

#CátedrasCiber

Academic Incubator

Nov. 20th 2025



Hackathon Internacional en Ciberseguridad



Academic Incubator: Cybersecurity and the 3 Missions of the University

Cybersecurity in the University: Teaching, Research and
Knowledge Transfer for Significant Impact



Prof. Jorge García
Head for KTO and Spin-offs
University of Oviedo



Cybersecurity: Understanding the Challenge

Cybersecurity encompasses the comprehensive set of policies, procedures, technologies, and controls that **protect information systems, networks, devices, and data** from unauthorized access, damage, disruption, or exploitation.

State-of-the-Art Evolution

Studies reveal ongoing challenges in keeping pace with sophisticated threats, requiring **continuous innovation** in defense mechanisms, threat intelligence, and response capabilities.

Exponential Risk Growth

Recent research highlights persistent **gaps in cybersecurity risk data availability**, penalizing effective risk management strategies across organizations and infrastructures.



Cybersecurity: Understanding the Challenge

Critical Needs and Society Demands

- Protection of Critical Services
- Privacy, Data Protection & Trust
- Secure Digital Transformation
- Skills & Workforce Development
- Incident Response, Continuity & Resil.
- Secure AI, Ethics & Accountability
- Protection Against Cybercrime
- Support for SMEs and Public Sector
- Assurance, Certification & Compliance
- Ethical & Responsible Use of Technol
- ...



Innovative solutions emerge as collaborative environments where students, researchers and companies co-create practical solutions, bridging the gap between theory and real-world applications.

The Three Missions of the Modern University

Universities serve as dynamic engines of progress through **three interconnected dimensions** that define their role in society. These missions form the classical model of the modern institution, transforming it from a passive repository of knowledge into an active catalyst for economic and social development.

1

Mission 1: Teaching

2

Mission 2: Research

3

Mission 3: Knowledge Transfer

The Three Missions of the Modern University

Universities serve as dynamic engines of progress through **three interconnected dimensions** that define their role in society. These missions form the classical model of the modern institution, transforming it from a passive repository of knowledge into an active catalyst for economic and social development.

1

Mission 1: Teaching

Training students and **transforming knowledge into competencies and skills** through learning processes. Equipping citizens with values, capabilities, and practical expertise.

2

Mission 2: Research

Generating new knowledge, fostering innovation, and driving scientific and technological development. **Using resources to create valuable knowledge assets.**

3

Mission 3: Knowledge Transfer

Valorizing knowledge through relationships with society and industry, promoting open innovation and measurable impact. **Converting knowledge assets into tangible resources.**

The Three Missions of the Modern University

Beyond Transfer: Innovation and Significant Impact

Innovation vs. Transfer

Transfer: **bringing knowledge to external environments.**

Innovation: introducing transformative changes, improvements, new technologies, and processes that fundamentally reshape realities and create **unprecedented value.**

What is “Significant Impact”

1. **Trascends** (academy)el ámbito académico.
2. Generates un **verifiable value.**
3. It has empiric **evidence** (indicators).
4. It is **sustained in time** (continuous improvement)
5. **Relevant** change (not just incremental).

Innovation is broader and more profound than transfer: it encompasses the creation of disruptive value and meaningful transformation that extends far beyond simple knowledge dissemination.



**Cátedra de
Ciberseguridad**
Universidad de Oviedo

Mission 1: Training Cybersecurity Excellence

Universities play a key role in developing **cybersecurity talent** through diverse educational pathways (from traditional academic programs to innovative, industry-aligned training initiatives that address the critical skills shortage)

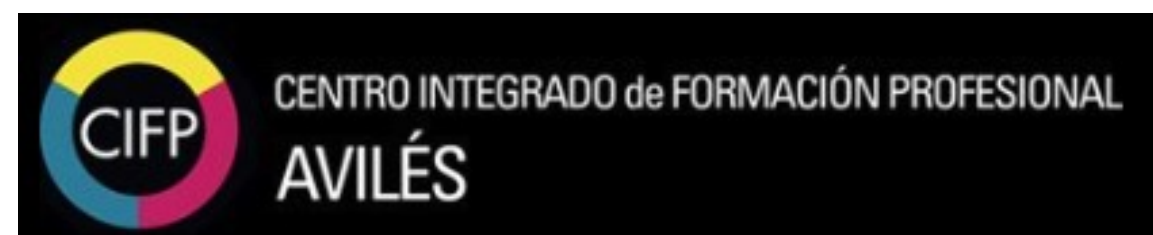


Mission 1: Teaching Cybersecurity Excellence

0

Vocational Training

Professional formation (FP) modules at institutions like CIFP Avilés provide practical, career-focused cybersecurity training directly aligned with labor market demands and industry certifications.



Máster de FP en Ciberseguridad en Entornos de las Tecnologías de la Información.

El CIPF de Avilés es el único centro de Asturias en el que se imparte el Curso de Especialización en Ciberseguridad en Entornos de TIC.

Mission 1: Teaching Cybersecurity Excellence

1

Formal University Degree Programs

Specialized undergraduate and master's degrees incorporate cybersecurity subjects—both dedicated programs and cross-disciplinary (eng., comp. science, business).



BSc. in Cibersecurity and IA – Universidad de Málaga (UMA, España)

BSc. in Cybersecutiry ENgineering, –
Universidad Rey Juan Carlos (URJC, España)

BSc. in Cybersecurity – Universidad San Jorge (Zaragoza, España)

...



Cyber Security BSc – University of Warwick (Reino Unido)

Bachelor in Cybersecurity – ESIEA, Graduate School of Engineering (Francia)

BSc in Cyber Security Engineering – Tallinn University of Technology (TalTech, Estonia)

Mission 1: Teaching Cybersecurity Excellence

1

Formal University Degree Programs

Specialized undergraduate and master's degrees incorporate cybersecurity subjects—both dedicated programs and cross-disciplinary (eng., comp. science, business).



MSc. in Cybersecurity and Cyberintelligence

– Universitat Politècnica de València (UPV)

MSc. in Cybersecutiry – Universidad de Alcalá (UAH)

MSc. in Ciberseguridad – Universidad Politécnica de Madrid (UPM)

...



MSc in Software and Systems Security (Cyber Security) – University of Oxford (Reino Unido)

MSc in Cybersecurity and Cyber Defence – University of Luxembourg

MSc Cyber Security (Joint) – Master School EIT Digital – EIT Digital / EU programme

Mission 1: Teaching Cybersecurity Excellence

2

Innovation in Education

Non-conventional offerings including hackathons, entrepreneurship challenges, micro-credentials, and gamified learning experiences bridge teaching and transfer missions while fostering security culture and practical competencies.



Mission 1: Teaching Cybersecurity Excellence

3

Lifelong Learning Courses

Microcredentials and Lifelong Modules (Expert, Specialist, Master), as a continuous educational offerings that enable individuals to update, expand, or acquire new knowledge and skills throughout their professional and personal lives. It includes flexible programmes such as short courses, micro-credentials, executive education, and reskilling/upskilling pathways.

Mission 1: Teaching Cybersecurity Excellence

Universities play a pivotal role in developing cybersecurity talent through diverse educational pathways. These range from traditional academic programs to innovative, industry-aligned training initiatives that address the critical skills shortage affecting organizations worldwide.

- 📄 **Exemplar Initiative:** The Cybersecurity Chair coordinated by INCIBE and University of Oviedo strengthens university teaching and research while promoting knowledge transfer and attracting diverse talent to the field.

Mission 1: Teaching Cybersecurity Excellence

Training Offer

1. Training Model

Regular Training vs. Life-Long Training

Microcredentials

2. Design Methodology

Analysis of existing offer

Intermediation with main actors in the ecosystem

Design of Modules

3. Modular, Stackable Proposal

4. Conclusions

1. Training Model

Regular Training

B.Sc Degree (240 ECTS) /
M.Sc Degree (60-120 ECTS).

Q&A Agency (ES: ANECA) verification.
Long Term process.

Recognized in Spain (BOE / RUCT) and
in Europe (EM).

Acceso to Ph.D.

Acces to public funded grants.

General, Basic-Specialised, structured
training,
hard and soft skills.



Life-Long Learning

Variable duration
(specifically: **short**)

Flexible, agile structure, but with
IQAS.

Digital Microcredential:
EuroPASS.

Reskilling and Upskilling.

Public and Private **Funds**.

Practical training,
based on need of industry/society.

1. Training Model: Microcredentials



- Operational Structure within UNIOVI.
- Specific regulations and rules.
- Intermediation.
- Short training.
- Flexible format.
- Digital, Portable certificate, Europass, based on Standards (ESCO).
- Inclusive access.
- Quality Guarantee. ICAS.
- Funding available.
- Industry experts as trainers.
- Modularity and stackability

2. Design Methodology

Analysis of existing offer

Available training model sin cybersecurity, different focus and solutions.

- **U. Cantabria:** Microcredential about Cybersecurity with a General Scope.
- **Mondragon Unibertsitatea:** Microcredentials in Corporate Cybersecurity
- **U. Castilla-La Mancha:** Microcredential on introduction to CS, focused on threatens and good practices.
- **U. Complutense de Madrid:** Microcredential in forensic informatics and ethical hacking for TIC professionals
- **U. Politécnica de Cataluña:** Microcredential in cybersecurity for transportation systems.
- ...

2. Design Methodology

Analysis of existing offer

Available training model sin cybersecurity, different focus and solutions.

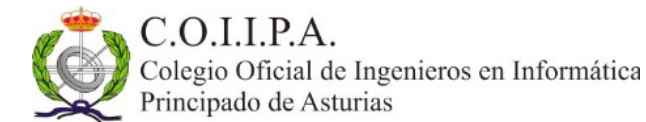


Intermediation with Actors

Companies in the sector: ClusterTIC Asturias

Professional associations: COIIPA

Faculty at University of Oviedo



Objectives

Define capacities in UNIOVI

Define needs from the society/industry

Identify existing gaps



Desing

Methodologies,
Modularity and Stackability,
Duration & Schedule,
Faculty,
Resources & Economic Analisis...

3. Modular Proposal

Microcredentials

<https://www.uniovi.es/ccuniovi/oferta-de-microcredenciales/>

Introduction to Secure Systems Design and the Role of the CISO [5 ECTS]	Management of assets for cybersecurity (CyberITAM) [5 ECTS]	Pentesting & offensive security [5 ECTS]	Implementation and verification of ENS [3 ECTS]
Fundamentals on cybersecurity: protocols, serv. & attack vectors (CCNA CyberOPS Part I) [5 ECTS]	Defense Strategies and forensic analysis on cybersecurity (CCNA CyberOPS Part II) [5 ECTS]	Cybersecurity in industrial and critical environments [6 ECTS]	Digital forensic analysis in Windows, Linux & Android [5 ECTS]
Managmt. & response to cyber-incidents [6 ECTS]	Regulatory compliance of the NIS2 Directive on cybersecurity [0,5 ECTS]	Secure development of environments (DevSecOps) [7 ECTS]	Cybersecurity & risk management [3 ECTS]
		Personal data protection and information security [1 ECTS]	Blockchain tech, smart contracts, decentralized apps and Web 3.0 [5 ECTS]

3. Modular Proposal: stackability

Expert on Direction of Security (Networks and Infrastructures)

Introduction to Secure Systems Design and the Role of the CISO [5 ECTS]	Management of assets for cybersecurity (CyberITAM) [5 ECTS]	Pentesting & offensive security [5 ECTS]	Implementation and verification of ENS [3 ECTS]
Fundamentals on cybersecurity: protocols, serv. & attack vectors (CCNA CyberOPS Part I) [5 ECTS]	Defense Strategies and forensic analysis on cybersecurity (CCNA CyberOPS Part II) [5 ECTS]	Cybersecurity in industrial and critical environments [6 ECTS]	Digital forensic analysis in Windows, Linux & Android [5 ECTS]
Managmt. & response to cyber-incidents [6 ECTS]	Regulatory compliance of the NIS2 Directive on cybersecurity [0,5 ECTS]	Secure development of environments (DevSecOps) [7 ECTS]	Cybersecurity & risk management [3 ECTS]
		Personal data protection and information security [1 ECTS]	Blockchain tech, smart contracts, decentralized apps and Web 3.0 [5 ECTS]



3. Modular Proposal: stackability

Expert on Direction of Security (Secure Development of Applications)

Introduction to Secure Systems Design and the Role of the CISO [5 ECTS]	Management of assets for cybersecurity (CyberITAM) [5 ECTS]	Pentesting & offensive security [5 ECTS]	Implementation and verification of ENS [3 ECTS]
Fundamentals on cybersecurity: protocols, serv. & attack vectors (CCNA CyberOPS Part I) [5 ECTS]	Defense Strategies and forensic analysis on cybersecurity (CCNA CyberOPS Part II) [5 ECTS]	Cybersecurity in industrial and critical environments [6 ECTS]	Digital forensic analysis in Windows, Linux & Android [5 ECTS]
Managmt. & response to cyber-incidents [6 ECTS]	Regulatory compliance of the NIS2 Directive on cybersecurity [0,5 ECTS]	Secure development of environments (DevSecOps) [7 ECTS]	Cybersecurity & risk management [3 ECTS]
		Personal data protection and information security [1 ECTS]	Blockchain tech, smart contracts, decentralized apps and Web 3.0 [5 ECTS]



3. Modular Proposal: stackability

Specialist on Corporate Cybersecurity

Introduction to Secure Systems Design and the Role of the CISO [5 ECTS]	Management of assets for cybersecurity (CyberITAM) [5 ECTS]	Pentesting & offensive security [5 ECTS]	Implementation and verification of ENS [3 ECTS]
Fundamentals on cybersecurity: protocols, serv. & attack vectors (CCNA CyberOPS Part I) [5 ECTS]	Defense Strategies and forensic analysis on cybersecurity (CCNA CyberOPS Part II) [5 ECTS]	Cybersecurity in industrial and critical environments [6 ECTS]	Digital forensic analysis in Windows, Linux & Android [5 ECTS]
Managmt. & response to cyber-incidents [6 ECTS]	Regulatory compliance of the NIS2 Directive on cybersecurity [0,5 ECTS]	Secure development of environments (DevSecOps) [7 ECTS]	Cybersecurity & risk management [3 ECTS]
		Personal data protection and information security [1 ECTS]	Blockchain tech, smart contracts, decentralized apps and Web 3.0 [5 ECTS]



3. Modular Proposal: stackability

Specialist on Offensive and Deffensive Cybersecurity

Introduction to Secure Systems Design and the Role of the CISO [5 ECTS]	Management of assets for cybersecurity (CyberITAM) [5 ECTS]	Pentesting & offensive security [5 ECTS]	Implementation and verification of ENS [3 ECTS]
Fundamentals on cybersecurity: protocols, serv. & attack vectors (CCNA CyberOPS Part I) [5 ECTS]	Defense Strategies and forensic analysis on cybersecurity (CCNA CyberOPS Part II) [5 ECTS]	Cybersecurity in industrial and critial environments [6 ECTS]	Digital forensic analysis in Windows, Linux & Android [5 ECTS]
Managmt. & response to cyber-incidents [6 ECTS]	Regulatory compliance of the NIS2 Directive on cybersecurity [0,5 ECTS]	Secure development of environments (DevSecOps) [7 ECTS]	Cybersecurity & risk management [3 ECTS]
		Personal data protection and information security [1 ECTS]	Blockchain tech, smart contracts, decentralized apps and Web 3.0 [5 ECTS]



3. Modular Proposal: stackability

Life-long Learning M. on Techniques, Tactics, Proced. & General Dir. of Cybersecurity

Introduction to
Secure Systems
Design and the Role
of the CISO [5 ECTS]

Management of
assets for
cybersecurity
(CyberITAM) [5 ECTS]

Pentesting &
offensive security [5
ECTS]

Implementation and
verification of ENS [3
ECTS]

Fundamentals on
cybersecurity:
protocols, serv. &
attack vectors
(CCNA CyberOPS
Part I)
[5 ECTS]

Defense Strategies
and forensic analysis
on cybersecurity
(CCNA CyberOPS
Part II)
[5 ECTS]

Cybersecurity in
industrial and critical
environments [6
ECTS]

Digital forensic
analysis in Windows,
Linux & Android [5
ECTS]

Secure development
of environments
(DevSecOps) [7
ECTS]

Cybersecurity & risk
management [3
ECTS]

Managmt. &
response to cyber-
incidents
[6 ECTS]

Regulatory
compliance of the
NIS2 Directive on
cybersecurity
[0,5 ECTS]

Personal data
protection and
information security
[1 ECTS]

Blockchain tech,
smart contracts,
decentralized apps
and Web 3.0 [5 ECTS]

Master Thesis



4. Conclussions

Training Pathways:

Modular and stackable approach: 14 MUs, 5 TExp, 2 TEsp, 1 MFP.

From technical to stategic aspects .

Aligned with industry/society needs.

Collaboration with comapines and agents (training) .

Complementary to:

International Hackathon

Conferences,

Co-working sessions

Academic Incubator

4. Conclussions

Results and indicators

Assessment in progress (IQAS).

Level of response (average): **>175%** of applications, **>110%** of positions

Title of Microcredential	Positions	Admitted	Enrolled
Introducción a la construcción de sistemas seguros y rol del CISO	20	35	29
Pentesting y seguridad ofensiva	20	30	27
Ciberseguridad y gestión del riesgo	20	27	21
Directiva NIS2 y cumplimiento normativo en ciberseguridad	20	27	21
Implantación y verificación del Esquema Nacional de Seguridad (ENS)	20	28	23
Análisis forense digital en sistemas Windows, Linux y Android	20	26	22
Fundamentos de ciberseguridad: protocolos, servicios y vectores de ataque (CCNA CyberOPS Parte I)	20	23	19
Estrategias de defensa y análisis forense en ciberseguridad (CCNA CyberOPS Parte II)	20	21	17
Protección de datos personales y seguridad de la información	20	18	17
Desarrollo seguro en entornos DevSecOps	20	23	20



**Cátedra de
Ciberseguridad**

Universidad de Oviedo

Mission 2: Advancing Cybersecurity Research



Mission 2: Advancing Cybersecurity Research

Research represents the university's engine for innovation, generating new knowledge that addresses emerging threats and develops next-generation protection mechanisms. European and Spanish institutions have established dedicated research hubs combining investigation, technology development, and collaborative partnerships.

Dedicated Research Centers

Institutions that explicitly articulate research, technology transfer, and education as integrated pillars of excellence in cybersecurity investigation.



1



Mission 2: Advancing Cybersecurity Research

Research represents the university's engine for innovation, generating new knowledge that addresses emerging threats and develops next-generation protection mechanisms. European and Spanish institutions have established dedicated research hubs combining investigation, technology development, and collaborative partnerships.

Dedicated Research Centers

Institutions that explicitly articulate research, technology transfer, and education as integrated pillars of excellence in cybersecurity investigation.



1

2



Growing Publication Impact

Shows interest and “hot topics” on the research community



ScienceDirect



Mission 2: Advancing Cybersecurity Research

Research Impact by the Numbers

7,000+

Annual IEEE Proceedings

Conference publications in IEEE demonstrating sustained growth in cybersecurity research output and knowledge dissemination

8.58

Impact Factor Growth

IEEE Transactions on Information Forensics and Security journal rating, reflecting increasing research influence



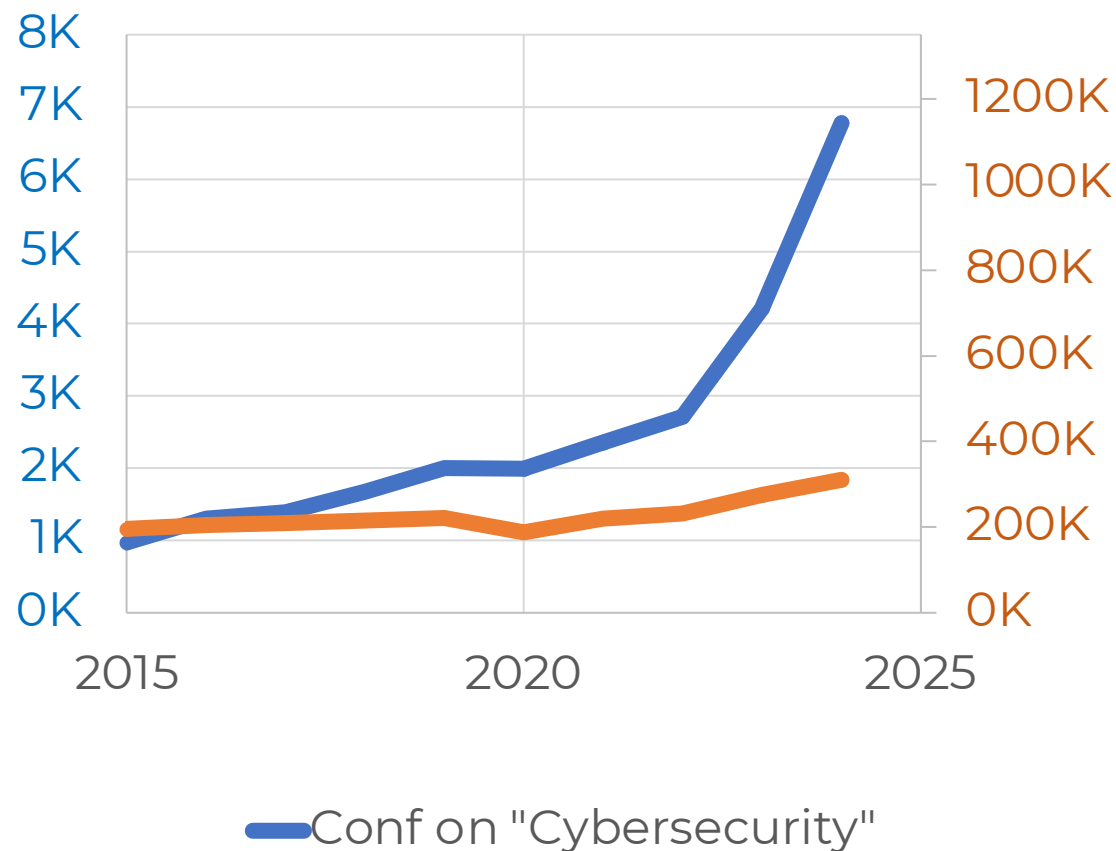
These metrics underscore the exponential growth in cybersecurity research activity, demonstrating how universities contribute foundational knowledge that shapes industry practices, informs policy development, and advances the state of defensive capabilities against evolving threats.

Source: IEEEExplore (nov 2025)

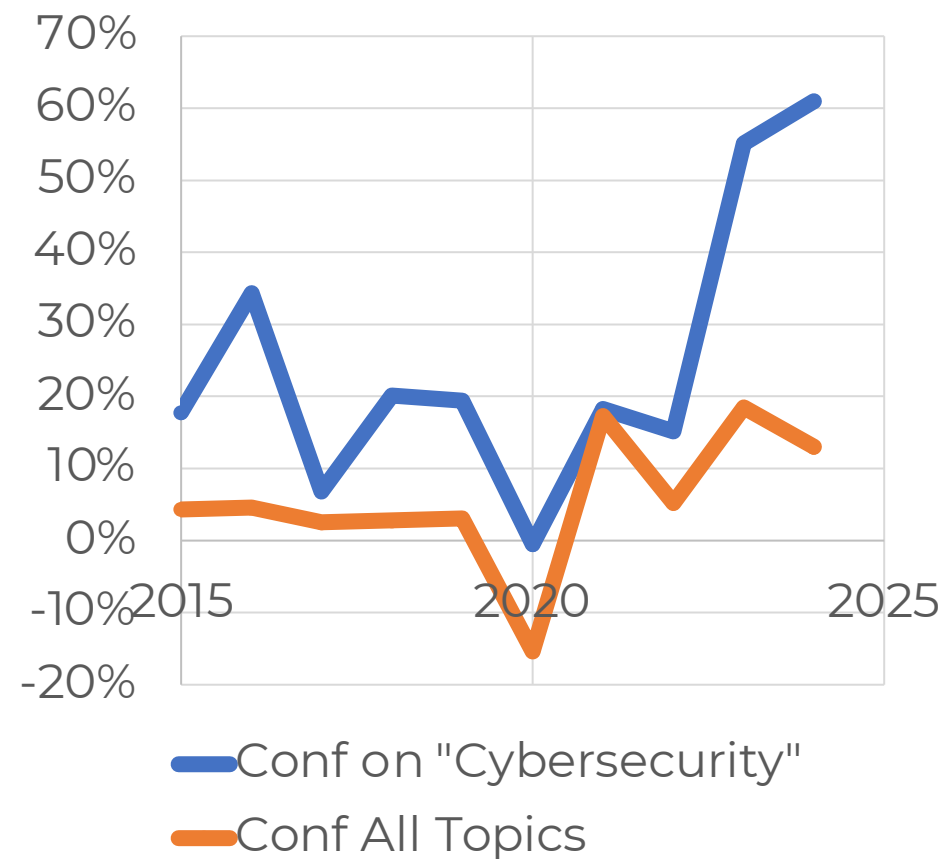
Mission 2: Advancing Cybersecurity Research

Research Impact by the Numbers

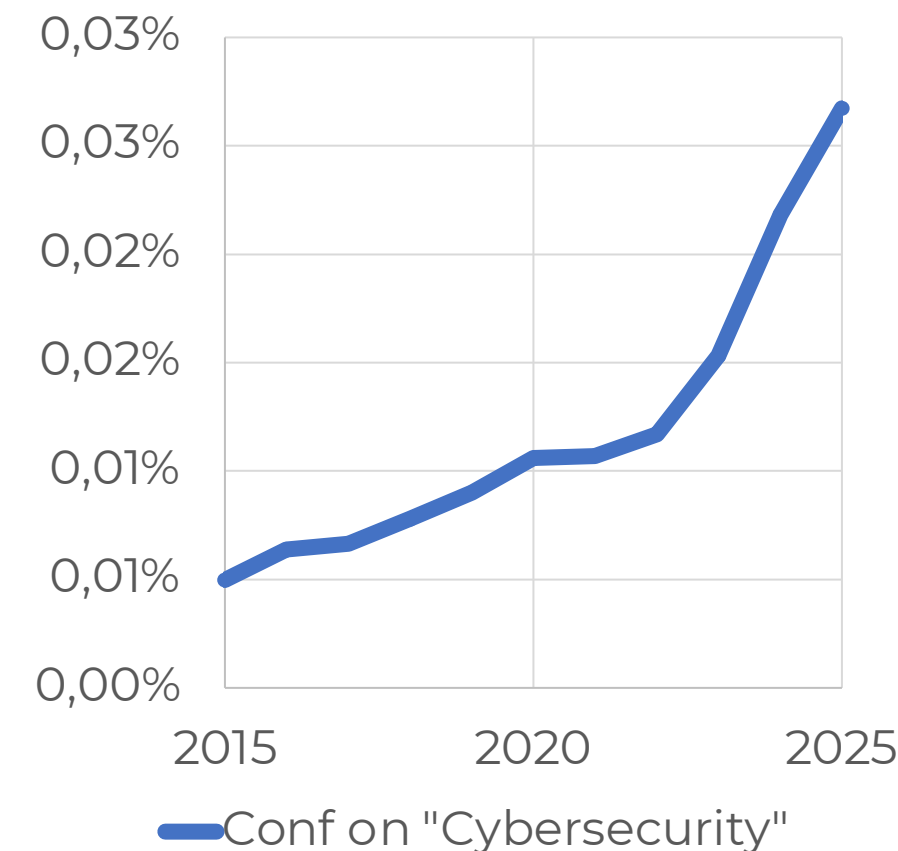
Conferences @ IEEE ("Cyber" vs All)



Yearly Increase on Conferences @ IEEE ("Cyber" vs All)



% of "Cyber" vs All)



Source: IEEEExplore (nov 2025)

Mission 2: Advancing Cybersecurity Research

Research represents the university's engine for innovation, generating new knowledge that addresses emerging threats and develops next-generation protection mechanisms. European and Spanish institutions have established dedicated research hubs combining investigation, technology development, and collaborative partnerships.

Dedicated Research Centers

Institutions that explicitly articulate research, technology transfer, and education as integrated pillars of excellence in cybersecurity investigation.



Funded Research Programs

European and national funding mechanisms support cybersecurity research through competitive calls, collaborative consortia, infrastructure investments, and public-private partnerships.

Growing Publication Impact

Shows interest and “hot topics” on the research community



Mission 2: Advancing Cybersecurity Research

	Level	Funding Line	TRL Range	Typical Budget	Strategic Fit
	Regional – Asturias	GRUPIN (Groups of Research)	1-4	~€40k-€120k for 2-3 years	Build research capacity, base for national/EU proposals.
		SEKUENS/IDEPA Innovation Projects for SMEs	4-7	~€100k-€500k	Applied cybersecurity solutions for industry/digital transition.
	National – Spain	INCIBE “Research Excellence Teams in Cybersecurity”	1-4	~€40k-€250k per team	Build high-level research teams in cybersecurity.
		INCIBE-University Chairs in Cybersecurity	2-6	~€150k-€500k	Education + research + industry transfer.
		CDTI Missions Science & Innovation – Strategic R&D	5-8	~€1M-€5M+	Large industrial R&D in secure systems, energy, infrastructure.

Mission 2: Advancing Cybersecurity Research



Level	Funding Line	TRL Range	Typical Budget	Strategic Fit
European Union	Horizon Europe – Cluster 3 “Civil Security for Society”	3-6	~€3M-€8M per project	International consortia for cybersecurity research, infrastructure resilience.
	Digital Europe Programme – Cybersecurity & Trust (via European Cybersecurity Competence Centre (ECCC))	7-9	~€5M-€20M+	Deployment of SOC's, cyber-ranges, skills, large scale.
	Connecting Europe Facility (CEF2) Digital – Critical Digital Infrastructure	8-9	~€5M-€30M	Secure infrastructure: energy, transport, services.
	European Defence Fund	2-4 to 6-7	€3–12M (research) €10–35M+ (devpt)	Reinforcing EU defence autonomy

Mission 2: Advancing Cybersecurity Research

Research represents the university's engine for innovation, generating new knowledge that addresses emerging threats and develops next-generation protection mechanisms. European and Spanish institutions have established dedicated research hubs combining investigation, technology development, and collaborative partnerships.

Dedicated Research Centers

Institutions that explicitly articulate research, technology transfer, and education as integrated pillars of excellence in cybersecurity investigation.



Funded Research Programs

European and national funding mechanisms support cybersecurity research through competitive calls, collaborative consortia, infrastructure investments, and public-private partnerships.

Growing Publication Impact

Shows interest and “hot topics” on the research community



Target on Impact and Innovation

Universities leverage research contracts with industry partners, participate in multinational consortia, secure patents, and transfer working prototypes to commercialization pathways.





**Cátedra de
Ciberseguridad**

Universidad de Oviedo

Mission 3: Knowledge Transfer and Innovation Ecosystems



Mission 3: Knowledge Transfer and Innovation Ecosystems

Innovation: From Campus to Market



Research Genesis

Innovations originate in labs addressing cybersecurity challenges

Develop & Validation

Testing in controlled environments, proof-of-concept and viability

Market Deployment

Solutions transfer to companies and citizens creating measurable societal value

The special case of Cybersecurity:



Intellectual Property Valorisation



Ecosystem Integration



Innovation Environments



Mission 3: Knowledge Transfer and Innovation Ecosystems

Some Cybersecurity Research Initiatives for Public Administrations

- Cybersecurity Competence Centers
- Living Labs
- Cyber Range Platforms
- Sector-Specific Innovation
- Public Procurement of Innovation



National and Regional Cybersecurity Competence Centers

Establishing dedicated public centers that coordinate applied research, professional training, and policy support creates a unified national cybersecurity ecosystem. These centers serve as strategic hubs connecting government agencies, research institutions, and industry partners.

01

European Leadership



02

National Implementation



03

Research Programs



04

Threat Intelligence



Living Labs: Real-World Cybersecurity Testing Environments

Living labs transform public facilities—municipalities, hospitals, university campuses—into active cybersecurity research environments. These labs enable testing and validation of security solutions within operational infrastructures.



cátedra
thin5G

CÁTEDRA MILLA DEL CONOCIMIENTO
GIJÓN SMART CITIES

It **bridges the gap** between theoretical research and practical implementation, allowing researchers, students, companies, and public administrators to **co-create** and validate cybersecurity solutions under authentic conditions.



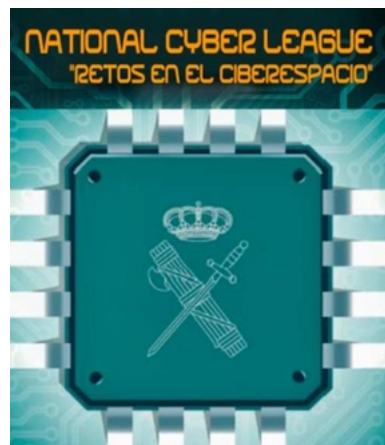
 **Plexigrid**

Cyber Range Platforms for Public Sector Organizations

Strategic Implementation

Universities and public CSIRT teams can establish cyber ranges—sophisticated simulation environments for advancing detection capabilities, training Security Operations Center (SOC) personnel, and conducting joint cyber exercises with critical infrastructure operators.

These platforms provide controlled environments where security teams can safely test response protocols, evaluate emerging threats, and refine incident management procedures without risking operational systems.



**NATIONAL CYBER LEAGUE
DE LA GUARDIA CIVIL**





Sector-Specific Innovation: Healthcare, Justice, Education.

The European Commission is investing €145.5 million to strengthen cybersecurity across healthcare systems and public institutions. These initiatives bring together hospitals, health systems, and cybersecurity providers in collaborative pilot programs that address sector-specific vulnerabilities and compliance requirements.



Healthcare Security

Research electronic health record protection, telemedicine security, pseudonymization techniques, and AI-assisted diagnostics security. Focus on GDPR compliance and patient data sovereignty.



Justice Systems

Develop risk models and business continuity frameworks specific to courts, registries, and law enforcement databases. Address chain of custody and evidence integrity requirements.



Education Networks

Design zero trust architectures for regional education networks, protecting student data and research information while enabling collaborative learning environments.



Sector-Specific Innovation: Energy.

Vulnerable Critical infrastructures

Unique Challenges in Energy Sectors

- Real-time operational requirements with zero tolerance for disruption
- Legacy system integration with modern digital controls
- Physical-cyber attack vector convergence
- Distributed system architectures across wide geographic areas
- Regulatory compliance and national security implications

Universities must develop domain-specific cybersecurity expertise that addresses these unique requirements through targeted research, specialized curricula, and industry-collaborative transfer initiatives.



Public Procurement of Innovation in Cybersecurity



Strategy of Public Procurement of Innovation

(IECPI) from  **incibe**—

224M€

Public procurement of innovation (PPI) transforms government purchasing power into a catalyst for applied cybersecurity research. Through challenge-based procurement, government agencies define security problems, and solutions are co-developed by universities and enterprises in collaborative frameworks.

This approach ensures research addresses genuine operational needs while accelerating the path from laboratory to deployment in public services.

Achieving Integrated Impact Across Three Missions

Significant impact emerges not from executing each mission independently, but through their strategic integration and coherent articulation.

Teaching Programs
Develop specialized talent with current, industry-relevant cybersecurity competencies and certifications

Continuous Feedback
Industry insights refine teaching curricula and research priorities, creating virtuous improvement cycles



Applied Research

Generate innovations addressing real-world challenges identified through teaching and industry partnerships

Industry Transfer

Deploy research outcomes to companies and organizations, creating measurable operational improvements

This **integrated approach** ensures universities generate authentic, measurable impact that extends far beyond traditional metrics of publications and graduations, creating lasting value for society and economy.

Organic Structure for Transfer



Vice-Rectorate of (Knowledge) Transfer and Business Relations

TTO & Spin-Off Companies

Business and Institutional Chairs

Life-Long Learning and Microcredentials

Scientific and Technological Services



Innovation Hub



CREATI.UO
Centro de Recursos y Apoyo a
la Transferencia e Innovación
de la Universidad de Oviedo



**Cátedra de
Ciberseguridad**
Universidad de Oviedo

<https://www.uniovi.es/transferencia>



- Protection of IP
- Valorisation strategy
- license agreements and contracts
- Fostering Spin-Offs and Startups
- Specific Entrepreneurial Programs

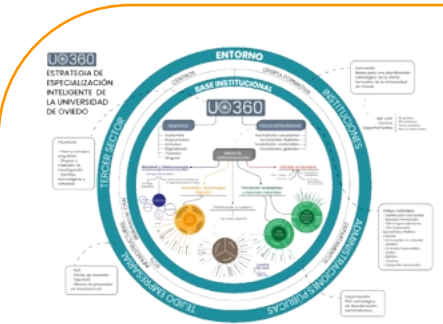
- Dissemination of Knowledge and Transfer Activities
- Direct connection iwth Inn. Ecosystem
- Institutional Events



**foro
transferencia**
Universidad de Oviedo 8 de mayo de 2024
Campus de Gijón



Innovation Ecosystem



Universidad de Oviedo



Oficina de
Transferencia de
Conocimiento



spinoff



INGENIUM
TTO
Network

HEI4S3 RM



Chairs

Chairs



The
Collider



European
Innovation
Council



Financiado por
la Unión Europea
NextGenerationEU



Escuela de
organización
Industrial



SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
E INFRAESTRUCTURAS DIGITALES



Instituto de Investigación Sanitaria
del Principado de Asturias



Fundación para la Investigación y la Innovación
Biosanitaria del Principado de Asturias



Asturias
emprende



GOBIERNO DEL
PRINCIPADO DE ASTURIAS

Regional Tech
Centers



SACI

The sessions this evening



16:45–17:30 – Round Table on Research and Technology Transfer

- o Moderator: Prof. Jose Quiroga Álvarez, Deputy-Director, School of Computer Engineering, University of Oviedo
- o MSc. Joseph Foley, Cybersecurity Technical Officer, MTU Ireland
- o Prof. Andrei Stan, Director, Department of Computer Science, TUIASI, Romania
- o Prof. José Manuel Redondo, Department of Computer Science, University of Oviedo
- o Prof. Jorge García, Head of the Knowledge Transfer Office, University of Oviedo.



17:30–18:30 – Round Table: on Training in Cybersecurity: Are We Meeting Society's Needs?

- o Moderator: Prof. Jorge García, UniOvi
- o Prof. Esther Lorenzo Fernández, UniOvi
- o MPh Stephanie Wallace Chavanne, Res. Chair of Cybersecurity, MTU Ireland
- o Prof. Vlad Mihai Chiriac, Lecturer & Principal Cybersecurity Engineer, TUIASI, Romania
- o Ms. Marie Skavø-Sinisalo, Project Manager, XAMK, Finland
- o Mr. Janne Niinisaari, RDI Expert, XAMK, Finland



18:30–19:00 – Networking and Poster Session

- o Vice-Rectorate for Knowledge Transfer, UniOvi
- o Prof. José Manuel Redondo, UniOvi
- o Prof. Jose Quiroga, UniOvi
- o Prof. Vlad M. Chiriac, TUIASI, Romania
- o Prof. Andrei Stan, TUIASI, Romania
- o Eng. Joseph Foley / MPh Stephanie Wallace Chavanne, MTU Ireland
- o Ms. Marie Skavø-Sinisalo / Mr. Janne Niinisaari, XAMK, Finland
- o Prof. Miguel Hernández Cáceres, UniOvi
- o Prof. José García Fanjul, UniOvi

#CátedrasCiber

Academic Incubator

TANK YOU!!!!



Hackathon Internacional en Ciberseguridad



Universidad de Oviedo