Teaching Guide				
Identifying Data				2020/21
Subject (*)	External Internship		Code	614530016
Study programme	Máster Universitario en Ciberseguridade			
Descriptors				
Cycle	Period	Year	Type	Credits
Official Master's Degree	1st four-month period	Second	Obligatory	15
Language	SpanishGalician			
Teaching method	Face-to-face			
Prerequisites				
Department	Ciencias da Computación e Tecnoloxías da InformaciónEnxeñaría de Computadores			
Coordinador		E-mail		
Lecturers	Dafonte Vazquez, Jose Carlos Fernández Caramés, Tiago Manuel Fernández Iglesias, Diego López Rivas, Antonio Daniel Novoa De Manuel, Francisco Javier	E-mail	carlos.dafonte@udc.es tiago.fernandez@udc.es diego.fernandez@udc.es daniel.lopez@udc.es francisco.javier.novoa@udc.es	
Web	faitic.uvigo.es			
General description	The mission of the master is to train highly qualified professionals in all technical, organizational, operational and forensic processes related to digital security. The teaching staff belongs to the areas of Telematic Engineering, Signal Theory and Communications, Computer Science and Artificial Intelligence, Systems Engineering and Criminal Law of the two universities, and is complemented by the contribution of leading professionals from companies in the sector in Galicia and their commitment to support student practices.			
Contingency plan	1. Modifications to the contents 2. Methodologies *Teaching methodologies that are maintained *Teaching methodologies that are modified 3. Mechanisms for personalized attention to students 4. Modifications in the evaluation *Evaluation observations: 5. Modifications to the bibliography or webgraphy			

Study programme competences	
Code	Study programme competences
A1	CE1 - 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
A2	CE2 - Deep knowledge of cyberattack and cyberdefense techniques
A3	CE3 - 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
A4	CE4 - To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks, databases, computer programs and information services
A5	CE5 - To design, deploy and operate a security management information system based on a referenced methodology
A6	CE6 - To develop and apply forensic research techniques for analysing incidents or cybersecurity threats

A7	CE7 - 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
A8	CE8 - Skills for conceive, design, deploy and operate cybersecurity systems
A9	CE9 - Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity
A10	CE10 - Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments
A11	CE11 - Ability to collect and interpret relevant data the field of computer and communications security
A12	CE12 - 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
A13	CE13 - Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks
A14	CE14 - Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards
A15	CE15 - 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
A16	CE16 - Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization
A17	CE17 - Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery
A18	CE18 - Ability to correctly interpret the information sources in the discipline of criminal law (laws, doctrine, jurisprudence) both at the national and international levels
A19	CE19 - To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector
A20	CE20 - Knowledge about the firms specialized in cybersecurity in the region
B1	CB1 - 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
B2	CB2 - 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
B3	CB3 - 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
B4	CB4 - Students will learn to communicate their conclusions ---and the hypotheses and ultimate reasoning in their support--- to expert and nonexpert audiences in a clear and unambiguous way
B5	CB5 - Students will apprehend the learning skills enabling them to study in a style that will be selfdriven and autonomous to a large extent
B6	CG1 - 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
B7	CG2 - Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security
B8	CG3 - 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 communication
B9	CG4 - 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
B10	CG5 - 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
B11	CG6 - 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	CT1 - 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
C2	CT2 - Ability for oral and written communication in Galician language
C3	CT3 - 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
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society
C5	CT5 - Ability for oral and written communication in English

Learning outcomes			
Learning outcomes	Study programme competences		
Experience in the performance of the profession and its most common functions in a real business environment.	AJ1 AJ2 AJ3 AJ4 AJ5 AJ6 AJ7 AJ8 AJ9 AJ10 AJ11 AJ12 AJ13 AJ14 AJ15 AJ16 AJ17 AJ18 AJ19 AJ20	BJ1 BJ2 BJ3 BJ4 BJ5 BJ6 BJ7 BJ8 BJ9 BJ10 BJ11	CJ1 CJ2 CJ3 CJ4 CJ5

Contents	
Topic	Sub-topic
The student will make a stay in the company developing functions of a Master in Cybersecurity	

Planning				
Methodologies / tests	Competencies	Ordinary class hours	Student?s personal work hours	Total hours
Clinical practice placement	A1 A2 A3 A4 A5 A6 A7 A8 A9 A10 A11 A12 A13 A14 A15 A16 A17 A18 A19 A20 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 C1 C2 C3 C4 C5	375	0	375
Personalized attention		0		0
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	Description
Clinical practice placement	Prácticas externas: Estancia en empresas desarrollando funcións propias dun Master en Ciberseguridad

Personalized attention	
Methodologies	Description

Clinical practice placement	The students will have a tutor in the company and a tutor in the University, to whom the students will be able to consult doubts about the activity to develop and to whom they will have to present the results of their work.

Assessment			
Methodologies	Competencies	Description	Qualification
Clinical practice placement	A1 A2 A3 A4 A5 A6 A7 A8 A9 A10 A11 A12 A13 A14 A15 A16 A17 A18 A19 A20 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 C1 C2 C3 C4 C5	The evaluation will be carried out by the tutor in the University based on the memory of the work done in the company and the evaluation of the student by the tutor in the company.	0

Assessment comments

Sources of information	
Basic	
Complementary	

Recommendations
Subjects that it is recommended to have taken before
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.