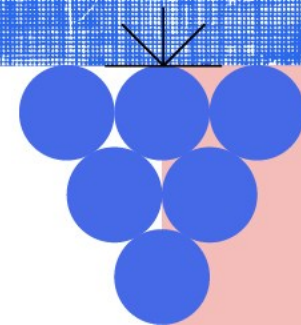


# Horizonte Europa 2026-2027 – Cluster 3 Digital Europe Programme (DIGITAL).



**NCC-PT**

PORTUGAL CYBERSECURITY  
COORDINATION CENTRE



# O Centro Europeu de Competências em Cibersegurança e a rede de Centros Nacionais de Coordenação

**Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho de 20  
de maio de 2021**

- **Cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC) e a Rede de Centros Nacionais de Coordenação (NCCs)**

**Promover a investigação, a inovação e adoção de produtos e serviços inovadores no domínio da cibersegurança**



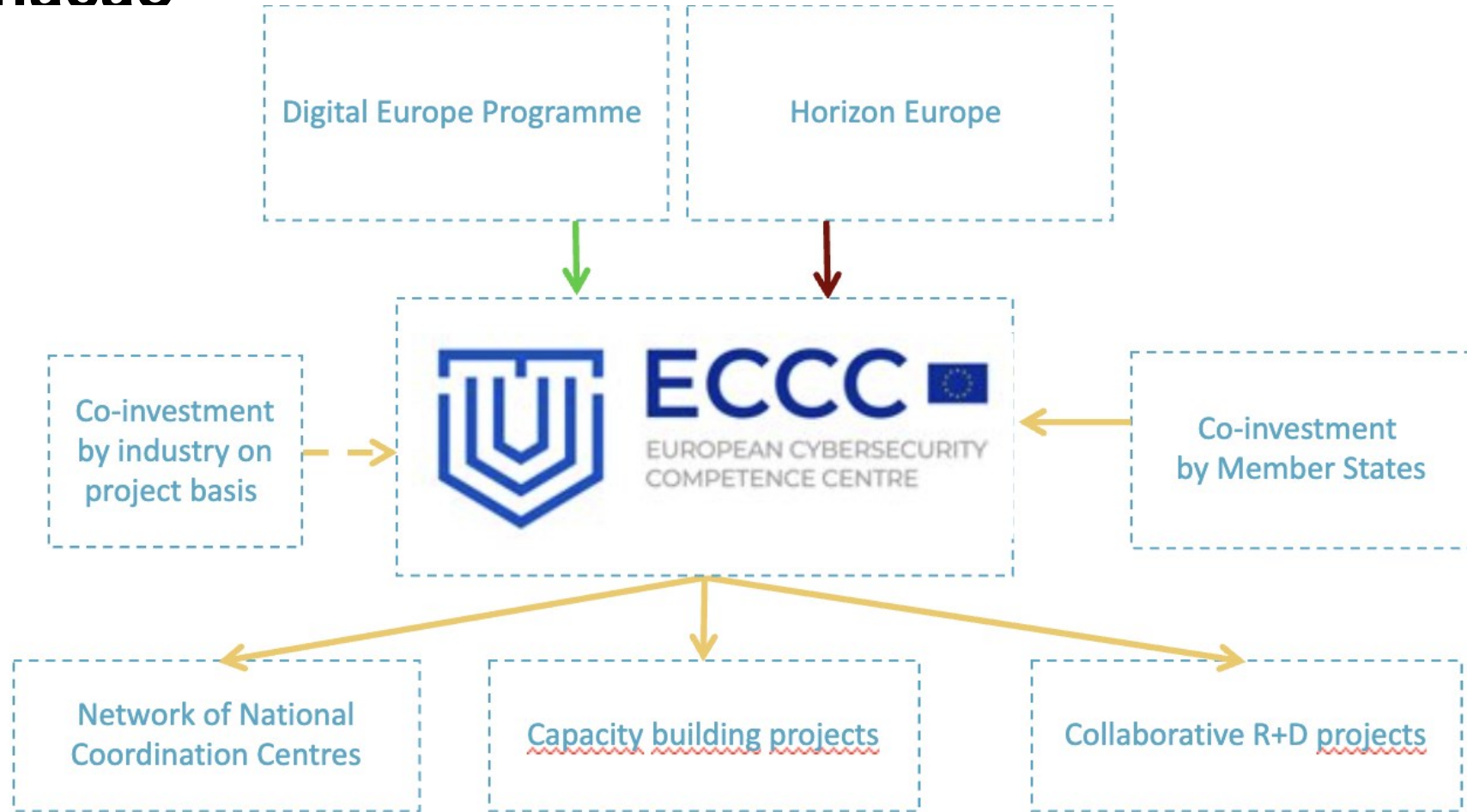
# O Centro Europeu de Competências em Cibersegurança e a rede de Centros Nacionais de Coordenação



- Reforçar a liderança e autonomia estratégica no domínio da cibersegurança, conservando e desenvolvendo as capacidades e aptidões de investigação, académicas, societárias, tecnológicas e industriais no domínio da cibersegurança;
- Apoiar as capacidades e competências tecnológicas da União em relação à resiliência e fiabilidade das infraestruturas de redes e sistemas de informação, incluindo as infraestruturas críticas o *hardware* e *software* de uso comum; e
- Aumentar a competitividade global da indústria de cibersegurança da União, assegurando normas elevadas de cibersegurança e transformar a cibersegurança numa vantagem competitiva.



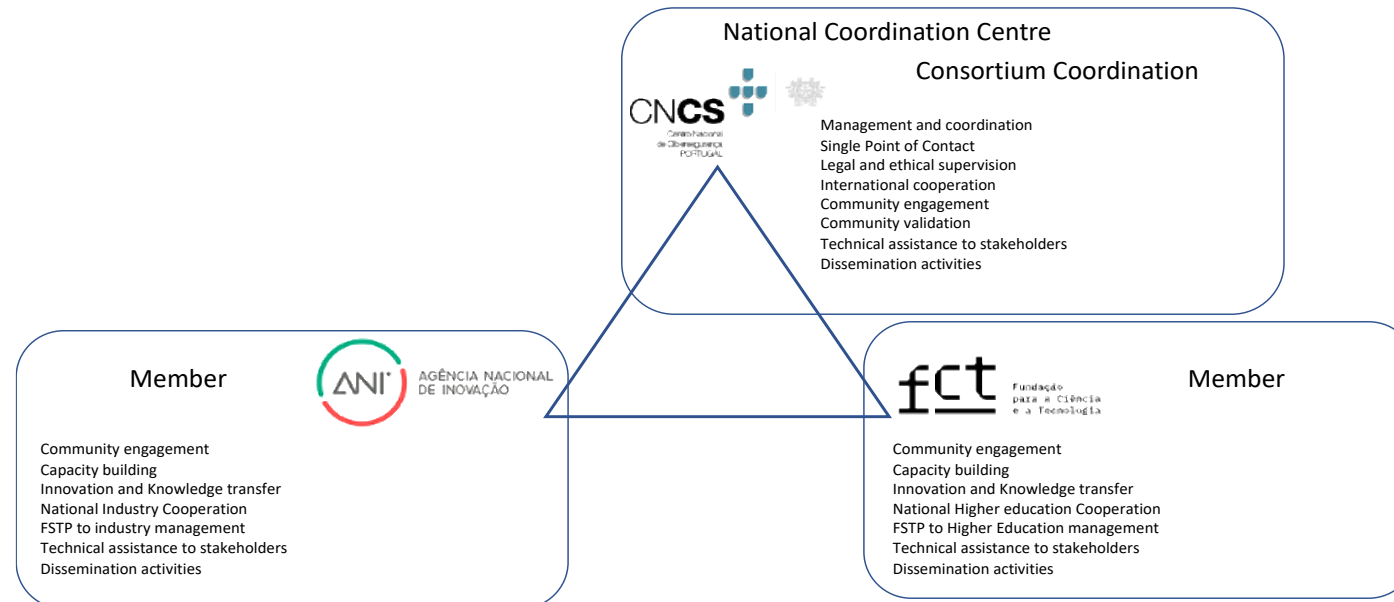
# O Centro Europeu de Competências em Cibersegurança e a rede de Centros Nacionais de Coordenação



# Em Portugal - O NCC-PT

Despacho 11491/2022 de 28 setembro

Designa o Centro Nacional de Cibersegurança como centro nacional de coordenação para efeitos do Regulamento (EU) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, e criação de consórcio entre o Centro Nacional de Cibersegurança, a Agência Nacional de Inovação, S. A., e a Fundação para a Ciência e a Tecnologia, I. P.



# Em Portugal - O NCC-PT

## Artigo 7º do Regulamento (1/2)

- a) Atuar como ponto de contacto a nível nacional para a Comunidade
- b) Fornecer conhecimentos especializados e contribuir ativamente para as atribuições estratégicas estabelecidas no artigo 5º do nº 2 (**atribuições estratégicas do ECCC**), tendo em conta os desafios nacionais e regionais pertinentes em matéria de cibersegurança em diferentes setores
- c) Promover, incentivar e facilitar a participação da sociedade civil, da indústria, em especial de empresas em fase de arranque e de PME, das comunidades académica e de investigação e de outras partes interessadas a nível nacional em projetos transfronteiriços e em ações no domínio da cibersegurança financiadas pelos programas pertinentes da União;
- d) Prestar assistência técnica às partes interessadas, apoiando-as na sua fase de candidatura aos projetos geridos pelo Centro de Competências
- e) Procurar estabelecer sinergias com atividades relevantes a nível nacional, regional e local, como, por exemplo, as políticas nacionais em matéria de investigação, desenvolvimento e inovação no domínio da cibersegurança, nomeadamente as políticas indicadas nas estratégias nacionais de cibersegurança;



# Em Portugal - O NCC-PT

## Artigo 7º do Regulamento (2/2)

f) Executar ações específicas para as quais o Centro de Competências tenha concedido subvenções, nomeadamente através da prestação de apoio financeiro a terceiros

g) Sem prejuízo das competências dos Estados-Membros em matéria de educação e tendo em conta as atribuições pertinentes da ENISA, colaborar com as autoridades nacionais no que diz respeito a uma possível contribuição para a promoção e difusão de programas educativos em matéria de cibersegurança

h) Promover e difundir os resultados pertinentes do trabalho da Rede, da Comunidade e do Centro de Competências a nível nacional, regional ou local

i) Avaliar os pedidos apresentados por entidades estabelecidas no mesmo Estado-Membro ao centro nacional de coordenação com vista a fazerem parte da Comunidade

j) Preconizar e promover a participação de entidades pertinentes nas atividades desenvolvidas pelo Centro de Competências, pela Rede e pela Comunidade e acompanhar, consoante necessário, o nível de participação e montante do apoio financeiro público concedido à investigação, desenvolvimento e implantação no domínio da cibersegurança



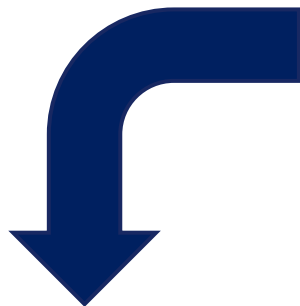
# A Comunidade de Cibersegurança

Comunidade Nacional (via NCC-PT)	Comunidade ATLAS (via ECCC)
Acesso facilitado a informação sobre oportunidades de financiamento nacionais e europeias	Participação direta em iniciativas e projetos europeus de grande escala
Apoio técnico do NCC-PT nas candidaturas e no alinhamento com políticas nacionais	Integração em redes europeias de excelência em cibersegurança
Possibilidade de criação de parcerias locais e sinergias com entidades portuguesas	Maior visibilidade internacional e acesso a parcerias transnacionais
Preparação e capacitação para o envolvimento em projetos europeus	Acesso a informação estratégica da UE e envolvimento em decisões estruturantes da comunidade
Representação dos interesses nacionais junto da estrutura europeia	Oportunidade de liderar ou integrar consórcios europeus em cibersegurança
Contribuição para a implementação da Estratégia Nacional de Cibersegurança	Contribuição direta para a autonomia digital europeia



# A Comunidade de Cibersegurança

## *Comunidade Nacional*



- *Entidades estabelecidas em Portugal e ativas na área da cibersegurança:*
  - *Empresas (incluindo Startups e PMEs)*
  - *Universidades e Centros de I&D*
  - *Entidades públicas*
  - *Associações, clusters e redes de inovação*

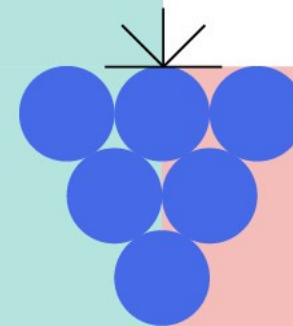
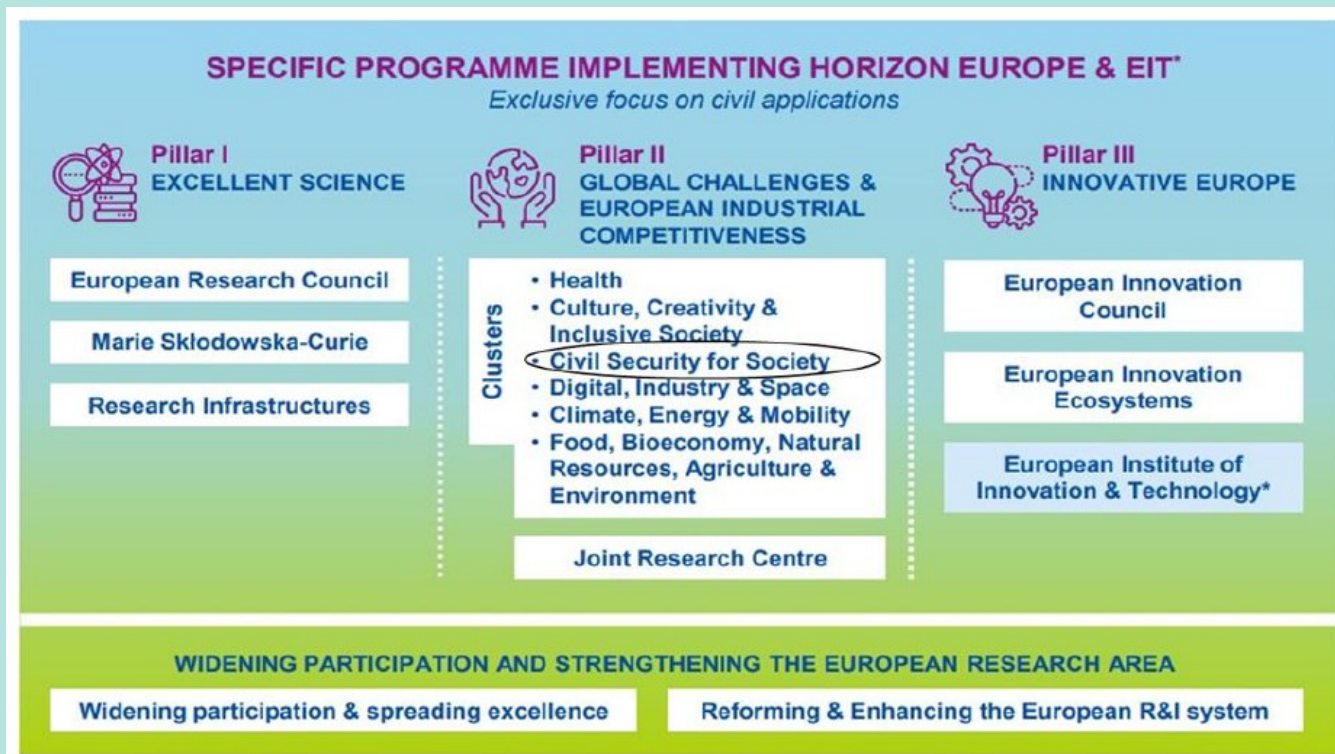
## *Comunidade Atlas*

*As entidades devem demonstrar a sua capacidade para contribuir para a missão e que possuem conhecimentos especializados em matéria de cibersegurança no tocante a, pelo menos, um dos seguintes domínios:*

- a) Meio académico, investigação ou inovação;*
- b) Desenvolvimento industrial ou de produtos;*
- c) Formação e educação;*
- d) Segurança da informação ou operações de resposta a incidentes;*
- e) Ética;*
- f) Normalização e especificações formais e técnicas.*



# Programa de Trabalhos do Horizonte Europa 2026-2027



## Cluster 3 – Civil Security for Society

O Cluster 3 fornece uma resposta de investigação e inovação a um contexto de ameaças e desafios em rápida evolução para a segurança interna, a segurança dos cidadãos, das infraestruturas críticas e da sociedade no seu todo.

(Programa de Trabalhos do Horizonte Europa 2026-2027)



# Cluster 3 – Civil Security for Society

- **Destino – Cibersegurança**
- **Ações propostas:**
  - Reforçar a capacidade da UE para detetar, prevenir e responder a ciberameaças, incluindo as que visam infraestruturas críticas;
  - Contribuir para a autonomia estratégica aberta da Europa, apoiando o desenvolvimento de infraestruturas digitais fiáveis, tecnologias emergentes, capacidades de cibersegurança e cadeias de abastecimento seguras.
- **Impactos esperados:**
  - Aumento da cibersegurança e de um ambiente online mais seguro através do desenvolvimento e utilização eficaz das capacidades da UE e dos Estados-Membros em tecnologias digitais para proteção de dados e redes;
  - Promoção da soberania tecnológica neste domínio, respeitando simultaneamente a privacidade e os direitos fundamentais;
  - Contribuição para serviços, processos e produtos seguros, bem como para infraestruturas digitais robustas capazes de resistir e contrariar ciberataques e ameaças híbridas.



# Cluster 3 – Civil Security for Society

- **HORIZON-CL3-2026-02-CS-ECCC – Três tópicos**
  - **Abertura da call:** 09 março 2026
  - **Prazo de submissão:** 15 setembro 2026, 17:00:00 CET (Bruxelas)
  - **Avaliação:** novembro 2026
  - **Resultados da avaliação:** janeiro 2027
  - **Assinatura do Grant Agreement:** maio 2027



# HORIZON-CL3-2026-02-CS-ECCC

HORIZON-CL3-2026-02-CS-ECCC-01 (RIA)

EUR  
20 000 000

Approaches and tools for security in software and hardware development and assessment

HORIZON-CL3-2026-02-CS-ECCC-02 (IA)

EUR  
21 200 000

Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

HORIZON-CL3-2026-02-CS-ECCC-03 (RIA)

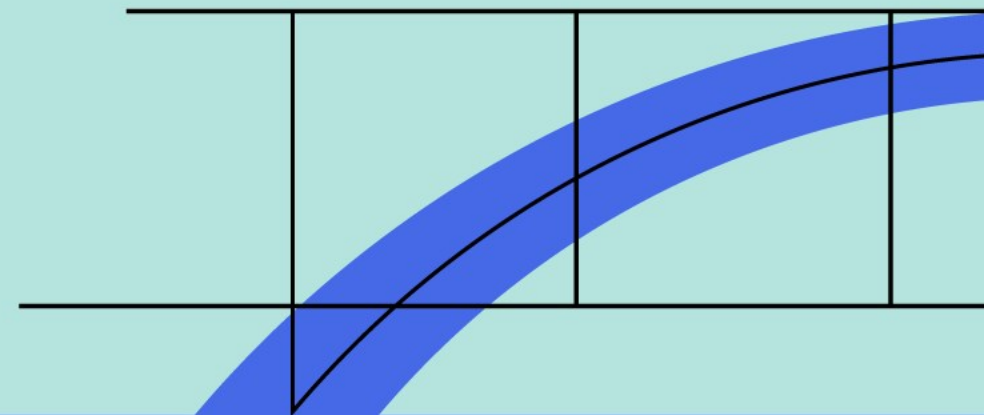
EUR  
15 000 000

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations



# HORIZON-CL3-2026-02-CS-ECCC-01

*Approaches and tools for security in software and hardware development and assessment*



# HORIZON-CL3-2026-02-CS-ECCC-01 (1/3)

## Âmbito

A crescente complexidade e globalização das cadeias de abastecimento de software e hardware introduzem novas vulnerabilidades exploráveis por adversários cibernéticos. Garantir a **segurança de componentes de software e hardware** ao longo de todo o ciclo de vida dos sistemas digitais é essencial. O tópico pretende apoiar o desenvolvimento de **ferramentas e processos inovadores**, que visem assegurar todo o ecossistema de desenvolvimento de software e hardware.

As propostas devem explicitamente ter uma área de foco, mas podem abordar ambas:

- a) **Sistemas de hardware seguros baseados em chips confiáveis**
- b) **Segurança da cadeia de abastecimento de software**

# HORIZON-CL3-2026-02-CS-ECCC-01 (2/3)

## Resultados esperados

- Quadros de **segurança reforçados para cadeias de hardware e software**, assentes em arquiteturas *root-of-trust* e gestão segura do ciclo de vida;
- **Arquiteturas de chips seguras e confiáveis** para sistemas de computação e redes de próxima geração;
- **Abordagens integradas de *security-by-design*** no desenvolvimento de software, alinhadas com requisitos regulamentares;
- **Metodologias de testes de segurança**, incluindo verificação formal e testes orientados por IA;
- Metodologias normalizadas para **avaliação de segurança de hardware**, contribuindo para certificação em cibersegurança.



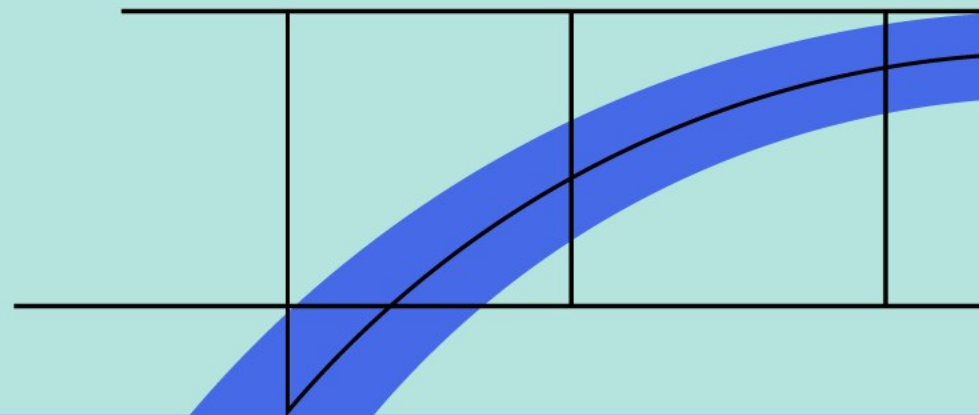
# HORIZON-CL3-2026-02-CS-ECCC-01 (3/3)

- Tipo de ação:  
*Research and Innovation Actions (RIA)*
- Montante por projeto:  
EUR 3–4 milhões
- Número indicativo de projetos financiados:  
4–5



# HORIZON-CL3-2026-02-CS-ECCC-02

*Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)*



# HORIZON-CL3-2026-02-CS-ECCC-02 (1/3)

## Âmbito

Reforçar a resiliência dos sistemas e algoritmos de IA face a várias ameaças e ataques, tais como o reforço da resistência contra ataques adversariais, injeções de *backdoors* e *data poisoning*.

As propostas objetivam desenvolver técnicas de deteção de anomalias em tempo real e de mitigação para defesa contra ataques adversariais, bem como técnicas robustas de aprendizagem federada, em sinergia com os principais esforços em matéria de transparência da IA e em conformidade com o AI Act.



# HORIZON-CL3-2026-02-CS-ECCC-02 (2/3)

## Resultados esperados

- **Modelos e sistemas de IA robustos** capazes de resistir a diferentes classes de manipulação adversarial;
- **Mecanismos de defesa inovadores** para modelos e sistemas de IA contra novas famílias de ataques;
- Metodologias **para deteção e mitigação** de *data poisoning*, *backdoors* e *misclassification*;
- Sistemas de IA que utilizam **tecnologias de melhoria da privacidade** que mantenham a confidencialidade dos dados e a conformidade regulamentar, permitindo implementações internas de IA fiáveis (por exemplo, para governos e empresas).



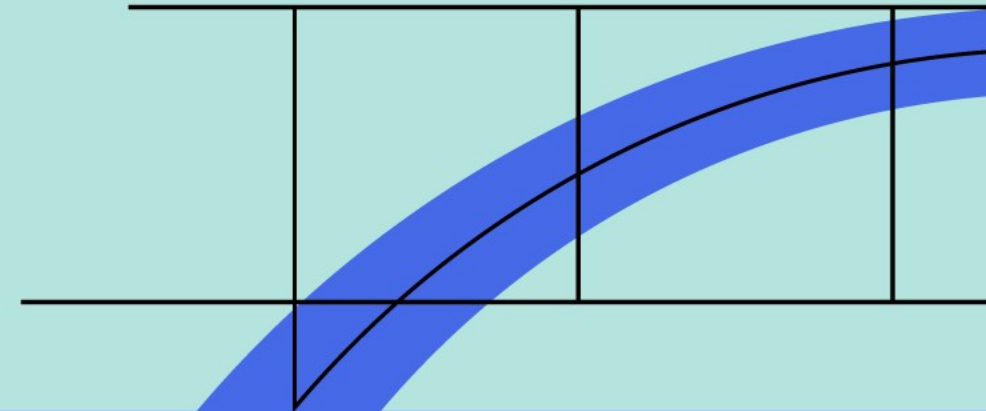
# HORIZON-CL3-2026-02-CS-ECCC-02 (3/3)

- Tipo de ação:  
*Innovation Actions (IA)*
- Montante por projeto:  
EUR 3–4 milhões
- Número indicativo de projetos financiados:  
4–5



# HORIZON-CL3-2026-02-CS-ECCC-03

*Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations*



# HORIZON-CL3-2026-02-CS-ECCC-03 (1/3)

## Âmbito

Desenvolvimento de **novas assinaturas digitais e esquemas criptográficos avançados** para *wallets/eIDs* em aplicações de privacidade e negócio;

Desenvolvimento de ***High-Assurance Cryptographic Software (HACS)*** incluindo métodos automatizados de avaliação.



# HORIZON-CL3-2026-02-CS-ECCC-03 (2/3)

## Resultados Esperados

- Primitivas criptográficas com resistência quântica, incluindo, se for o caso, abordagens e esquemas que não se baseiem modelos de *Lattice* e que reforcem a segurança e a privacidade das carteiras digitais (wallets/eIDs);
- Ferramentas de verificação formal, abordagens melhoradas de *High-Assurance Cryptographic Software* (HACS) e a sua integração em fluxos de trabalho de software, para proporcionar garantias de segurança robustas na migração pós-quântica e permitir uma avaliação simplificada e baseada em evidências de sistemas seguros que utilizam criptografia.



# HORIZON-CL3-2026-02-CS-ECCC-03 (3/3)

- Tipo de ação:  
*Research and Innovation Actions (RIA)*
- Montante por projeto:  
*EUR 3–4 milhões*
- Número indicativo de projetos financiados:  
4–5



# HORIZON-CL3-2026-02-CS-ECCC

## Elegibilidade

- Apenas entidades estabelecidas em Estados-Membros ou Países Associados;
- Entidades controladas direta ou indiretamente por países não elegíveis não podem participar.

## Modelo financeiro

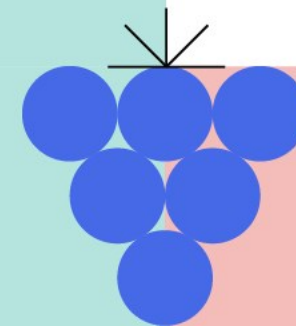
- Lump Sum

## Segurança

- Possível utilização ou produção de informação classificada (EUCI e SEN).



# PROGRAMA DE TRABALHOS DEP- 2025-2027



# PROGRAMA DE TRABALHOS 2025-2027

## O Programa de Trabalhos sobre Cibersegurança do ECCC 2025-2027

Centrado na promoção da cibersegurança da UE com financiamento de projetos em áreas como a transição para infraestruturas pós-quânticas, a criação de uma infraestrutura europeia de testes para criptografia pós-quântica (PQC) e a implementação de ferramentas de cibersegurança baseadas em IA para melhorar a deteção e análise de ameaças.

O programa inclui também iniciativas para reforçar as capacidades de cibersegurança para as PME e prestadores serviços essenciais, em particular os prestadores de cuidados de saúde,

**Call de financiamento específicos e um investimento total de 355 milhões de euros até 2027**



# PROGRAMA DE TRABALHOS 2025-2027

**Dotação de aproximadamente 355M€ em ações de uptake focadas em 3 objetivos específicos**

1	Uptake de tecnologias emergentes ( IA, Transição Pós-Quântica, entre outros)
2	Implementação do Cyber Solidarity Act
3	Ações focadas no aumento da maturidade e resiliência ( NIS2, CRA, DORA, CSA, RGPD e IA Act) - Importância dada à área da saúde



# PROGRAMA DE TRABALHOS 2025-2027

Areas and topics with indicative allocations (in million EUR)		2025	2026	2027	Total
<b>New technologies, AI &amp; post-quantum transition</b>					<b>139</b>
2.1	Cybersecure tools, technologies and services relying on AI	15	15	15	45
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions		20		20
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	25			25
2.4	Transition to post-quantum Public Key Infrastructures	15			15
2.5	Migration of Cyber Hubs to PQC			4	4
2.6	Uptake of innovative cybersecurity solutions for SMEs	15		15	30
<b>Cyber Solidarity Act and EU Action Plan on Cable Security Implementation</b>					<b>97</b>
2.7	National Cyber Hubs	5	5		10
2.8	Cross-Border Cyber Hubs	5		15	20
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		2		2
2.10	Coordinated preparedness testing and other preparedness actions	10	15	15	40
2.11	Mutual assistance		2	2	4
2.12	Regional Cable Hubs	10	5	6	21
<b>Additional actions improving EU cyber resilience</b>					<b>110</b>
2.13	Enhancing the NCC Network	10	11	17	38
2.14	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		20	12	32
2.15	Dedicated action to reinforce hospitals and healthcare providers	30			30
2.16	Dual-use technologies		10		10
<b>Programme Support Actions</b>		<b>3</b>	<b>3</b>	<b>3</b>	<b>9</b>
<b>TOTAL (in million EUR)</b>		<b>143</b>	<b>108</b>	<b>104</b>	<b>355</b>



# PROGRAMA DE TRABALHOS 2025-2027

Call planning 2025-2026 – Datas indicativas – datas sujeitas a alterações

	WP 2026	
	HE-2026	DEP-2026-11
Call publication	09/12/2025	01/09/2026
Call opening	March 2026	01/09/2026
Call Closing	15/09/2026	02/02/2027
Evaluation period	05/10-13/11/26	15/02-26/03/2027
Time to Inform (TTI)	mid December 2026	May 2027
Time to sign (TTS)	mid May 2027	end October 2027
total EU budget (EUR)	56,200,000	105,000,000

# Criação de consórcios & Boas práticas de candidatura



## Relevance

- Alignment with the objectives and activities
- Contribution to long-term policy and strategic objectives
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU\*



## Implementation

- Maturity of the proposed action
- Soundness and efficiency of the implementation plan
- Capacity of the applicants or consortium to carry out the proposed work



## Impact

- Achievement of the expected outcomes and deliverables, as well as communication and dissemination
- Competitiveness strengthen and contribution to society



# Criação de consórcios & Boas práticas de candidatura

## Construa um Consórcio Forte (se aplicável)

- *Inclua parceiros com competências complementares (técnicas, académicas, implementação, divulgação).*
- *Assegure o equilíbrio geográfico (especialmente para impacto europeu).*
- *Defina funções e responsabilidades claras (Work Packages).*
- *Estabeleça uma entidade coordenadora experiente com experiência na gestão de projetos europeus.*



# Criação de consórcios & Boas práticas de candidatura

## Papel do NCC-PT na Formação de Consórcios

### NCC-PT como facilitador estratégico

#### Missão:

- Apoiar entidades nacionais na integração em consórcios europeus competitivos, especialmente no contexto do Programa Europa Digital e Horizonte Europa.
- Contribuir ativamente para aumentar a visibilidade dos produtos e serviços de cibersegurança nacionais junto do ecossistema europeu, promovendo assim uma maior soberania digital europeia.



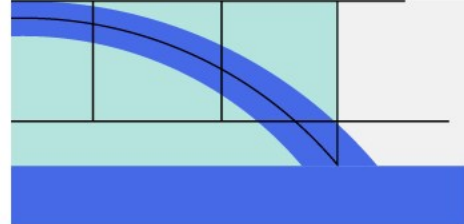
# Criação de consórcios & Boas práticas de candidatura

## Papel do NCC-PT na Formação de Consórcios

### Atividades principais

- **Matchmaking ativo**
  - Ligação entre parceiros nacionais e europeus
  - Identificação de complementaridades técnicas e estratégicas
- **Receção e difusão de pedidos de consórcios**
  - Apoio a entidades que procuram parceiros
  - Promoção de oportunidades junto do ecossistema nacional

**O NCC-PT atua como ponte entre oportunidades europeias e capacidades nacionais, acelerando a criação de consórcios sólidos e competitivos**



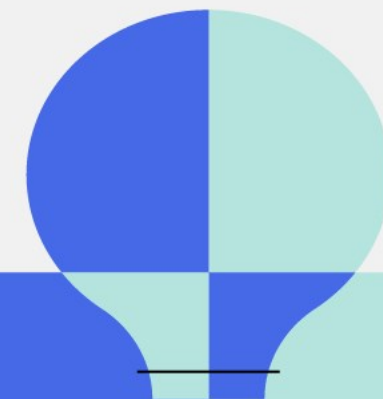
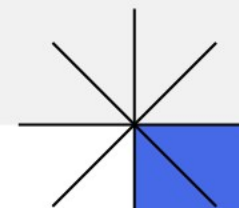
**NCC-PT**

PORTUGAL CYBERSECURITY  
COORDINATION CENTRE



[ncc.info@cncs.gov.pt](mailto:ncc.info@cncs.gov.pt)

<https://ncc.cncs.gov.pt>



# Obrigado!

[jornadas.fccn.pt](http://jornadas.fccn.pt)

[fccn.pt](http://fccn.pt)