & lifecycle management
- **Secure interoperability** and integration of systems
- **AI-based automation** tools for cyber threat intelligence
- Secure infrastructure, secure Identities and usability for a security chain covering communication, data collection, data transport, and data processing

Scope

- **Cloud, edge computing, IoT** requires **advanced, smart security and privacy**. Their complexity underlines the need for **proactive and automated detection, analysis, and mitigation** of cybersecurity attacks, and in application domains such as, e.g., smart cities.
- **Identification and analysis of regulatory aspects** for the developed technologies or solutions is encouraged.

Budget EUR 28M : 4-6M per action

Privacy-preserving and identity management technologies *HORIZON-CL3-2023-CS-01-02*

Expected outcomes

- Improved **scalable** and reliable **privacy-preserving and identity management** technologies for **federated processing and secure sharing** of personal and industrial data
- Improving privacy-preserving technologies for **cyber threat intelligence** (sharing)
- **Privacy by design**
- **Contribution to European data spaces** (in synergy with *DATA Topics of Horizon Europe Cluster 4*) and **eID** compliant European solutions
- Research and development of **self-sovereign identity** management technologies and solutions
- Provide resource efficient and secure digital identity **solutions for SMEs**
- Strengthened European ecosystem of **open-source developers and researchers of privacy-preserving solutions**
- **Usability** of privacy-preserving and identity management technologies

Scope

- **Advanced privacy-preserving technologies** have the potential to **enable and foster the value** in personal and non-personal (industrial) **data assets**. Further work is required to ensure and test their applicability in **real-world use case scenarios**.
- Proposed solutions should be **validated and piloted in realistic**, **federated data infrastructures**, e.g., European data spaces. They should be **GDPR compliant by-design**. **Open-source** solutions are encouraged.
- Consortia should bring **interdisciplinary expertise** and capacity covering **the supply and the demand** side. Participation of **SMEs** is strongly encouraged. The consortium should include **legal professionals.**
- **Identification and analysis of regulatory aspects** for the developed technologies or solutions is encouraged.

Budget EUR 15.7M : 2-4M per action

Security of robust AI systems
HORIZON-CL3-2023-CS-01-03

Expected outcomes

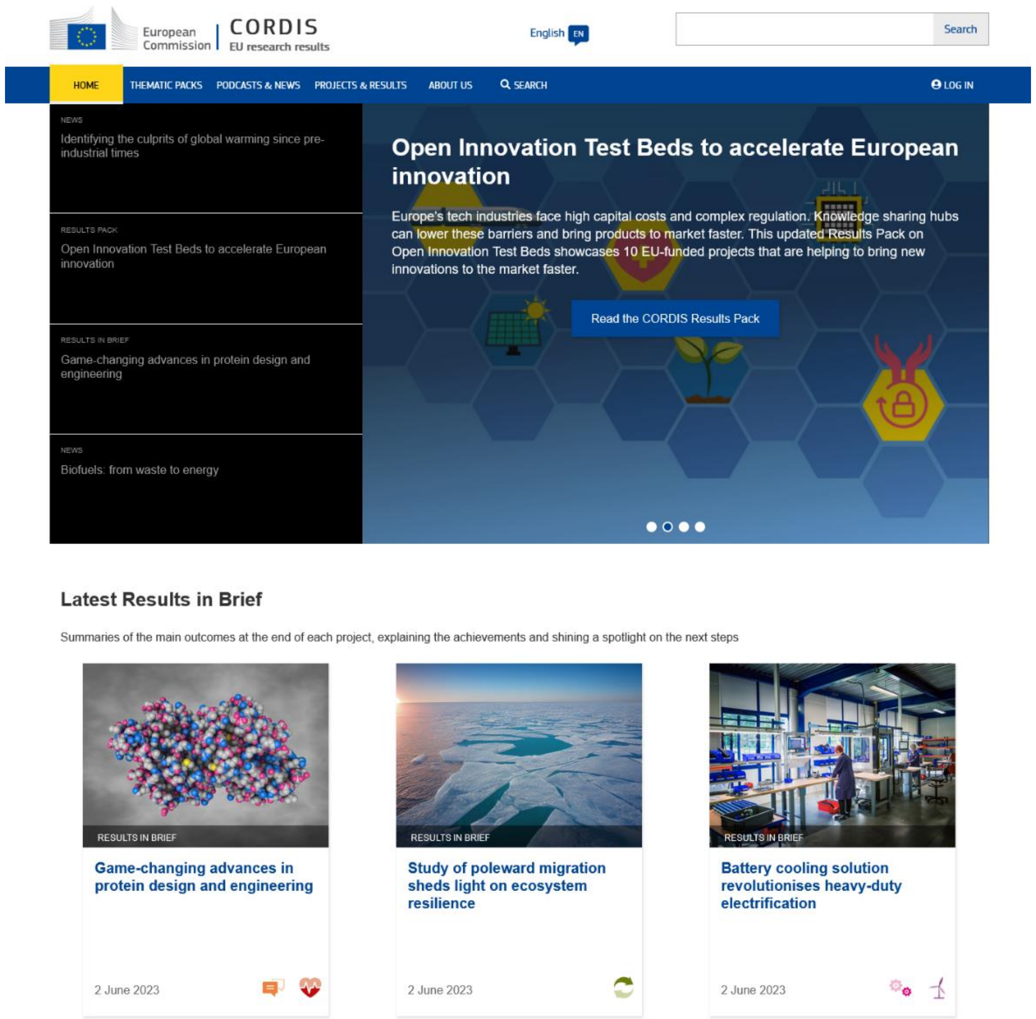
- Security-by-design concept and resilience to adversarial attacks
- Inclusion of context awareness in machine learning in order to boost resiliency

Scope

- **Concerns exist over the security and robustness of AI** algorithms including the risks of adversarial machine learning and data poisoning.
- Develop ***security-by-default*** **AI algorithms**, leading to possible **certification** schemes in the future.
- Proposals should demonstrate **awareness of the EU approach on AI** such as the proposed *Artificial Intelligence Act*.
- **Identification and analysis of regulatory aspects** for the developed technologies or solutions is encouraged.

Budget EUR 15M : 4-6M per action

Acciones anteriores



NEWS
Identifying the culprits of global warming since pre-industrial times

RESULTS PACK
Open Innovation Test Beds to accelerate European innovation

RESULTS IN BRIEF
Game-changing advances in protein design and engineering

NEWS
Biofuels: from waste to energy

Open Innovation Test Beds to accelerate European innovation

Europe's tech industries face high capital costs and complex regulation. Knowledge sharing hubs can lower these barriers and bring products to market faster. This updated Results Pack on Open Innovation Test Beds showcases 10 EU-funded projects that are helping to bring new innovations to the market faster.

Read the CORDIS Results Pack

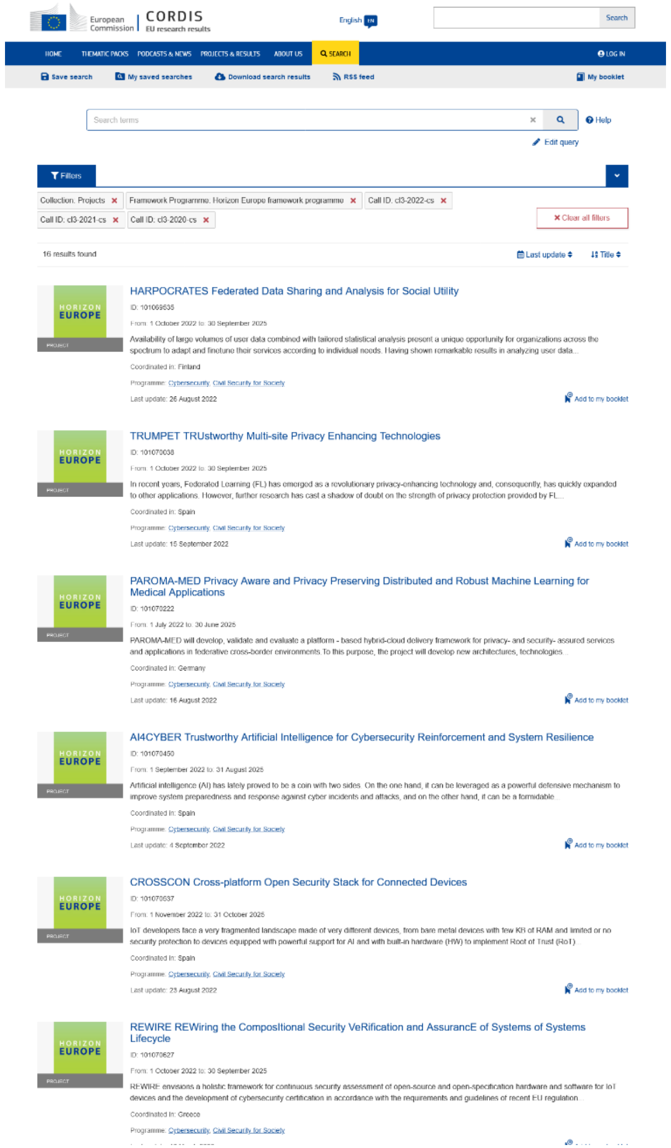
Latest Results in Brief

Summaries of the main outcomes at the end of each project, explaining the achievements and shining a spotlight on the next steps

RESULTS IN BRIEF
Game-changing advances in protein design and engineering
2 June 2023

RESULTS IN BRIEF
Study of poleward migration sheds light on ecosystem resilience
2 June 2023

RESULTS IN BRIEF
Battery cooling solution revolutionises heavy-duty electrification
2 June 2023



Collection: Projects ✕ | Framework Programme: Horizon Europe framework programme ✕ | Call ID: cl3-2022-cs ✕ | Call ID: cl3-2021-cs ✕ | Call ID: cl3-2020-cs ✕

16 results found

HARPOCRATES Federated Data Sharing and Analysis for Social Utility
ID: 101069535
From: 1 October 2022 to: 30 September 2025
Availability of large volumes of user data combined with tailored statistical analysis present a unique opportunity for organizations across the spectrum to adapt and finetune their services according to individual needs. Having shown remarkable results in analyzing user data...
Coordinated in: Finland
Programme: Cybersecurity, Civil Security for Society
Last update: 26 August 2022
Add to my booklet

TRUMPET TRUstworthy Multi-site Privacy Enhancing Technologies
ID: 101070038
From: 1 October 2022 to: 30 September 2025
In recent years, Federated Learning (FL) has emerged as a revolutionary privacy-enhancing technology and, consequently, has quickly expanded to other applications. However, further research has cast a shadow of doubt on the strength of privacy protection provided by FL...
Coordinated in: Spain
Programme: Cybersecurity, Civil Security for Society
Last update: 15 September 2022
Add to my booklet

PAROMA-MED Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning for Medical Applications
ID: 101070222
From: 1 July 2022 to: 30 June 2025
PAROMA-MED will develop, validate and evaluate a platform - based hybrid-cloud delivery framework for privacy- and security- assured services and applications in federative cross-border environments.To this purpose, the project will develop new architectures, technologies...
Coordinated in: Germany
Programme: Cybersecurity, Civil Security for Society
Last update: 16 August 2022
Add to my booklet

AI4CYBER Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience
ID: 101070450
From: 1 September 2022 to: 31 August 2025
Artificial intelligence (AI) has lately proved to be a coin with two sides. On the one hand, it can be leveraged as a powerful defensive mechanism to improve system preparedness and response against cyber incidents and attacks, and on the other hand, it can be a formidable...
Coordinated in: Spain
Programme: Cybersecurity, Civil Security for Society
Last update: 4 September 2022
Add to my booklet

CROSSCON Cross-platform Open Security Stack for Connected Devices
ID: 101070537
From: 1 November 2022 to: 31 October 2025
IoT developers face a very fragmented landscape made of very different devices, from bare metal devices with few KB of RAM and limited or no security protection to devices equipped with powerful support for AI and with built-in hardware (HW) to implement Root of Trust (RoT)...
Coordinated in: Spain
Programme: Cybersecurity, Civil Security for Society
Last update: 23 August 2022
Add to my booklet

REWIRE REWiring the ComposItional Security VeRification and AssurancE of Systems of Systems Lifecycle
ID: 101070627
From: 1 October 2022 to: 30 September 2025
REWIRE envisions a holistic framework for continuous security assessment of open-source and open-specification hardware and software for IoT devices and the development of cybersecurity certification in accordance with the requirements and guidelines of recent EU regulation...
Coordinated in: Greece
Programme: Cybersecurity, Civil Security for Society

https://cordis.europa.eu/programme/id/HORIZON.2.3.3

European
Commission

DIGITAL EUROPE PROGRAMME

#DigitalEuropeProgramme

Europa DIGITAL

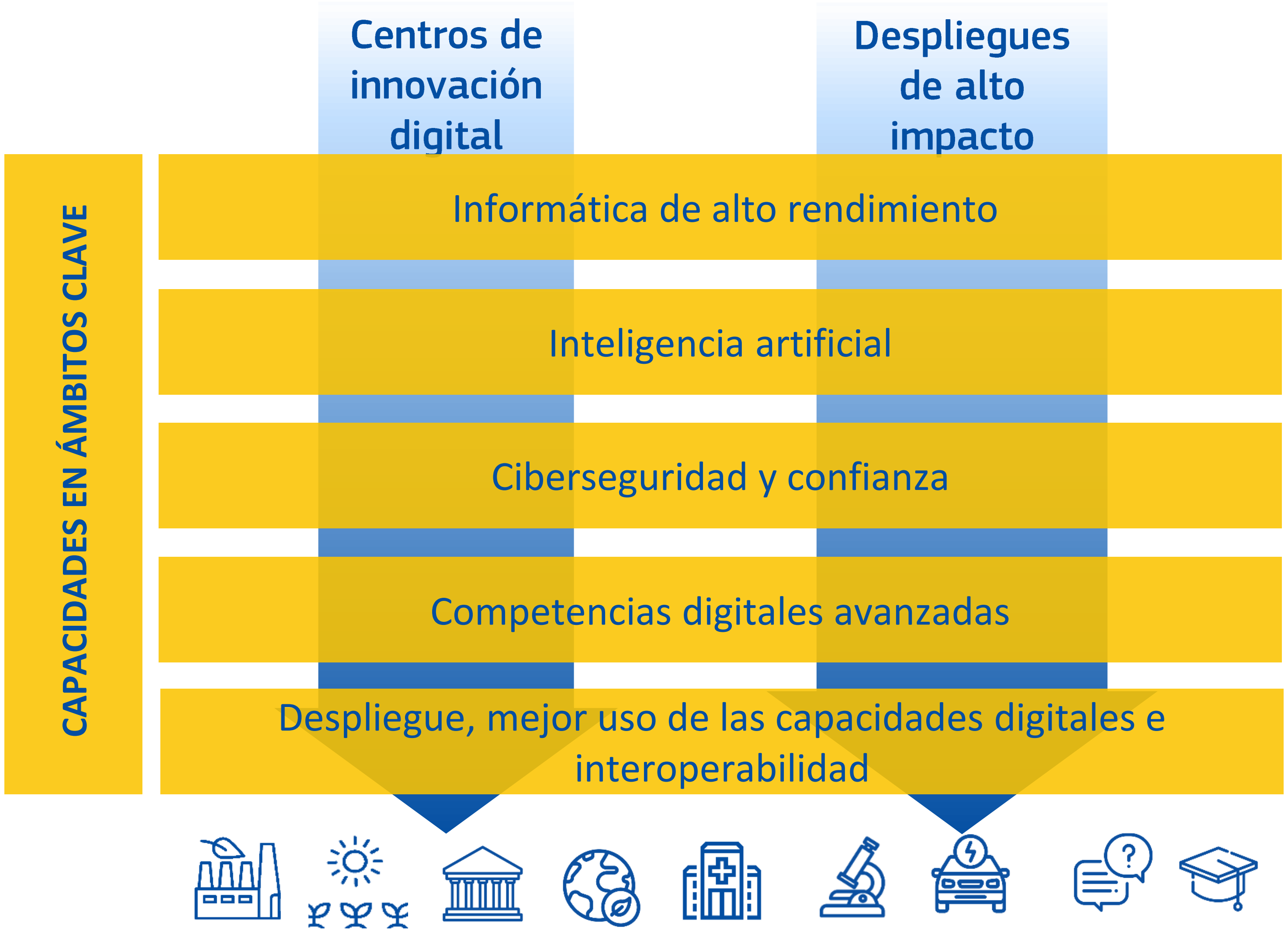
Centrado en llevar la tecnología digital a las empresas y los ciudadanos.

Acelerará la recuperación económica y la transformación digital de la sociedad y la economía europeas.

Complementa otros programas de la UE como el programa Horizonte Europa.

Financiación estratégica en cinco áreas cruciales.

Europa DIGITAL - Estructura



Centros de innovación digital

Despliegues de alto impacto

CAPACIDADES EN ÁMBITOS CLAVE

Informática de alto rendimiento

Inteligencia artificial

Ciberseguridad y confianza

Competencias digitales avanzadas

Despliegue, mejor uso de las capacidades digitales e interoperabilidad

WP DIGITAL 2023-24

SOCs

- Expresión de Interés en SOCs Nacionales
- Expresión de Interés en Plataformas SOC transfronterizas
- Fortalecimiento del ecosistema SOC
- Adopción de soluciones innovadoras de ciberseguridad
- Ciberseguridad del sector sanitario

Mecanismo de Emergencia de Ciberseguridad

- Apoyo a la Preparación y Asistencia Mutua
- Coordinación entre las esferas civiles y de defensa
- Estandarización en ciberseguridad
- Apoyo a la aplicación de la legislación europea y las estrategias nacionales

Europa DIGITAL SO3: Convocatorias 2023

Tema	Budge	Apertura	Plazo
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST *Apoyo a la Preparación y Asistencia Mutua*	EUR 35M	25/05/23	26/09/23
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE *Coordinación entre las esferas civil y de defensa*	EUR 3M		
Digital-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION *Normalización en el Área de Ciberseguridad*	EUR 3M		
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION *Apoyo a la aplicación de la legislación europea y las estrategias nacionales en materia de ciberseguridad*	EUR 30M		

Preparedness Support and Mutual Assistance

FSTP

Objectives

- Assist MSs in their efforts to improve their preparedness for cyber incidents
- Support mutual assistance between MSs for both preparedness and incident response.

Scope

- Testing of essential entities operating critical infrastructure
- Support for threat and risk assessments
- Risk monitoring service

Targeted stakeholders

- National cybersecurity authorities, competence centres or Coordination Centres (as defined in Regulation (EU) 2021/887)
- Entities capable of aggregating demand from end beneficiaries
- Multi-country consortia are not mandatory but will positively contribute to the impact of the action

Grants for Financial Support

- EUR 35M
- 48 months
- Indicative budget: EUR 3-7M per action

Preparedness Support and Mutual Assistance (and II)

FSTP

Outcomes and deliverables

- Preparedness support services
- Threat assessment and risk assessment services
- Risk monitoring services
- Mutual assistance among Member States

KPIs to measure outcomes and deliverables

- Number of penetration tests provided
- Number of essential entities supported
- Number of threat assessments / risk scenario analyses carried out
- Number of risk monitoring services provided
- Number of potential number of users covered per test/exercise
- Number and nature of vulnerabilities discovered
- Number of cross-border actions/exercises

Coordination Between the C.Civilian and Defence Spheres

Objective

- Enhance exchange and coordination between the cybersecurity civilian and defence spheres
- In particular, foster synergies between cybersecurity actions in Horizon Europe, Digital and defence related actions from programmes such as the European Defence Agency and the European Defence Fund

Scope

- Organise activities to exchange on cybersecurity technologies relevant to both civilian and defence, e.g.: meetings or workshops
- Collaborative activities between stakeholders of the civil and defence communities (academia, SMEs, industry, public authorities, etc.)

Targeted stakeholders

- Stakeholders in either the civilian or defence community:
  - Industrial players
  - Defence Ministries and Agencies
  - SMEs and start-ups
- *Multi-country consortia are not mandatory but will positively contribute to the impact of the action*

Coordination and Support Actions

- 100% funding rate
- EUR 3M
- 24 months

Coordination Between the Cybersecurity Civilian and Defence Spheres (and II)

Outcomes and deliverables

- Concrete activities such as discussions, meetings, white papers, workshops, which strengthen the links between the cybersecurity civilian and defence spheres.
- Synergies between these communities, such as common activities to exchange know-how and information.

KPIs to measure outcomes and deliverables

- Number of cybersecurity workshops/trainings/events organised, as well as the number of participants per each of them; Number of stakeholders from both communities involved in organised activities
- Number of common activities involving both communities
- Number of Industrial stakeholders, including large enterprises, SMEs and start-ups participating in cybersecurity activities that are directly relevant for the defence and civilian sector.
- Number of active collaborations implemented with other relevant initiatives or European players.
- White papers produced aiming to support the implementation of better cooperation between the two communities.

Standardisation in the Area of Cybersecurity (I)

Objective

- Support further standardisation in the area of cybersecurity
- Re: the proposed Cyber Resilience Act with a view to improve the awareness and engage stakeholders in standardisation work

Scope

- Ensure wide stakeholder participation in standardisation activities
  - in particular in relation facilitate the implementation of the Cyber Resilience Act
- Meetings, workshops and collaborative activities, with both the private and the public sector

Targeted stakeholders

- Cybersecurity standardisation stakeholders
  - European standardisation and conformity assessment bodies
- Industrial players, including SMEs and start-ups
- *Multi-country consortia are not mandatory but will positively contribute to the impact of the action*

Coordination and Support Actions

- 100% funding rate
- EUR 3M
- 36mos

Standardisation in the Area of Cybersecurity (II)

Outcomes and deliverables

- Organization of events, workshops, stakeholder consultations, and production of white papers, all fostering the development of harmonised standards and conformity with requirements stemming from above mentioned legislative framework.
- Support for participation of relevant European experts in European and international cybersecurity standardisation fora.

KPIs to measure outcomes and deliverables

- Number of standardisation work items directly relevant for the development of harmonised standards for CRA presented in white papers, reporting on substantive discussions, options considered, conclusions taken and their relevance to the policy objectives.
- Number of experts participating in cybersecurity standardisation activities that are directly relevant for the development of harmonised standards for CRA.
- Number of standardisation activities in the area of cybersecurity that are directly relevant for the development of harmonised standards for CRA.
- Number of SMEs and start-ups participating in cybersecurity standardisation activities that are directly relevant for the development of harmonised standards for CRA.
- Number of cybersecurity standardisation workshops/trainings/events organised, as well as the number of attendees per each of them.
- Number of active collaborations implemented with other relevant initiatives or European players.
- Number of open access guidance material produced aiming to support the implementation of standards developed for the CRA and to support conformity with the requirements of the CRA
- Number of open access educational/audio-visual material produced aiming to support the implementation of standards developed for the CRA and to support conformity with the requirements of the CRA.

Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies

Objectives

- At least one of these objectives:
  - Development of trust between MSs
  - Effective operational cooperation of organisations entrusted with EU or Member State's national level cybersecurity
    - In particular cooperation of CSIRTs or Operators of Essential Services
  - Better security and notification processes and means for OESs
  - Improved cybersecurity of information systems in the EU
  - Alignment of MSs' implementations of NIS2
  - Support certification in line with the Cybersecurity Act

Scope

- At least one of the following priorities:
  - Improve the monitoring and handling of incidents
  - Collaboration, communication, awareness-raising activities, knowledge exchange and training
  - Twinning schemes involving at least two different MSs
  - […]
  - Enable businesses across all sectors and consumers to use products with digital elements securely.
  - Support to cybersecurity certification

Targeted stakeholders

- Industrial stakeholders, including SMEs and start-ups
- MSs' competent authorities
- CSIRTs, including sectorial CSIRTs
- SOCs
- OESs
- ISACs
- Actors in the Cyber Resilience Act (including certification bodies)
- Multi-country consortia are not mandatory but will positively contribute to the impact of the action

Simple Grants

- 50% funding rate
- EUR 30M
- 36mos
- Indicative budget: EUR 1-5M per action

DIGITAL
EUROPE
PROGRAMME

Support for Implementation of EU Legislation on Cybersec and National Cybersec Strategies (and II)

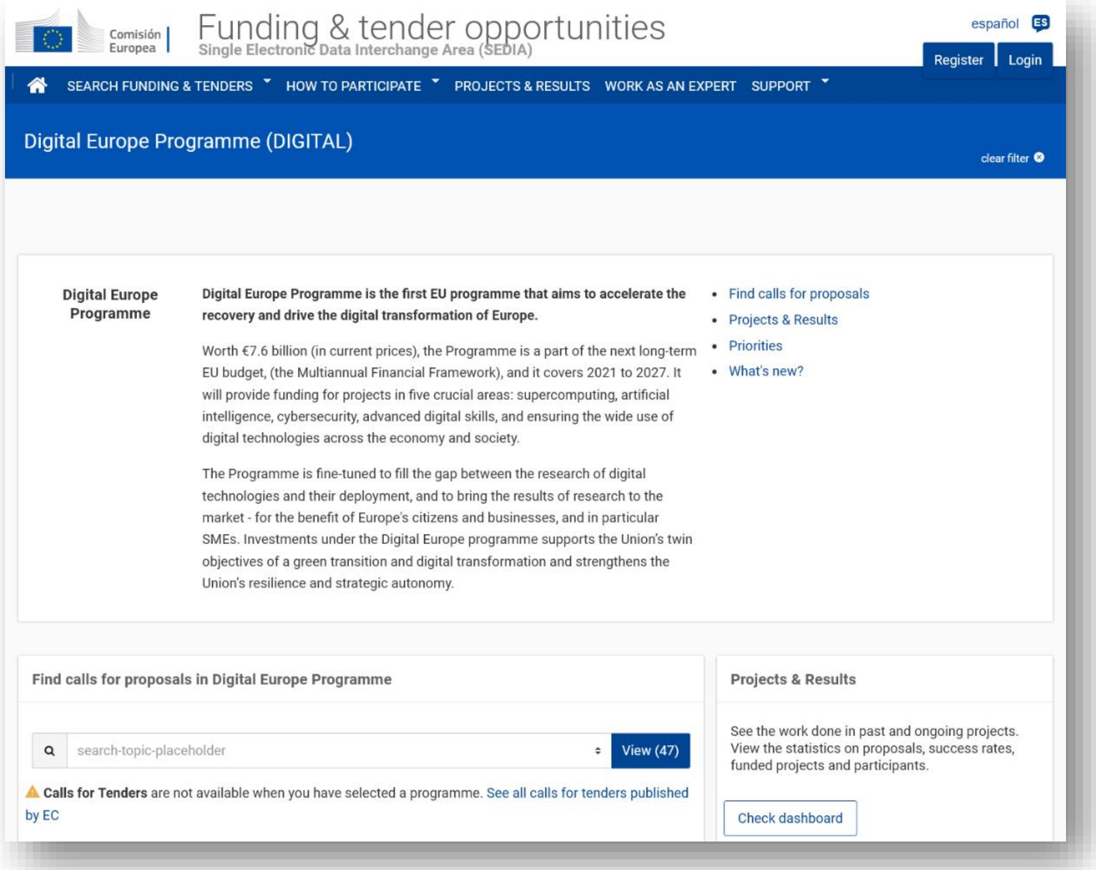
Outcomes and deliverables

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.
- Organization of events, workshops, stakeholder consultations and white papers.
- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.
- Support actions in the area of certification.

KPIs to measure outcomes and deliverables

- Number of technologies and IT-based solutions, processes and methods for handling cybersecurity incidents implemented, validated, piloted or deployed.
- Number of activities organised for collaboration, communication, awareness-raising or knowledge exchange and training (on the implementation of the NIS2 Directive).
- Number of twinning schemes implemented between at least two Member States for effective cross-border collaboration preventing, detecting and countering cybersecurity incidents.
- […]
- Number of communication, awareness-raising events, knowledge exchange and training activities about the rules of the CRA.
- Number of activities organised to promote sharing of technical specifications, best practices and use-cases amongst actors that have obligations under the CRA.
- Uptake of CRA compliant products across sectors.

Funding & tender portal



Digital Europe Programme (DIGITAL)

Digital Europe Programme

Digital Europe Programme is the first EU programme that aims to accelerate the recovery and drive the digital transformation of Europe.

Worth €7.6 billion (in current prices), the Programme is a part of the next long-term EU budget, (the Multiannual Financial Framework), and it covers 2021 to 2027. It will provide funding for projects in five crucial areas: supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and ensuring the wide use of digital technologies across the economy and society.

The Programme is fine-tuned to fill the gap between the research of digital technologies and their deployment, and to bring the results of research to the market - for the benefit of Europe's citizens and businesses, and in particular SMEs. Investments under the Digital Europe programme supports the Union's twin objectives of a green transition and digital transformation and strengthens the Union's resilience and strategic autonomy.

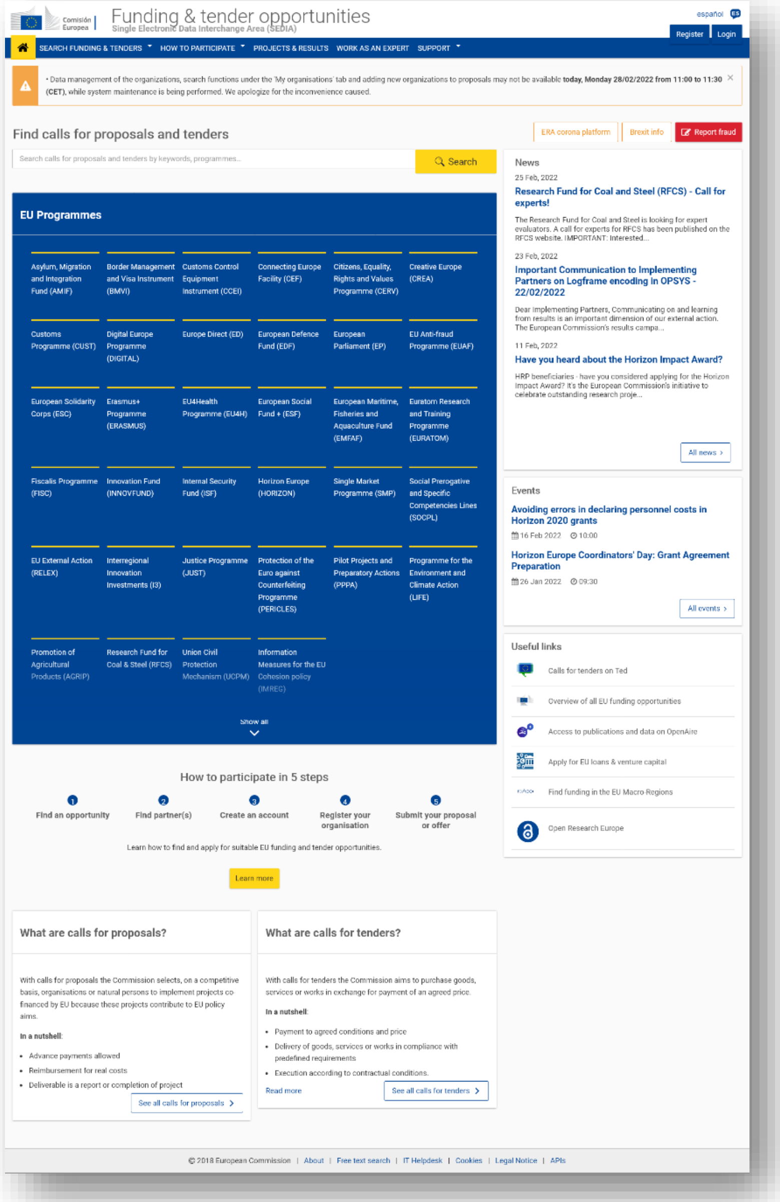
- Find calls for proposals
- Projects & Results
- Priorities
- What's new?

Find calls for proposals in Digital Europe Programme

⚠ **Calls for Tenders** are not available when you have selected a programme. See all calls for tenders published by EC

Projects & Results

See the work done in past and ongoing projects. View the statistics on proposals, success rates, funded projects and participants.



• Data management of the organizations, search functions under the 'My organisations' tab and adding new organizations to proposals may not be available **today, Monday 28/02/2022 from 11:00 to 11:30 (CET)**, while system maintenance is being performed. We apologize for the inconvenience caused.

Find calls for proposals and tenders

EU Programmes

Asylum, Migration and Integration Fund (AMIF)	Border Management and Visa Instrument (BMVI)	Customs Control Equipment Instrument (CCEI)	Connecting Europe Facility (CEF)	Citizens, Equality, Rights and Values Programme (CERV)	Creative Europe (CREA)
Customs Programme (CUST)	Digital Europe Programme (DIGITAL)	Europe Direct (ED)	European Defence Fund (EDF)	European Parliament (EP)	EU Anti-fraud Programme (EUAF)
European Solidarity Corps (ESC)	Erasmus+ Programme (ERASMUS)	EU4Health Programme (EU4H)	European Social Fund + (ESF)	European Maritime, Fisheries and Aquaculture Fund (EMFAF)	Euratom Research and Training Programme (EURATOM)
Fiscalis Programme (FISC)	Innovation Fund (INNOVFUND)	Internal Security Fund (ISF)	Horizon Europe (HORIZON)	Single Market Programme (SMP)	Social Prerogative and Specific Competencies Lines (SOCPL)
EU External Action (RELEX)	Interregional Innovation Investments (I3)	Justice Programme (JUST)	Protection of the Euro against Counterfeiting Programme (PERICLES)	Pilot Projects and Preparatory Actions (PPPA)	Programme for the Environment and Climate Action (LIFE)
Promotion of Agricultural Products (AGRIP)	Research Fund for Coal & Steel (RFCS)	Union Civil Protection Mechanism (UCPM)	Information Measures for the EU Cohesion policy (IMREG)		

How to participate in 5 steps

1. Find an opportunity
2. Find partner(s)
3. Create an account
4. Register your organisation
5. Submit your proposal or offer

Learn how to find and apply for suitable EU funding and tender opportunities.

What are calls for proposals?

With calls for proposals the Commission selects, on a competitive basis, organisations or natural persons to implement projects co-financed by EU because these projects contribute to EU policy aims.

In a nutshell:

- Advance payments allowed
- Reimbursement for real costs
- Deliverable is a report or completion of project

See all calls for proposals ›

What are calls for tenders?

With calls for tenders the Commission aims to purchase goods, services or works in exchange for payment of an agreed price.

In a nutshell:

- Payment to agreed conditions and price
- Delivery of goods, services or works in compliance with predefined requirements
- Execution according to contractual conditions.

Read more

See all calls for tenders ›

News

25 Feb, 2022

Research Fund for Coal and Steel (RFCS) - Call for experts!

The Research Fund for Coal and Steel is looking for expert evaluators. A call for experts for RFCS has been published on the RFCS website. IMPORTANT: Interested...

23 Feb, 2022

Important Communication to Implementing Partners on Logframe encoding in OPSYS - 22/02/2022

Dear Implementing Partners, Communicating on and learning from results is an important dimension of our external action. The European Commission's results campa...

11 Feb, 2022

Have you heard about the Horizon Impact Award?

HRP beneficiaries - have you considered applying for the Horizon Impact Award? It's the European Commission's initiative to celebrate outstanding research proje...

Events

Avoiding errors in declaring personnel costs in Horizon 2020 grants

16 Feb 2022 10:00

Horizon Europe Coordinators' Day: Grant Agreement Preparation

26 Jan 2022 09:30

Useful links

- Calls for tenders on Ted
- Overview of all EU funding opportunities
- Access to publications and data on OpenAire
- Apply for EU loans & venture capital
- Find funding in the EU Macro-Regions
- Open Research Europe

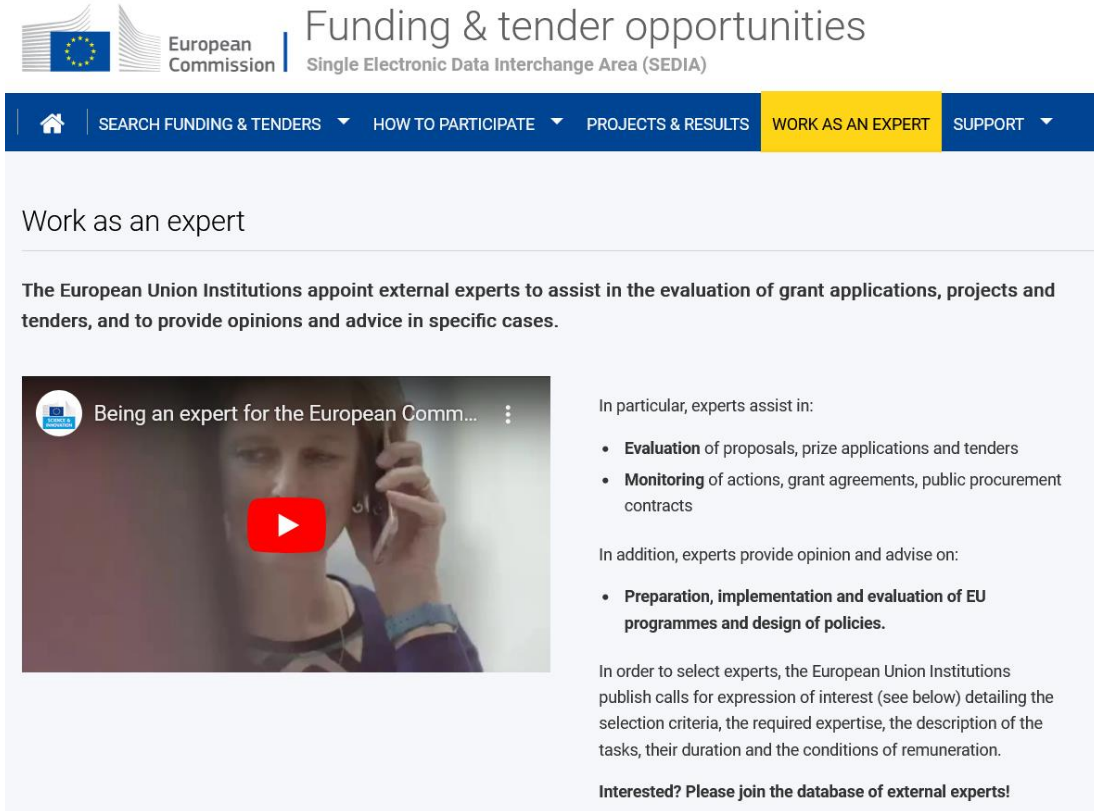
© 2018 European Commission | About | Free text search | IT Helpdesk | Cookies | Legal Notice | APIs

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

European Commission

Convertirse en *experto*

- Expertos externos asisten la CE en:
  - Evaluación de las propuestas, las solicitudes de premios y las ofertas
  - Seguimiento de las acciones, los acuerdos de subvención y los contratos públicos
- Toda la información en el *F&T Portal.*


European Commission
Funding & tender opportunities
Single Electronic Data Interchange Area (SEDIA)
SEARCH FUNDING & TENDERS
HOW TO PARTICIPATE
PROJECTS & RESULTS
WORK AS AN EXPERT
SUPPORT
Being an expert for the European Comm...

Work as an expert

The European Union Institutions appoint external experts to assist in the evaluation of grant applications, projects and tenders, and to provide opinions and advice in specific cases.

In particular, experts assist in:

- **Evaluation** of proposals, prize applications and tenders
- **Monitoring** of actions, grant agreements, public procurement contracts

In addition, experts provide opinion and advise on:

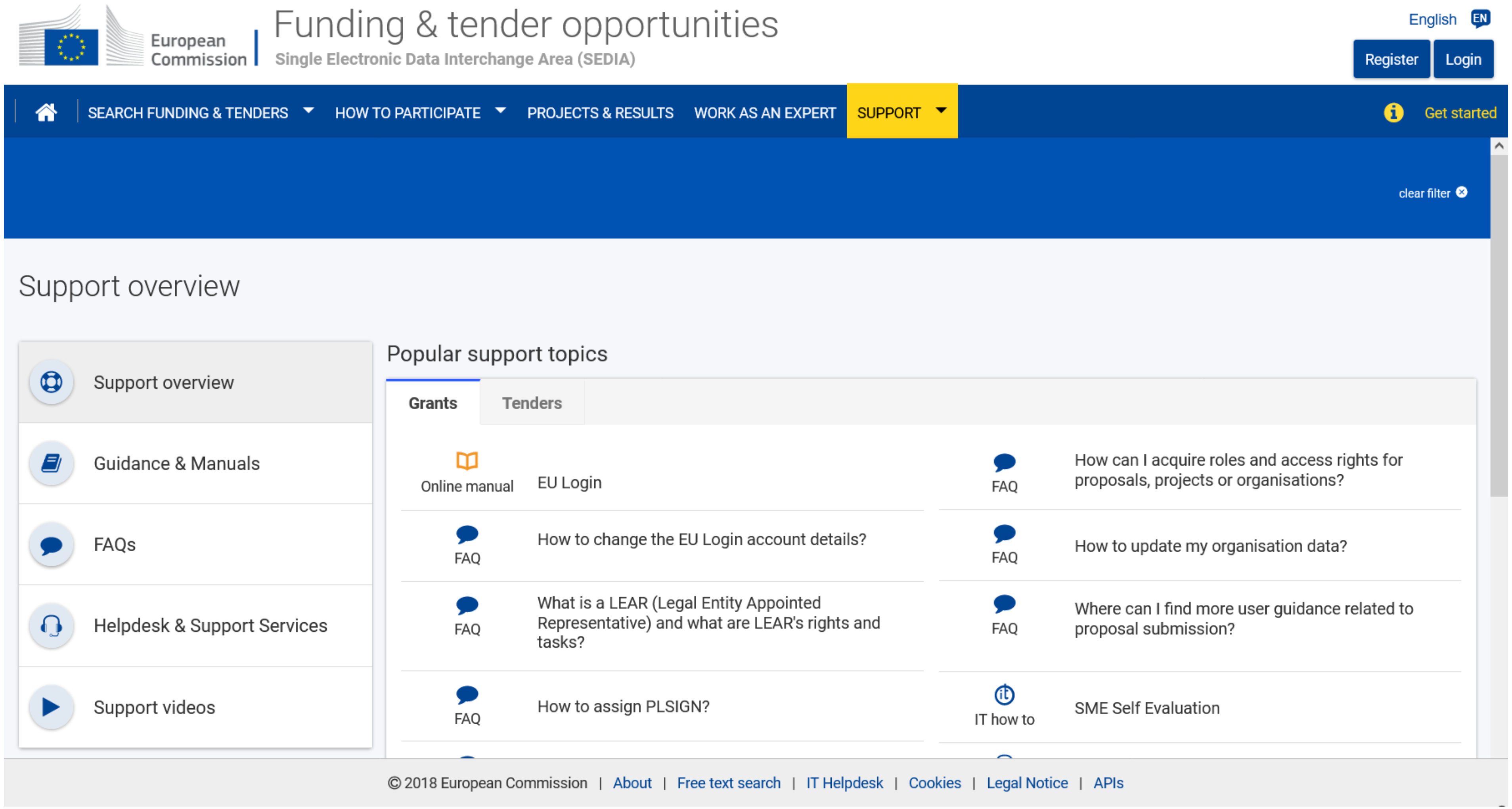
- **Preparation, implementation and evaluation of EU programmes and design of policies.**

In order to select experts, the European Union Institutions publish calls for expression of interest (see below) detailing the selection criteria, the required expertise, the description of the tasks, their duration and the conditions of remuneration.

Interested? Please join the database of external experts!

DIGITAL EUROPE PROGRAMME

¿Preguntas?



European Commission

Funding & tender opportunities

Single Electronic Data Interchange Area (SEDIA)

English EN

Register Login

SEARCH FUNDING & TENDERS ▾ HOW TO PARTICIPATE ▾ PROJECTS & RESULTS WORK AS AN EXPERT SUPPORT ▾ Get started

clear filter

Support overview

- Support overview
- Guidance & Manuals
- FAQs
- Helpdesk & Support Services
- Support videos

Popular support topics

Grants | Tenders

Online manual	EU Login	FAQ	How can I acquire roles and access rights for proposals, projects or organisations?
FAQ	How to change the EU Login account details?	FAQ	How to update my organisation data?
FAQ	What is a LEAR (Legal Entity Appointed Representative) and what are LEAR's rights and tasks?	FAQ	Where can I find more user guidance related to proposal submission?
FAQ	How to assign PLSIGN?	IT how to	SME Self Evaluation

© 2018 European Commission | About | Free text search | IT Helpdesk | Cookies | Legal Notice | APIs

Información adicional (DIGITAL)

Convocatoria - Apoyo fundamental

- Detalles sobre la **admisibilidad y admisibilidad**
- Información a los solicitantes sobre la **capacidad financiera y operativa**
- Criterios de exclusión
- **Procedimiento de evaluación**
- Garantías, hitos y entregables obligatorios, certificados y cualquier otra descripción de las condiciones legales para participar en subvenciones
- Apoyo financiero a terceros
- Todos los **anexos obligatorios** para la convocatoria (por ejemplo, cuestiones éticas, de seguridad)
- Descripción del **tipo de acción**
- Otras disposiciones jurídicas y operativas importantes
- **Ayuda a los solicitantes** y cómo contactar la Comisión

Criterios de adjudicación

Pertinencia

- Alineación con los objetivos y actividades
- Contribución a los objetivos estratégicos y políticos a largo plazo
- Refuerzo de la cadena de suministro de tecnología digital de la Unión*
- Resiliencia frente a los obstáculos financieros*

Aplicación

- Madurez de la acción propuesta
- Solidez y eficiencia del plan de ejecución
- Capacidad de los solicitantes para llevar a cabo el trabajo propuesto

Impacto

- Logro de los resultados esperados, así como comunicación y difusión
- Fortalecimiento de la competitividad y contribución a la sociedad
- Sostenibilidad ambiental*

* La convocatoria establece la aplicabilidad de estos criterios

Categorías presupuestarias y costes aceptables (I)

- A. Gastos de personal
  - A.1 Empleados, A.2 Personas físicas con contrato directo, A.3 Personas en comisión de servicio y A.4 propietarios de PYME y beneficiarios de personas físicas
- C. Compras
  - C.1 Viajes y dietas
  - C.2 Equipos
  - C.3 Otros bienes, obras y servicios

- B. Gastos de subcontratación
- Restricciones debidas a la seguridad:
  - El trabajo subcontratado debe realizarse en los países elegibles
  - Solo son subvencionables los costes de las actividades realizadas en los países subvencionables

Categorías presupuestarias y costes aceptables (II)

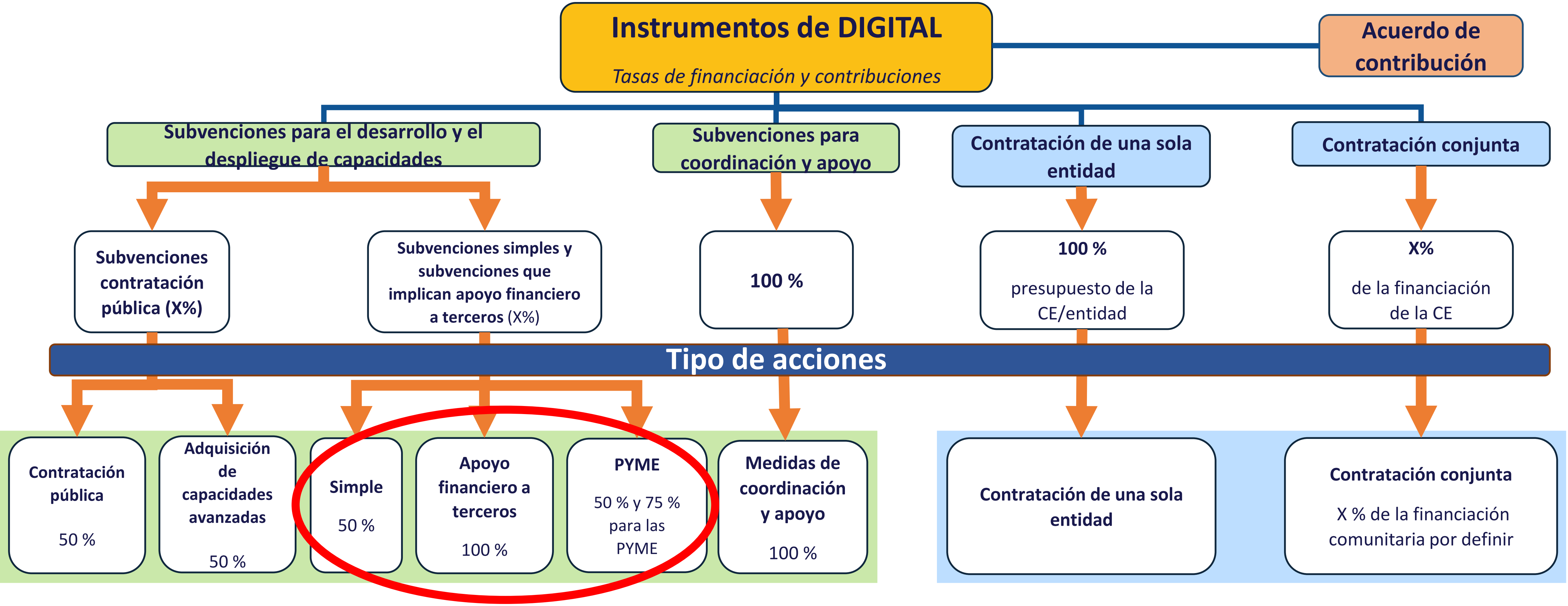
- Otras categorías de costes. Costes de apoyo financiero a terceros (*Financial Support to Third Parties – FSTP*)
  - Importe máximo por tercero (i.e., 60 000 EUR), a menos que se exija un importe superior debidamente justificado en el formulario de solicitud

- Propuesta para proporcionar:
  - por qué se necesita FSTP,
  - cómo se gestionará,
  - una lista de los diferentes tipos de actividades que pueden recibir apoyo, y
  - los resultados a obtener.

Categorías presupuestarias y costes aceptables (III)

- Las convocatorias *FSTP* debe seguir las siguientes condiciones:
  - abiertas, publicadas ampliamente y ajustarse a las normas de la UE en materia de transparencia, igualdad de trato, conflicto de intereses y confidencialidad;
  - publicarse en el *Funding & Tenders Portal* y en los sitios web de los participantes;
  - permanecer abiertas durante al menos dos meses;
  - si se modifican los plazos de convocatoria, esto debe publicarse inmediatamente y todos los solicitantes registrados deben ser informados del cambio;
  - el resultado de la convocatoria debe publicarse en los sitios web de los participantes, incluida una descripción de los proyectos seleccionados, las fechas de adjudicación, la duración del proyecto y los nombres legales del destinatario final y los países;
  - las convocatorias deben tener una clara dimensión europea.

Instrumentos y tipos de acciones



Instrumentos de DIGITAL

Tasas de financiación y contribuciones

Acuerdo de contribución

Subvenciones para el desarrollo y el despliegue de capacidades

- **Subvenciones contratación pública (X%)**
- **Subvenciones simples y subvenciones que implican apoyo financiero a terceros** (X%)

Subvenciones para coordinación y apoyo

- **100 %**

Contratación de una sola entidad

- **100 %** presupuesto de la CE/entidad

Contratación conjunta

- **X%** de la financiación de la CE

Tipo de acciones

- **Contratación pública** 50 %
- **Adquisición de capacidades avanzadas** 50 %
- **Simple** 50 %
- **Apoyo financiero a terceros** 100 %
- **PYME** 50 % y 75 % para las PYME
- **Medidas de coordinación y apoyo** 100 %
- **Contratación de una sola entidad**
- **Contratación conjunta** X % de la financiación comunitaria por definir

Keep in touch

ec.europa.eu/

europa.eu/

@EU_Commission

@EuropeanCommission

European Commission

europeancommission

@EuropeanCommission

EUTube

EU Spotify

¡Gracias!

Picture on slide #10 by Piotr Małecki, CC BY-SA 3.0 via Wikimedia Commons.

European Commission