



## EUROPEAN BACHELOR IN CYBERSECURITY & NETWORK MANAGEMENT – EQF LEVEL 6



**Level**  
6 EQF (European  
Qualifications Framework)



**Duration**  
1 year



**Credits**  
60 ECTS



**Target group**  
Students - people seeking  
employment - employees  
and professionals in the  
sector



**Admission requirements**  
Candidates holding a level 5  
EQF qualification or a  
qualification equivalent to the  
attainment of 120 ECTS



**Course Structure**  
Full-time or work-study



**Pedagogical methods**  
Theoretical courses, tutorials  
and practical work  
Case studies and professional  
scenarios  
Individual and group projects



**Professional assessments :**

- Continuous assessment
- Written exam + Case Study (3h)
- Written exam + Case Study (3h)
- Activity report and professional support (30 min)

**CCE :**

- Quizzes (1h20)

**Modern language :**

- Reading Comprehension (1h)
- Listening (45min)

**The FEDE, as a certifier, is in charge of the assessment processes**

- Organisation and planning of exam sessions
- Development of topics and model answers
- Ensuring compliance with examination regulations and supervision (anonymity, integrity, confidentiality)
- Assessment and marking of papers
- Reporting results, issuing diplomas, diploma supplements and certificates

[www.fede.education/en/fede-quality-charter](http://www.fede.education/en/fede-quality-charter)

In response to the explosion of cyber threats and the increase in global economic losses, cybersecurity has become a strategic issue for all sectors.

**The European Bachelor in Cybersecurity and Network Management** trains professionals capable of designing, securing and managing reliable and resilient digital infrastructures. It meets strong market demand in a context marked by the rise of IoT, the growing role of AI in threat detection and the importance of compliance standards such as GDPR or ISO 27001.

### LEARNING OUTCOMES

- Assess risks and recommend corrective actions using recognised audit methodologies (OWASP, CVSS, ISO 27005)
- Configure, deploy and administer security solutions (firewalls, VPNs, IAM) according to standards (ISO 27001, NIST)
- Implement a secure network architecture and Cloud environments
- Lead an incident response strategy and use a SIEM system to detect, analyse and address cyber threats
- Carry out penetration tests and technical audits using specialised tools (Metasploit, Nmap, Burp Suite)
- Design cybersecurity policies in compliance with current standards (GDPR, NIS2, ISO 27001)
- Ensure proactive monitoring to anticipate threats and adapt defence systems
- Raise staff awareness of cybersecurity issues to embed a security culture within the organisation

### PROGRAMME

#### PROFESSIONAL SKILLS (485 À 620 HOURS)

Python programming - SQL databases -Applied mathematics and algorithmic optimisation - Introduction to IT project management - Introduction to systems and network administration - Hardening and security of operating systems - Network security : segmentation, firewalls and monitoring - Identity and access security (IAM) - Cryptography and data protection - Security of digital applications and services - Incident response and cyber crisis management - Securing cloud and Big Data environments - Standards, compliance and risk management in cybersecurity - Cybersecurity monitoring and foresight

#### Professional assignment (≥12 weeks)

Internship - Apprenticeship - Salaried employment

#### MODERN LANGUAGE (60-80 HOURS)

Modern language 1 - CEFR Level B1  
German, English, Spanish, French, Italian, Portuguese  
Modern language 2 and 3 (optional)  
German, English, Arabic, Chinese, Spanish, French, Italian, Portuguese

### CAREER DESTINATIONS

**List of careers accessible at the beginning of a career (0 to 2 years of experience) :**

- SOC analyst
- Network or systems security technician
- Cybersecurity monitoring officer
- Junior cybersecurity consultant
- Junior IAM (Identity and Access Management) specialist
- Cloud or IoT security specialist

**Possible career developments after 2 to 5 years of experience :**

- IT security auditor
- DevSecOps engineer
- Senior cybersecurity consultant
- Cybersecurity project manager
- Incident response and digital forensic specialist
- Cybersecurity manager
- Industrial cybersecurity expert (SCADA, OT systems)

### FEDE'S ASSET - EUROPEAN DEGREE

#### EUROPEAN CULTURE AND CITIZENSHIP (40H)

**The European project: Culture and Democracy for Active Citizenship**

- Importance of History (OHE - Observatory on History Teaching in Europe)
- Contemporary Europe
- Europe and the World
- Cultures and diversity in Europe
- European citizenship
- The Workings of the European Union
- Importance, challenges and future of European construction
- Focus on corruption (GRECO)

#### Intercultural management and human resources

- Culture and cultural diversity
- Intercultural communication in an organisation
- Managing intercultural aspects and resolving cultural conflicts
- Working in Europe
- Social protection systems in Europe
- Corporate Social Responsibility (CSR)