EUROPASS SUPPLEMENT TO THE CERTIFICATE OF THE HIGHER DEGREE SPECIALIZATION COURSE

NAME OF THE SPECIALIZATION COURSE

Advanced Vocational Training Specialization Course on Cybersecurity in Information Technology Environments

---

DESCRIPTION OF THE SPECIALIZATION COURSE

The holder has acquired the general competence relating to:
Define and implement security strategies in information systems by performing cybersecurity diagnostics, identifying vulnerabilities and implementing the necessary measures to mitigate them by applying current regulations and industry standards, following quality protocols, occupational risk prevention and environmental respect.

Within this framework, each PROFESSIONAL MODULE includes the following LEARNING OUTCOMES acquired by the holder.

"Cybersecurity Incidents."
The titleholder:
- Develops cybersecurity prevention and awareness plans, establishing standards and protection measures.
- Analyzes cybersecurity incidents using tools, detection mechanisms and security alerts.
- Investigates cybersecurity incidents by analyzing the risks involved and defining possible countermeasures to adopt.
- Implements cybersecurity measures in networks and systems by responding to detected incidents and applying appropriate protection techniques.
- Detects and documents cybersecurity incidents following established procedures.

"Bastioning of networks and systems".
The titleholder:
- Design securitization plans incorporating best practices for system and network bastioning.
- Configures access control and authentication systems for people while preserving the confidentiality and privacy of data.
- Administers access credentials to computer systems applying the established operational and security requirements.
- Design computer networks taking into account security requirements.
- Configures devices and computer systems in compliance with security requirements.
- Configures devices for the installation of computer systems, minimizing the probability of exposure to attacks.
- Configures computer systems minimizing the probability of exposure to attacks.

" Safe production start-up ".
The titleholder:
- Tests web and mobile applications by analyzing the code structure and execution model.
- Determines the level of security required by applications by identifying common attack vectors and their associated risks.
- Detects and fixes web application vulnerabilities by analyzing their source code and configuring web servers.
- Detects security problems in applications for mobile devices, monitoring their execution and analyzing files and data.
- Implements secure software deployment systems, using tools for the automation of the construction of its elements.

"Computer Forensic Analysis.".
The titleholder:

- Applies forensic analysis methodologies characterizing the preservation, acquisition, analysis and documentation phases.
- Performs forensic analysis on mobile devices, applying established, updated and recognized methodologies.
- Performs Cloud forensic analysis, applying established, updated and recognized methodologies.
- Performs forensic analysis on IoT devices, applying established, updated and recognized methodologies.
- Documents forensic analysis by preparing reports including applicable regulations.

"Ethical Hacking.
The titleholder:

- Determines monitoring tools to detect vulnerabilities by applying ethical hacking techniques.
- Attacks and defends in test environments, wireless communications by gaining access to networks to demonstrate their vulnerabilities.
- Attacks and defends in test environments, networks and systems by gaining access to third-party information and systems.
- Consolidates and utilizes compromised systems guaranteeing future access.
- Attacks and defends web applications in test environments, gaining access to unauthorized data or functionality.

"Cybersecurity regulations".
The titleholder:

- Identifies the main points of application to ensure regulatory compliance by recognizing roles and responsibilities.
- Designs regulatory compliance systems by selecting the applicable legislation and jurisprudence.
- Relates the relevant regulations for compliance with the criminal liability of organizations and legal entities with the established procedures, compiling and applying the current rules.
- Applies national legislation on personal data protection, relating the established procedures with the laws in force and with the existing jurisprudence on the subject.
- Collects and applies the current national and international cybersecurity regulations, updating the established procedures according to the laws and existing jurisprudence on the subject.

JOBS THAT CAN BE PERFORMED WITH THIS SPECIALIZATION COURSE

The most relevant occupations and jobs are as follows:

- Cybersecurity expert.
- Cybersecurity auditor.
- Cybersecurity consultant.
- Ethical hacker.

CERTIFICATE ISSUANCE, ACCREDITATION AND LEVEL

Body issuing the certificate of the higher degree specialization course on behalf of the King: Ministry of Education and Vocational Training or the autonomous communities within the scope of their own competences. The certificate has academic and professional effects valid throughout the State.

Official course duration: 720 hours.

Certificate level (national or international).

- NATIONAL: Non-university higher education.
- INTERNATIONAL:
  - Level P-5.5.4 of the International Standard Classification of Education (ISCED P-5.5.4).
  - Level 5C of the European Qualifications Framework (EQF 5C).

Access requirements: To access the specialization course it is necessary to hold one of the following Higher Vocational Training degrees:

a) Higher Technician in Network Computer Systems Administration established by the Royal Decree 1629/2009, of October 30.
b) Higher Technician in Multiplatform Applications Development, established by the Royal Decree 450/2010, of April 16.
c) Higher Technician in Web Applications Development, established by Royal Decree 686/2010, of May 20.
d) Higher Technician in Telecommunication and Computer Systems, established by Royal Decree 883/2011, of June 24.
e) Higher Technician in Electronic Maintenance, established by Royal Decree 1578/2011, of November 4.

Legal Basis. Regulations establishing the course of specialization in Cybersecurity in information technology environments:
Minimum teaching requirements established by the State: Royal Decree 479/2020, of April 7, which establishes the Specialization Course in Cybersecurity in Information Technology Environments and sets the basic aspects of the curriculum.

Explanatory note: This document is intended as additional information to the title in question, but has no legal validity whatsoever.

TRAINING OF THE OFFICIALLY RECOGNIZED SPECIALIZATION COURSE

PROFESSIONAL MODULES OF THE ROYAL DECREE OF T H E HIGHER GRADE SPECIALIZATION COURSE	**ECTS CREDITS**
Cybersecurity incidents.	9
Bastioning of networks and systems.	10
Safe production start-up.	7
Computer forensic analysis.	7
Ethical hacking.	7
Cybersecurity regulations	3
	TOTAL CREDITS
	43
OFFICIAL DURATION OF T H E SPECIALIZATION C O U R S E CERTIFICATE (HOURS)	***720***

* The minimum teaching requirements for the specialization course reflected in the table above, 50%, are valid throughout the national territory. The remaining 50% belongs to each Autonomous Community and may be reflected in **Annex I** of this supplement.

europass

INFORMATION ABOUT THE EDUCATION SYSTEM