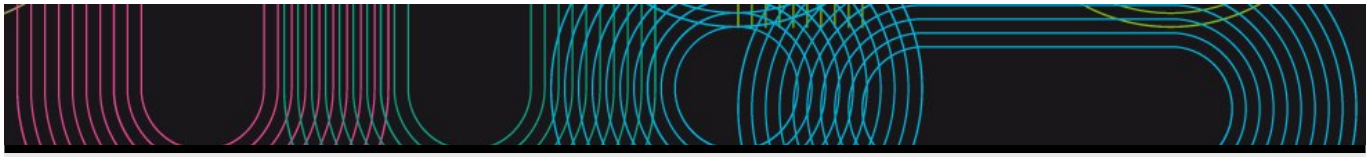

IDENTIFYING DATA				
Internship practice				
Subject	Internship practice			
Code	V05M175V01106			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	15	Mandatory	2nd	1st
Teaching language	Spanish			
Department				
Coordinator	Marcos Acevedo, Jorge			
Lecturers	Marcos Acevedo, Jorge			
E-mail	acevedo@uvigo.es			
Web	http://www.munics.es/			
General description	(*)La misión del máster es formar profesionales de alta cualificación en todos los procesos técnicos, organizativos, operativos y forenses relativos a la seguridad digital. El profesorado pertenece a las áreas de Ingeniería Telemática, Teoría de la Señal y Comunicaciones, Ciencias de la Computación e Inteligencia Artificial, Ingeniería de Sistemas y Derecho Penal de las dos universidades, y se complementa con la contribución de destacados profesionales de empresas del sector en Galicia y el compromiso de éstas en apoyar las prácticas de los estudiantes.			

Competencies	
Code	
A1	To possess and understand the knowledge that provides the foundations and the opportunity to be original in the development and application of ideas, frequently in a research context.
A2	Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization.
A3	Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements.
A4	Students will learn to communicate their conclusions ---and the hypotheses and ultimate reasoning in their support--- to expert and non-expert audiences in a clear and unambiguous way.
A5	Students will apprehend the learning skills enabling them to study in a style that will be self-driven and autonomous to a large extent.
B1	To have skills for analysis and synthesis. To have ability to project, model, calculate and design solutions in the area of information, network or system security in every application area.
B2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.
B3	Capacity for critical thinking and critical evaluation of any system designed for protecting information, any information security system, any system for network security or system for secure communications.
B4	Ethical commitment. Ability to design and deploy engineering systems and management systems with ethical and responsible criteria, based on deontological behaviour, in the field of information, network or communications security
B5	Students will have ability to apply theoretical knowledge to practical situations, within the scope of infrastructures, equipment or specific application domains, and designed for precise operating requirements
B6	Ability to do research. Ability to innovate and contribute to the advance of the principles, the techniques and the processes within their professional domain, designing new algorithms, devices, techniques or models which are useful for the protection public, private or commercial of digital assets.
C1	To know, to understand and to apply the tools of cryptography and cryptanalysis, the tools of integrity, digital identity and the protocols for secure communications.
C2	Deep knowledge of cyberattack and cyberdefense techniques.
C3	Knowledge of the legal and technical standards used in cybersecurity, their implications in systems design, in the use of security tools and in the protection of information.
C4	To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks, databases, computer programs and information services.

C5	To design, deploy and operate a security management information system based on a referenced methodology.
C6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.
C7	To demonstrate ability for doing the security audit of systems, equipment, the risk analysis related to security weaknesses, and for developing de procedures for certification of secure systems.
C8	Skills for conceive, design, deploy and operate cybersecurity systems.
C9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.
C10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.
C11	Ability to collect and interpret relevant data in the field of computer and communications security.
C12	Knowledge of the role of cybersecurity in the design of new industrial processes, as well as of the singularities and restrictions to be addressed in order to build a secure industrial infrastructure.
C13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.
C14	Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards.
C15	Ability to identify the value of information for an institution, economic or of other sort; ability to identify the critical procedures in an institution, and the impact due to their disruption; ability to identify the internal and external requirements that guarantee readiness upon security attacks.
C16	Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization.
C17	Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery.
C18	Ability to correctly interpret the information sources in the discipline of criminal law (laws, doctrine, jurisprudence) both at the national and international levels.
C19	To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector.
C20	Knowledge about the firms specialized in cybersecurity in the region.
D1	Ability to apprehend the meaning and implications of the gender perspective in the different areas of knowledge and in the professional exercise, with the aim of attaining a fairer and more egalitarian society.
D2	Ability for oral and written communication in Galician language.
D3	Ability to include sustainability principles and environmental concerns in the professional practice. To integrate into projects the principle of efficient, responsible and equitable use of resources.
D4	Ability to ponder the importance of information security in the economic progress of society.
D5	Ability for oral and written communication in English.

Learning outcomes	
Expected results from this subject	Training and Learning Results

Experience in the practice of the cybersecurity profession and its usual functions in some real company environment	A1 A2 A3 A4 A5 B1 B2 B3 B4 B5 B6 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 C20 D1 D2 D3 D4 D5

Contents

Topic
The student will make a stay in the company developing own functions of a Master in Ciberseguridad

Planning

	Class hours	Hours outside the classroom	Total hours
Practicum, External practices and clinical practices	375	0	375

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
Practicum, External practices and clinical practices	Stay in companies developing own functions of a Master in Ciberseguridad

Personalized assistance

Methodologies	Description
Practicum, External practices and clinical practices	The students will have a tutor in the company and a tutor in the University, to those who the students will be able to consult doubts on the activity to develop and to those who will have to present the results of the work made.

Assessment

	Description	Qualification	Training and Learning Results

Practicum, External practices and clinical practices	The evaluation will make it the tutor in the University in function of the memory of the work made in the company and of the evaluation of the student by part of the tutor in the company.	100

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

Contingency plan

Description

=== ADAPTATION OF THE METHODOLOGIES ===
* Educational Methodologies that keep
Any because the subject consists of the permanence in a company developing activities adapted to the degree

* Educational Methodologies that modify
All. The subject sewed in the stay in the company of the student during a time. In the case that the teaching was exclusively no face-to-face, the practice in the company only will be able to make if it does in the remote.

* Modifications (if they proceed) of the contents to give
There are no changes

* Additional Bibliography to facilitate the self-learning
There are not

* Other modifications
There are not more modifications

=== ADAPTATION OF THE EVALUATION ===
Unchanged