Engaging EU Projects Using the ECSF

C-Academy – Portugal

A bridge between national competence strategy and European harmonization

André Silva - CNCS

The Competencies Challenge

Structuring competencies is essential to reduce the talent gap

Skills Gap Crisis

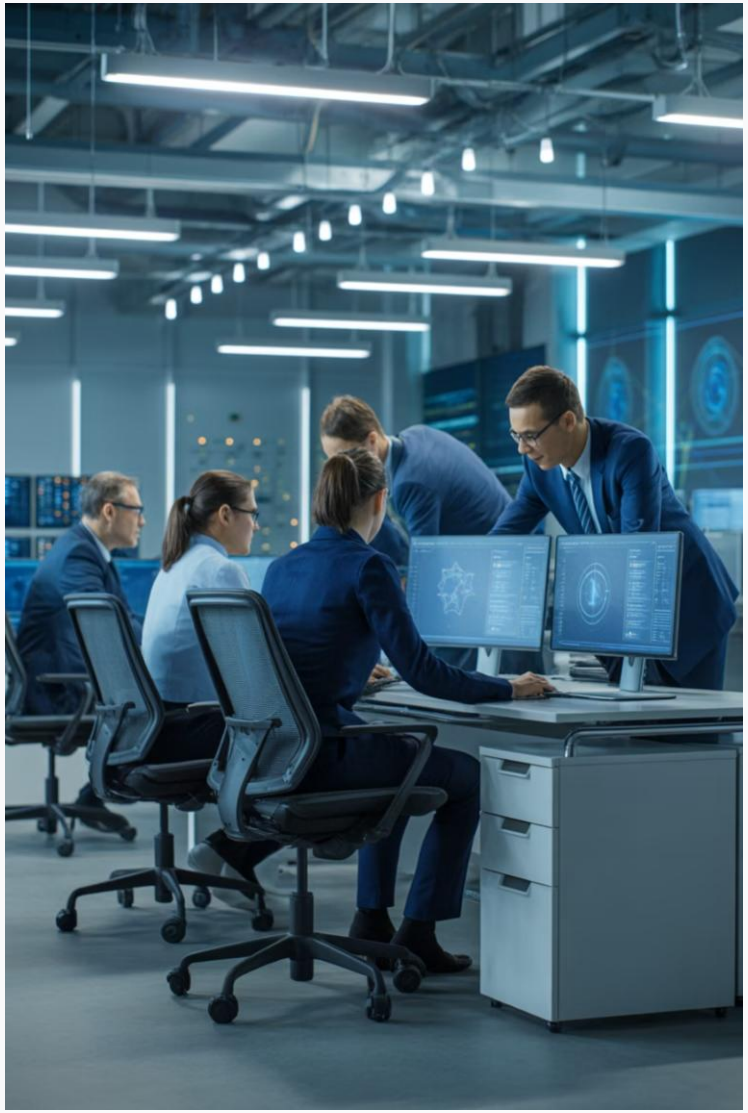
A growing shortage of cybersecurity professionals, limiting our ability to strengthen national digital resilience and support public administration, industry, and critical sectors.

Fragmented Approaches

Use of different terminology, role definitions, and competence expectations, making it difficult to compare skills or plan workforce development consistently across the country.

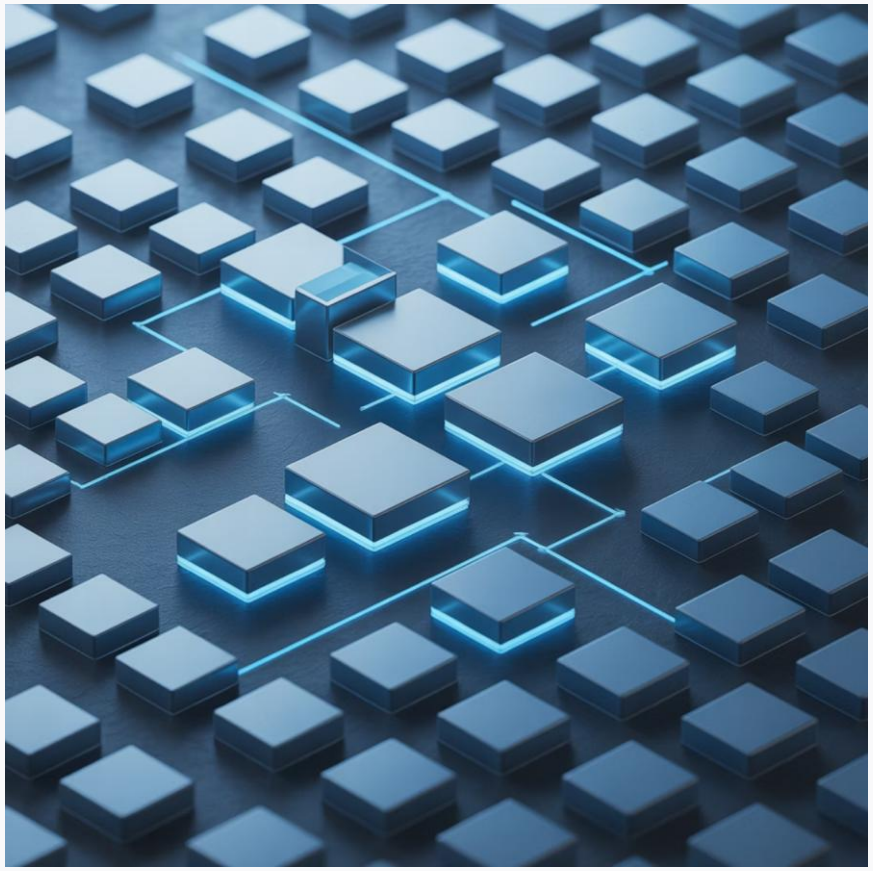
Training Inefficiencies

Without a common national competency structure, training paths were inconsistent, hard to benchmark, and often disconnected from operational needs .



Portugal’s National Competency Framework

A national framework designed for Portugal’s cybersecurity ecosystem



Portugal's Strategic Response

Portugal’s approach balances national specificity with awareness of European developments, ensuring relevance today and enabling future alignment.

- Designed for the Portuguese cybersecurity ecosystem and national skills needs
- Built around specialised and transversal competencies structured into profiles and proficiency levels
- Integrated with national regulatory, strategic and sectoral priorities
- Developed to support education, workforce planning and multi-sector adoption

Structure of the National Framework

A holistic view of cybersecurity competencies defined in Portugal's National Competency Framework

Specialised

Risk management

- Risk management

Incident and problem management

- Incident management
- Problem management

Technical

- Systems testing and evaluation
- Network management
- Network and systems security
- Information management
- Database management systems
- Network defence techniques
- Information systems architecture
- Systems administration
- Identity management, authentication and access control
- General knowledge in technologies
- Software development
- Forensic analysis
- Cryptology
- Threat analysis

Organisational

- Organisational policies
- Information system assurance
- Legal compliance, ethics and social acceptance
- Data protection and privacy
- Human resources management
- Organisational awareness
- Requirements analysis
- Procurement and third party management
- Auditing
- Knowledge management
- Asset management

Transversal

Leadership, strategy and decision-making

- Leadership
- Critical thinking
- Decision-making
- Creative thinking

Relational

- Communication
- Diversity management
- Personal relationships
- Conflict management

Architecture of the Cybersecurity Competencies Framework, structured in domains and subdomains.

Risk Management Knowledge

Domínio	Subdomínio	Competência	Conhecimento
Especializadas	Gestão de risco	Gestão de risco	**Competência de Gestão de risco**
Especializadas	Gestão de risco	Gestão de risco	Conhecimento da tolerância ao risco e da estratégia de gestão de risco.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento das normas, processos e práticas de gestão de risco nas cadeias de fornecimento.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento das organizações clientes e parceiros, incluindo os seus objetivos, estrutura, recursos e necessidades de informação.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento de avaliação de riscos.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento de gestão de risco e estratégias de mitigação.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento de metodologias de gestão de risco.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento de políticas, requisitos e procedimentos de gestão de risco de tecnologia de informação.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento de segurança em cadeias de fornecimento e das suas políticas, requisitos e procedimentos de gestão de risco.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento do contexto das organizações, incluindo os seus objetivos, estrutura, capacidades, e necessidades de informação.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento dos conceitos de segurança de informação, tecnologias e métodos empregues para garantir a segurança de informação.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento dos planos de proteção (e.g., políticas de gestão de riscos, políticas de gestão de segurança em cadeias de fornecimento, técnicas de manutenção de integridade).
Especializadas	Gestão de risco	Gestão de risco	Conhecimento dos princípios e métodos de análise estruturada.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento dos processos de gestão de risco (e.g., métodos de avaliação e mitigação de riscos).
Especializadas	Gestão de risco	Gestão de risco	Conhecimento dos requisitos do quadro de referências de gestão de risco.
Especializadas	Gestão de risco	Gestão de risco	Conhecimento dos meios de comunicação com pessoas e entidades, internas e externas, para a gestão de risco.

C-ACADEMY FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA

CNCS

From Strategy to Training: C-Academy

Turning the Framework into Action

01

- **Course Design**
  - Structure a complete training offer that covers all competencies, knowledge areas, and proficiency levels identified in the framework

02

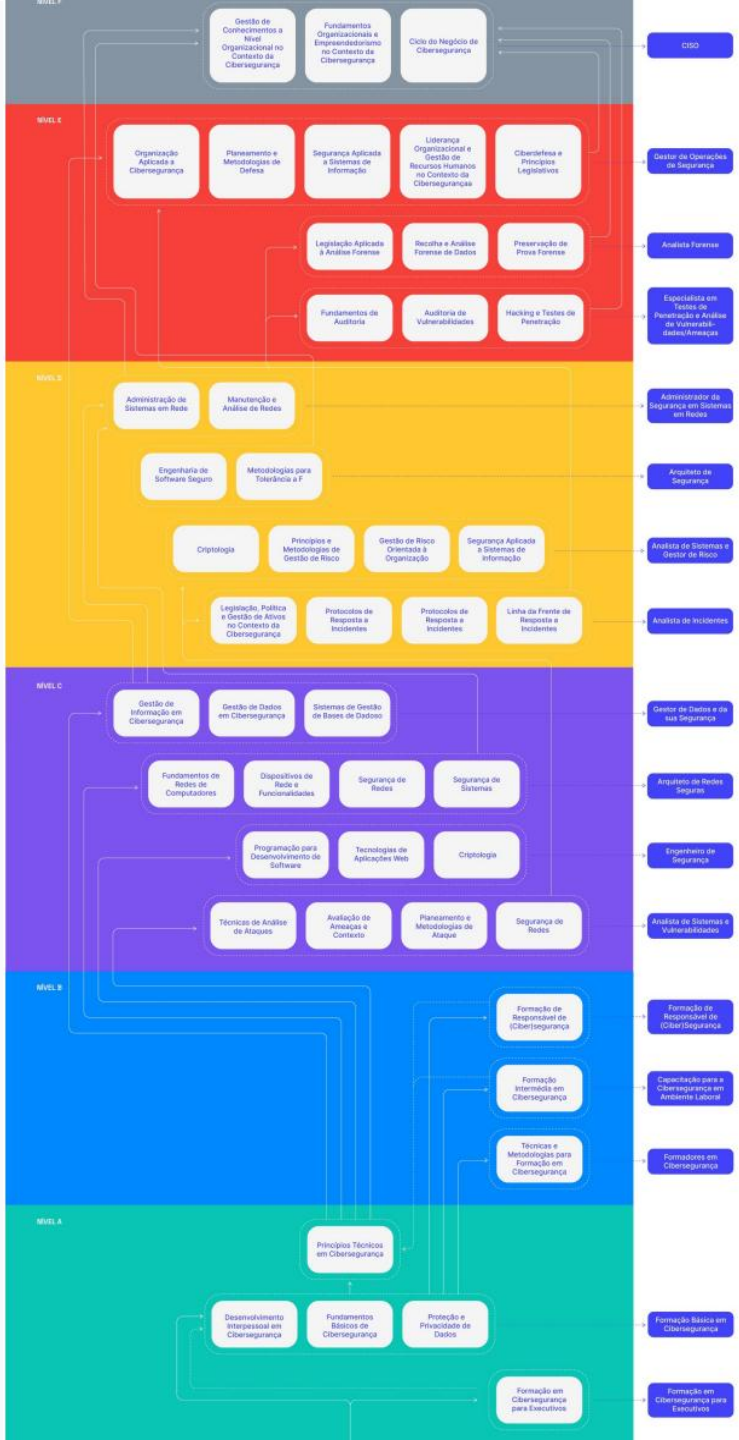
- **Development with Higher Education Institutions**
  - Contract Higher Education Institutions to design and produce the training programmes in line with C-Academy's technical guidelines and competency requirements.

03

- **Delivery & Certification**
  - Contract Higher Education Institutions to deliver the training programmes they previously developed under C-Academy guidance, with learning formally recognised through national certification and ECTS.

CACADEMY FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA

- National training programme created by the National Cybersecurity Centre (CNCS) under the Recovery and Resilience Plan (PRR)
- Executed through higher education institutions
- Provides 43 courses, each with 35 or 70 hours, covering multiple domains and levels of difficulty
- Training formats include online, in-person and hybrid, ensuring flexible participation
- Develops and strengthens cybersecurity skills across both public administration and the private sector



C-ACADEMY FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA

CNCS

C-Academy 2024 - 2026: Numbers and Impact

A national-scale programme delivering measurable results

43

Certified Courses

A comprehensive curriculum spanning multiple cybersecurity domains and proficiency levels

200+

Training Sessions Delivered

Consistent nationwide delivery demonstrating strong programme momentum and sustained demand

3500+

Certified Participants

Professionals equipped with formally validated competencies aligned with the National Competency Framework

20+

Higher Education Institutions

Robust academic partnerships ensuring quality, consistency, and broad territorial reach

300+

Training Sessions for Teachers

Strengthening educator capability to support a resilient, long-term cybersecurity education ecosystem

9800

Target Trainees by 2026

An ambitious national commitment to workforce development aligned with strategic cybersecurity needs

The ECSF Emerges

Introduced after the national framework, the ECSF provides a shared European reference model that enhances comparability, mobility, and strategic coherence across Member States.

Common Language

Standardised terminology and competence structures improve comparability and interoperability, creating a shared professional vocabulary for cybersecurity in Europe

Workforce Mobility

Portable, mutually recognisable competence descriptions support cross-border mobility and enable a more coherent European cybersecurity labour market

Strategic Alignment

A harmonised basis for EU-wide capability development, joint initiatives, and coordinated workforce planning across sectors and Member State

The ECSF adds a European layer of coherence, creating the conditions for structured alignment and broader impact.

The Current State

We want formal alignment

Current Position

- No formal mapping has been completed.
- Initial comparisons indicate strong alignment.

Analytical Work

Analyzing structural correspondences, terminology differences, competency scope, and professional profiles.

Adoption Phase

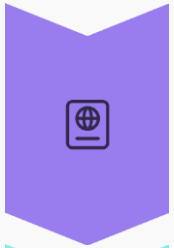
With formal validation, stakeholder consultation, and structured integration of both frameworks.

We want to ensure that the future alignment is evidence-based, interoperable, and fully coherent

C-ACADEMY TRAINING PATHS	ECSF PROFILES
Cybersecurity Training for Executives	
Basic Cybersecurity Training	
Cybersecurity Training for the Workplace	
Training for (Cyber) Security Officers	**Cyber Legal, Policy & Compliance Officer**
Systems and Vulnerability Analyst	**Cyber Threat Intelligence Specialist**
Security Engineer	**Cybersecurity Implementer**
Secure Network Architect	
Data and Security Manager	
Incident Analyst	**Cyber Incident Responder**
Systems Analyst and Risk Manager	**Cybersecurity Risk Manager**
Security Architect	
Network Systems Security Administrator	
Penetration Testing and Vulnerability/Threat Analysis Specialist	**Penetration Tester**
Forensic Analyst	**Digital Forensics Investigator**
Security Operations Manager	**Cybersecurity Architect**
CISO	**Chief Information Security Officer (CISO)**

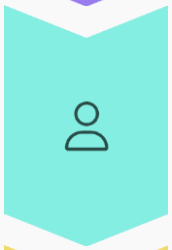
The Desired Path

Formal mapping and structured adaptation as the bridge between frameworks



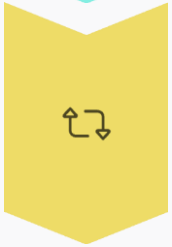
Formal Mapping

Match Portuguese competencies to ECSF roles and tasks to ensure full interoperability.



Adaptation of C-Academy training offer to the ECSF

Reviewing and adapting the C-Academy training programmes to ensure full alignment with ECSF profiles, enabling the creation of an official equivalences matrix.



Convergence & Integration

Evolving the national framework toward European alignment.

The Future: Profiling Tools

ECSF alignment enables a new generation of personalised, competence-driven learning and assessment tools.

Competency Assessment

- **Evaluates individual competencies and maps them to the ECSF-aligned national framework.**
- **Identifies strengths and development needs.**

Recommendation of C-Academy courses aligned to the ECSF

- **Suggests learning pathways based on profile and skill gaps.**
- **Highlights the C-Academy courses that best support progression.**

Organisational Team Assessment

- **Enables public and private organisations to assess the maturity of their teams.**
- **Identifies collective skill gaps and priority areas for upskilling or recruitment.**

Harmonised National Data

- **Generates consistent, comparable national data on cybersecurity competencies.**
- **Improves understanding of the national landscape and supports strategic decision-making.**

National → European Convergence

By aligning our national framework with the ECSF, we are reinforcing:

Interoperability

Clear mapping between national competencies and ECSF profiles.

Training Coherence

C-Academy aligned with European standards, reinforcing recognition and transparency.

Talent Mobility

Greater comparability of skills and easier cross-border mobility.

Ecosystem Maturity

A shared competence language strengthening collaboration across sectors.

This convergence does not replace what we built — it amplifies it.
It connects Portugal's national depth with Europe's shared coherence.

C-ACADEMY FORMAÇÃO AVANÇADA EM CIBERSEGURANÇA

CNCS

Learn More About C-Academy

Website:
C-Academy.pt

Contact:
c-academy@cncs.gov.pt