

A Cibersegurança na Transição Digital



O Caminho para a maturidade e
resiliência das organizações

Digitization vs. Digitalization vs. Digital Transformation

A Transformação Digital

“A transformação digital é mais do que a aplicação de um conjunto de tecnologias com impacto em alguns processos.

É uma mudança organizacional e operacional, mas sobretudo cultural, que se consegue através da integração de tecnologias, processos e competências de forma transversal aos diferentes níveis e funções da empresa.

Entra-se assim no domínio estratégico alavancado pela tecnologia, que deve ser planeado e executado por etapas, com objetivos bem definidos.

E que tem um poder verdadeiramente transformador: o de reposicionar as organizações, tornando os seus negócios mais ágeis e capazes de se adaptarem mais rapidamente à evolução do mercado, permitindo-lhes almejar a liderança nas suas áreas de atuação.”

*Francisco Almada Lobo, CEO e co-fundador da Critical Manufacturing

In: Dinheiro Vivo -<https://www.dinheirovivo.pt/opiniao/desmistificando-a-digitacao-a-digitalizacao-e-a-transformacao-digital--14825298.html>

A Transformação Digital e a Cibersegurança

Transformação Digital => Maior exposição digital

- O rápido desenvolvimento das tecnologias digitais estão a mudar significativamente as perspetivas de segurança;
- A natureza das ameaças e dos ataques estão constantemente a mudar, adaptando-se rapidamente a novas realidades e alvos;
- 5 exemplos:
 - **Indústria 4.0 - convergência entre o OT e o IT;**
 - **Cadeia de fornecimento;**
 - **Sistemas proprietários e a obsolescência de infraestrutura;**
 - **Falta de conhecimento especializado e de sensibilização;**
 - **Segurança física.**



A Transformação Digital e a Cibersegurança

Transformação Digital => Maior exposição digital

- A cibersegurança é fundamental nos projetos de transformação digital, pois protege os ativos digitais, a propriedade intelectual e os dados dos clientes e das organizações.
- À medida que os projetos de transformação digital evoluem, com a adoção de novas tecnologias e a integração de sistemas digitais, a cibersegurança ganha também importância, passando a ser tratada ao nível da Administração nas organizações.



A Transformação Digital e a Cibersegurança

Transformação Digital => Maior exposição digital => Maior Risco

Transformação Digital => Estratégia de cibersegurança => Maturidade => Resiliência

Digital transformation is increasing cyber risk.

IT security has very little involvement in directing efforts to ensure a secure digital transformation process.

ONLY 37% of respondents say the CIO is most involved.

ONLY 24% of respondents say the CISO is most involved.

82% of respondents believe their organizations experienced at least one data breach as a result of digital transformation.

55% of respondents say with certainty that at least one of these breaches was caused by a third party.

Digital transformation has significantly increased reliance on third parties.

58% of respondents say the primary change to their organizations is increased migration to the cloud.

58% of respondents say that despite the increased risk, their organizations do not have a third-party cyber risk management program.

63% of respondents say their organizations have difficulty ensuring there is a secure cloud environment.

56% of C-level executives say their organizations find it challenging to ensure third parties have policies and practices that guarantee the security of their information.

	C-SUITE	IT DEPT
Rushing to achieve digital transformation increases risk of a data breach	53%	71%
Do not want security measures to prevent the free flow of information in an open-business model	63%	45%

A Transformação Digital e a Cibersegurança

Transformação Digital => Maior exposição digital => Maior Risco

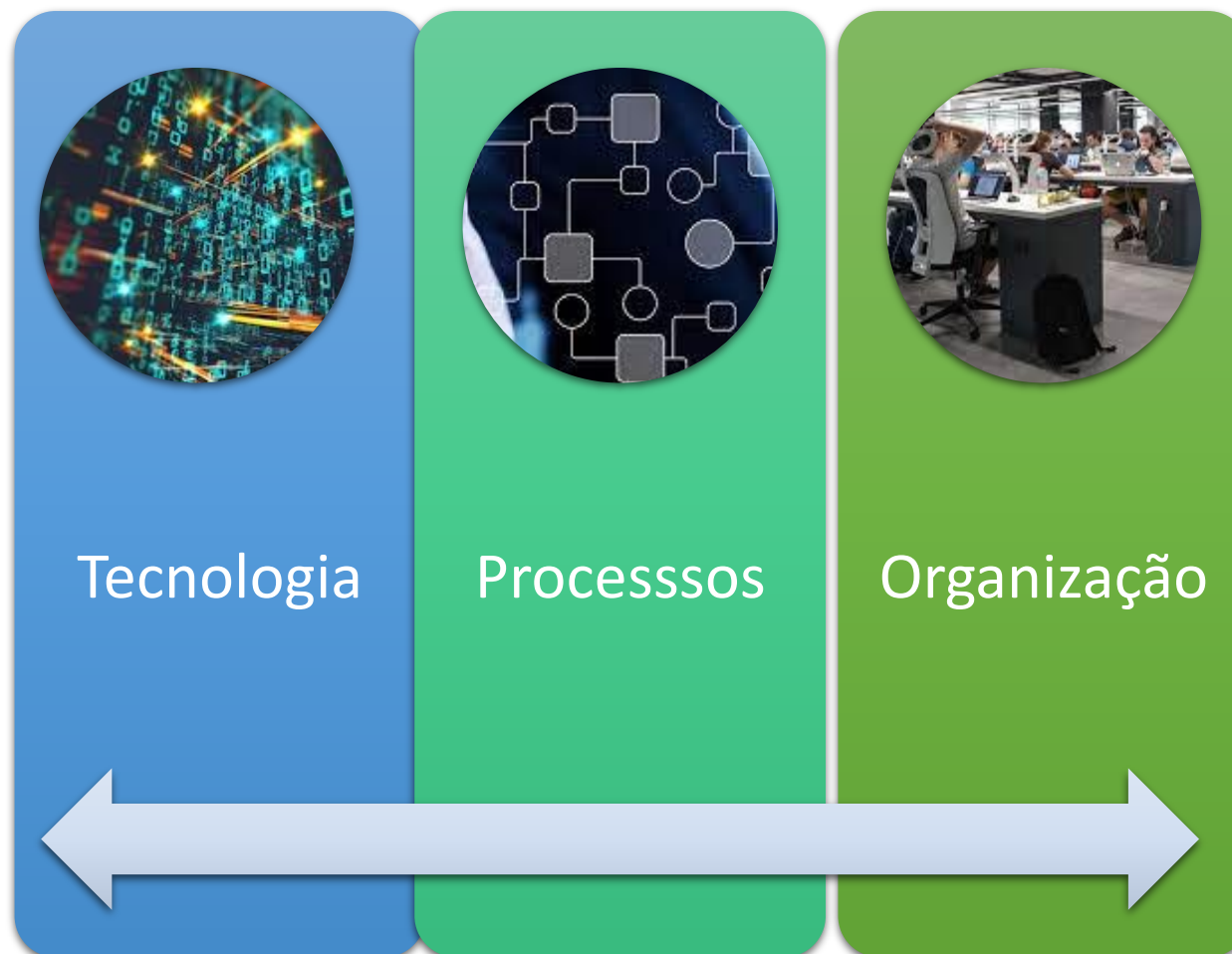
Transformação Digital => Estratégia de cibersegurança => Maturidade => Resiliência



*Fonte: observatório de cibersegurança, CNCS

A Transformação Digital e a Cibersegurança

Pilares essenciais:



Rede de Centros de Competência em Cibersegurança

Uma resposta de âmbito nacional e em rede para apoiar as organizações no caminho da maturidade e resiliência em cibersegurança.



Rede de Centros de Competência em Cibersegurança

- Apoiar a transformação digital das organizações sob o ponto de vista de cibersegurança (desde a capacitação, nos processos, na obtenção de financiamento e operação diária);
- Fomentar a colaboração e cooperação;
- Promover a criação de ecossistemas regionais.



Garantir a necessária proximidade destinada a apoiar a administração pública, os operadores de serviços essenciais, os prestadores de serviços digitais e as PME's em temas no âmbito da Cibersegurança.

Rede de Centros de Competência em Cibersegurança

“Ponto de Contacto Regional” que deverá, entre outras, atividades:

- Produzir e disponibilizar orientações adaptadas às organizações numa perspetiva regional, aconselhando-as na adoção das melhores práticas e processos em matérias de cibersegurança e segurança da informação;
- Servir de ponte e facilitador nas atividades de capacitação das organizações e seus recursos humanos através da C-Academy;
- Servir de ponte e facilitador aos processos de transformação digital disponibilizados com o apoio dos Polos de Inovação Digital;
- Orientar as organizações e agentes locais no cumprimento dos requisitos legais e de certificação.



Polo de inovação digital

Os Polos de Inovação Digital ou Digital Innovation Hubs (DIH) são **redes colaborativas** que incluem centros de competências digitais específicas, com o **objetivo de disseminação e adoção de tecnologias digitais avançadas** por parte das empresas, em especial, PME, via **desenvolvimento, teste e experimentação** dessas mesmas tecnologias.



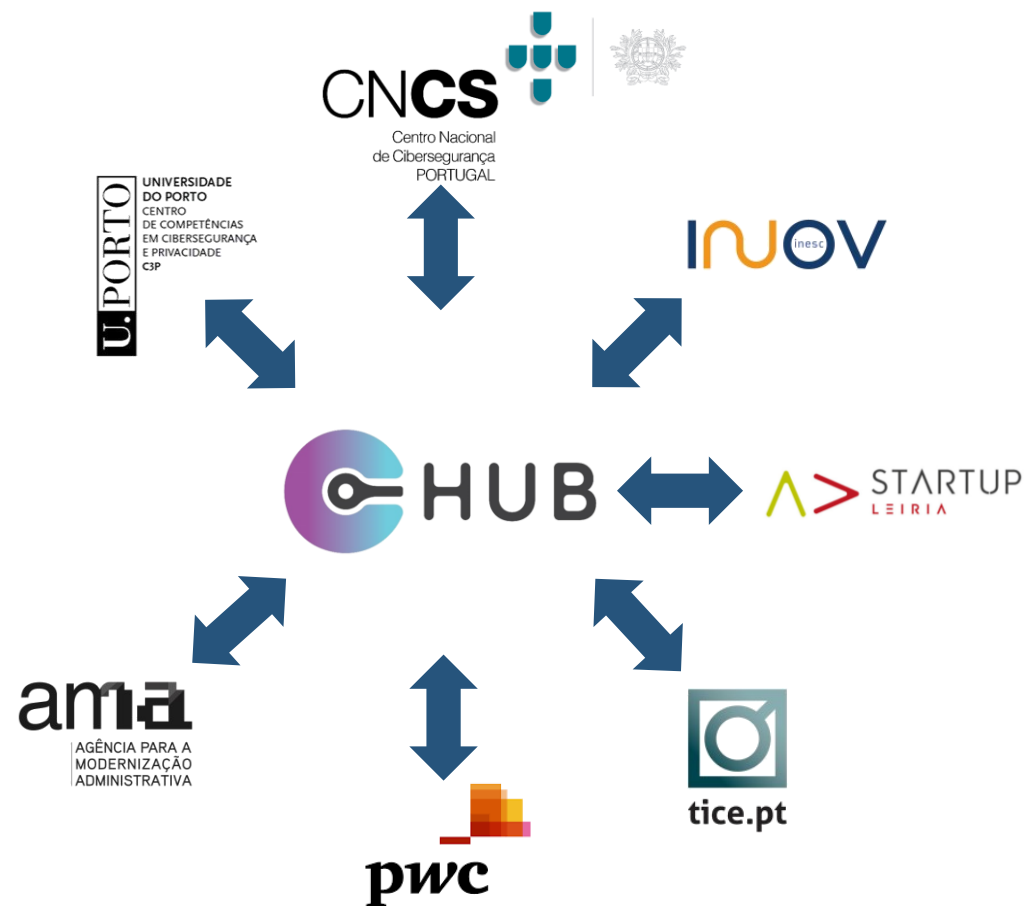
Os Polos de Inovação Digital atuam como uma porta de entrada e fortalecem o ecossistema de inovação, pois resultam de **cooperação entre vários parceiros com competências e atuações complementares**, incluindo centros de investigação, universidades, centros de interface tecnológico, incubadoras, *clusters* de competitividade, associações empresariais, agências de desenvolvimento, entre outros atores do ecossistema de inovação nacional ou regional.



Polo de inovação digital

Responder às necessidades, no apoio às PMEs e à AP, em matéria de Cibersegurança nos seus processos de transformação digital.

Como instrumento de dinamização das PMEs e AP – O C-HUB pretende responder às necessidades específicas destes atores, tirando partido da rede de consorciados e parceiros.



Innovation isn't something you can simply add to the mix, it needs to be a core part of the way the organisation works.

Polo de inovação digital

Privacidade, Tecnologias de Privacidade e Proteção de Dados

Criptoanálise

Computação Quântica

Protocolos Criptográficos

Dispositivos Móveis e IoT

Identidade Digital

Resposta a Incidentes e Gestão de Equipas CSIRT

Deteção de Intrusão

Engenharia Social

Segurança de Sistemas de controlo industrial

Análise Forense

Blockchain

Innovation isn't something you can simply add to the mix, it needs to be a core part of the way the organisation works.

Polo de inovação digital

Infraestrutura De Computação Alta Capacidade Para Processamento De Informação Classificada

Centro de Gestão da Inovação

Laboratório de Análise Funcional e Criptográfico

Infraestrutura Laboratorial de Iot Focado em I&D e Transferência de Tecnologia

Ambientes de Teste de Plataformas Nacionais de Interoperabilidade e Identificação Digital

Cyber Range

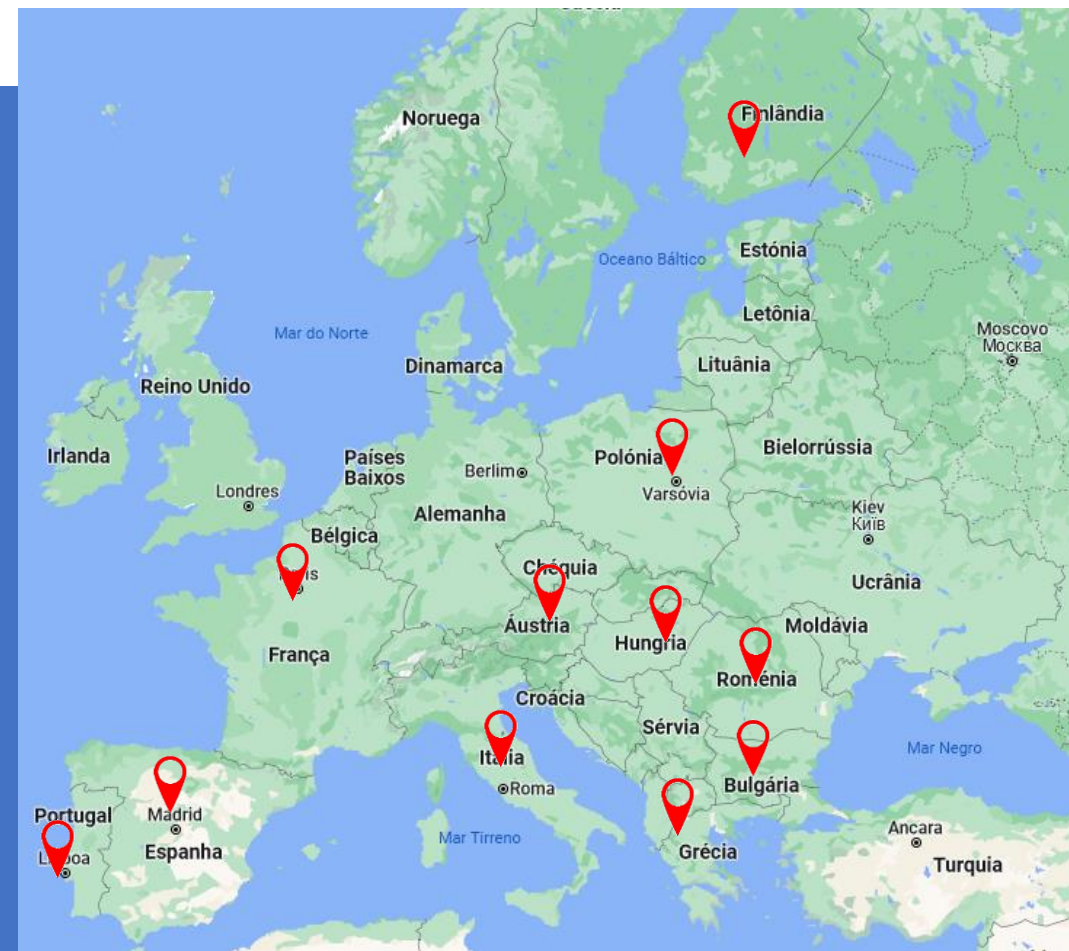
Innovation isn't something you can simply add to the mix, it needs to be a core part of the way the organisation works.

Polo de inovação digital



MoU's – Já estabelecidos com outros DIHs

AI4PA (Portugal); CONNECT5 (Portugal); AzoresInnovationHUB (Portugal); DIH DIGIHALL (France); CEA (France); Robocoast DIH (Finland); DIGS3 (Spain); Futures of Innovation and Technology Digital Innovation Hub (Romania); Transylvania Digital Innovation Hub (Romania); LIVINGTRAC (Greece); CityInnoHub (Romania); RoTechNation (Romania); Digital Innovation Zone DIH (Romania); Tuscany X.0 (Italy); DanubeDIH (Romania); EDIH L'Artis (Bulgaria); HealthGoDigital! (Poland); CrowdInMotion (Austria).



Innovation isn't something you can simply add to the mix, it needs to be a core part of the way the organisation works.

Centro Nacional de Coordenação em Cibersegurança



O Regulamento (EU) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021.

Procede à criação do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC)
e
Rede de Centros Nacionais de Coordenação (NCCs)

Missão do Centro de Competências e da Rede (1/2)

“1. A missão do Centro de Competências e da Rede contribui para que a União:

- a) Reforce a sua liderança e autonomia estratégica no domínio da cibersegurança, conservando e desenvolvendo as capacidades e aptidões de investigação, académicas, societais, tecnológicas e industriais da União no domínio da cibersegurança necessárias para aumentar a confiança e a segurança, nomeadamente a confidencialidade, a integridade e a acessibilidade dos dados, no mercado único digital;*
- b) Apoie as capacidades, aptidões e competências tecnológicas da União em relação à resiliência e fiabilidade das infraestruturas de redes e sistemas de informação, incluindo as infraestruturas críticas e o hardware e software de uso comum na União; e*
- c) Aumente a competitividade global da indústria de cibersegurança da União, assegure normas elevadas de cibersegurança em toda a União, e transforme a cibersegurança numa vantagem competitiva para outras indústrias da União.*

Centro Nacional de Coordenação em Cibersegurança



O Regulamento (EU) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021.

Procede à criação do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC)
e
Rede de Centros Nacionais de Coordenação (NCCs)

Missão do Centro de Competências e da Rede (1/2)

“1. A missão do Centro de Competências e da Rede contribui para que a União:

- a) Reforce a sua liderança e autonomia estratégica no domínio da cibersegurança, conservando e desenvolvendo as capacidades e aptidões de investigação, académicas, societais, tecnológicas e industriais da União no domínio da cibersegurança necessárias para aumentar a confiança e a segurança, nomeadamente a confidencialidade, a integridade e a acessibilidade dos dados, no mercado único digital;*
- b) Apoie as capacidades, aptidões e competências tecnológicas da União em relação à resiliência e fiabilidade das infraestruturas de redes e sistemas de informação, incluindo as infraestruturas críticas e o hardware e software de uso comum na União; e*
- c) Aumente a competitividade global da indústria de cibersegurança da União, assegure normas elevadas de cibersegurança em toda a União, e transforme a cibersegurança numa vantagem competitiva para outras indústrias da União.*

Centro Nacional de Coordenação em Cibersegurança



Missão do Centro de Competências e da Rede (2/2)

2. *O Centro de Competências e a Rede exercem as respetivas atribuições em colaboração com a ENISA e a Comunidade, sempre que adequado.*
3. *O Centro de Competências, nos termos dos atos legislativos que estabelecem os programas pertinentes, nomeadamente o Horizonte Europa e o Programa Europa Digital, utiliza os recursos financeiros pertinentes da União de modo a contribuir para a missão definida no n.º 1.”*

Coordenar as medidas de apoio financeiro relativo a iniciativas da União Europeia em matéria de investigação e desenvolvimento, da inovação, da tecnologia e do desenvolvimento industrial no domínio da cibersegurança, nomeadamente ao abrigo do **Horizonte Europa** — Programa-Quadro de Investigação e Inovação, criado pelo Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho de 28 de abril de 2021, e do **Programa Europa Digital**, criado pelo Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho.

Centro Nacional de Coordenação em Cibersegurança



As atribuições dos Centros de Nacionais de Coordenação (1/3)

- *Atuar como pontos de contacto a nível nacional para a Comunidade a fim de apoiar o Centro de Competências na consecução da sua missão e dos seus objetivos, em especial coordenando a Comunidade através da coordenação dos membros da Comunidade nos respetivos Estados-Membros;*
- *Fornecer conhecimentos especializados e contribuir ativamente para as atribuições estratégicas estabelecidas no artigo 5.o, n.o 2, tendo em conta os desafios nacionais e regionais pertinentes em matéria de cibersegurança em diferentes setores;*
- *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;*
- *Prestar assistência técnica às partes interessadas, apoiando-as na sua fase de candidatura aos projetos geridos pelo Centro de Competências em relação à sua missão e aos seus objetivos e em plena conformidade com as regras de boa gestão financeira, especialmente no que diz respeito aos conflitos de interesses;*

Centro Nacional de Coordenação em Cibersegurança



As atribuições dos Centros de Nacionais de Coordenação (2/3)

- *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;*
- *Executar ações específicas para as quais o Centro de Competências tenha concedido subvenções, nomeadamente através da prestação de apoio financeiro a terceiros, nos termos do artigo 204.o do Regulamento Financeiro, ao abrigo das condições especificadas nas convenções de subvenção em causa;*
- *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;*
- *Promover e difundir os resultados pertinentes do trabalho da Rede, da Comunidade e do Centro de Competências a nível nacional, regional ou local;*
- *Avaliar os pedidos apresentados por entidades estabelecidas no mesmo Estado-Membro ao centro nacional de coordenação com vista a fazerem parte da Comunidade;*

Centro Nacional de Coordenação em Cibersegurança

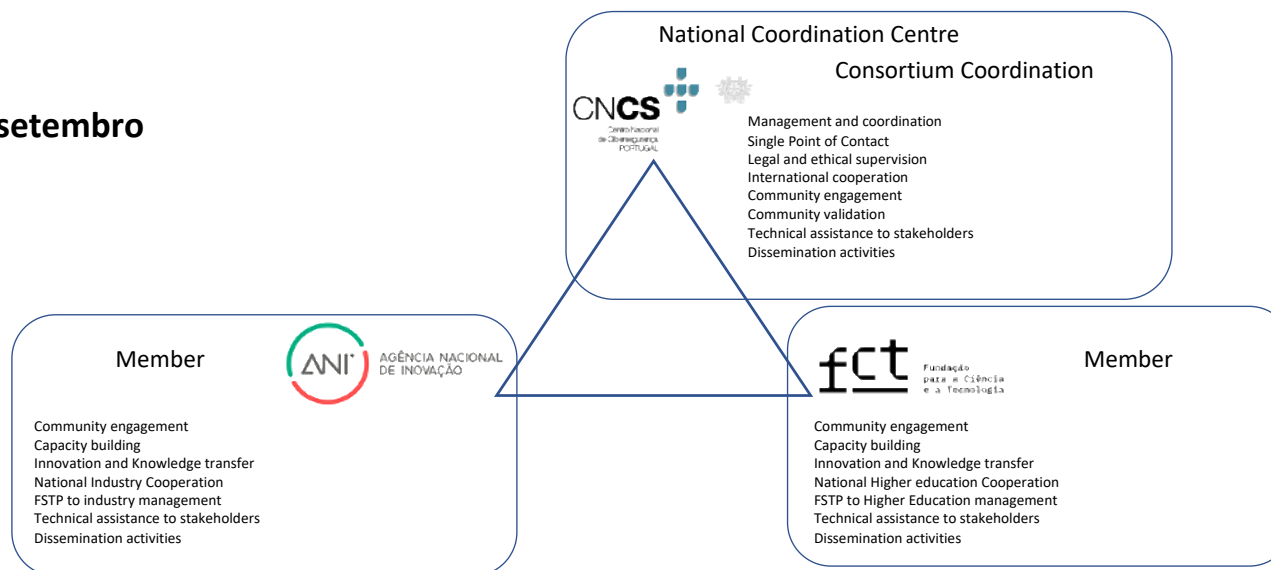


As atribuições dos Centros de Nacionais de Coordenação (3/3)

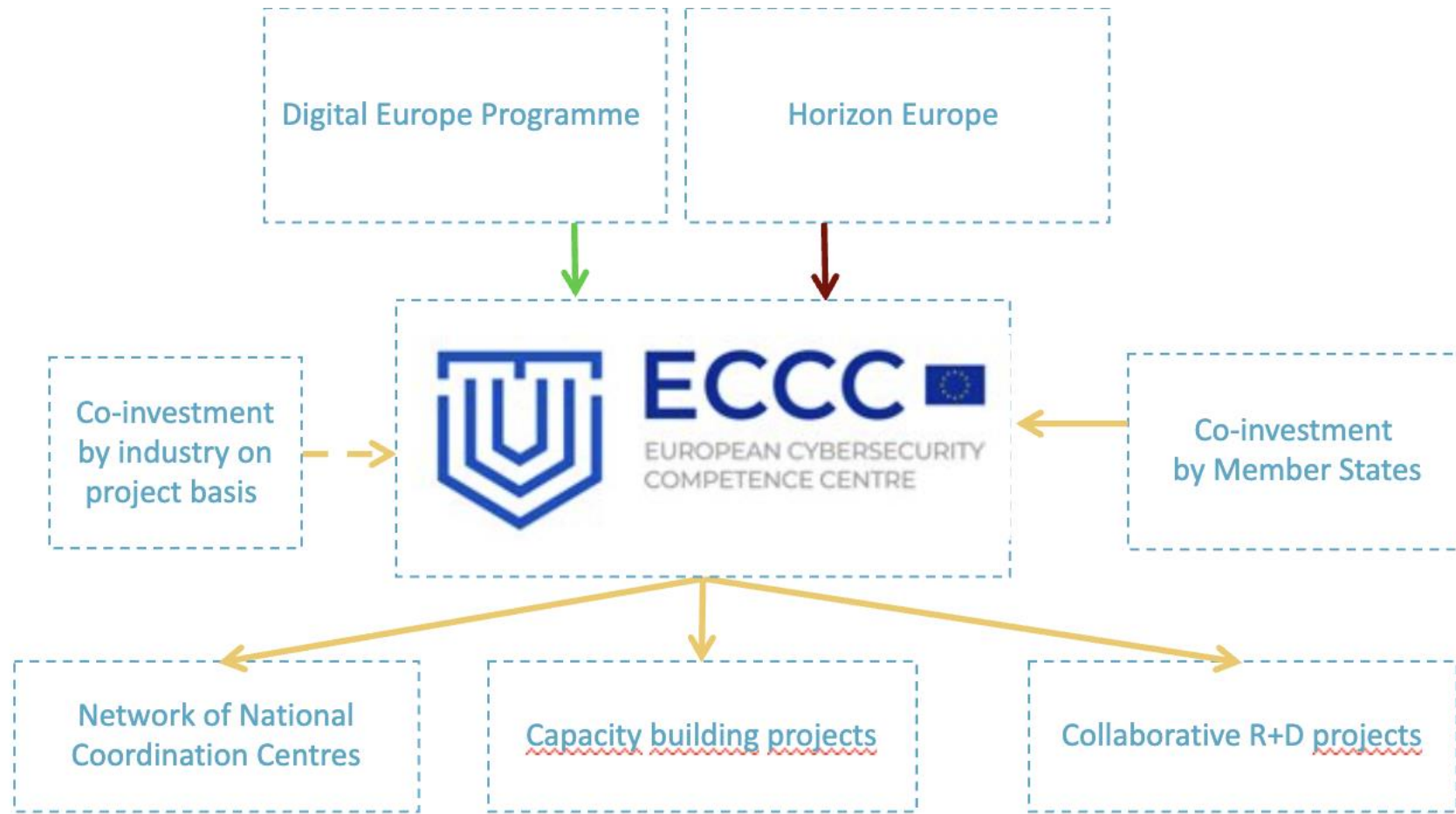
- Preconizar e promover a participação de entidades pertinentes nas atividades desenvolvidas pelo Centro de Competências, pela Rede e pela Comunidade e acompanhar, consoante necessário, o nível de participação e montante do apoio financeiro público concedido à investigação, desenvolvimento e implantação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

Em Portugal

Despacho 11491/2022 de 28 setembro



Centro Nacional de Coordenação em Cibersegurança





Obrigado pela atenção

António Rio Costa
antonio.costa@cncs.gov.pt