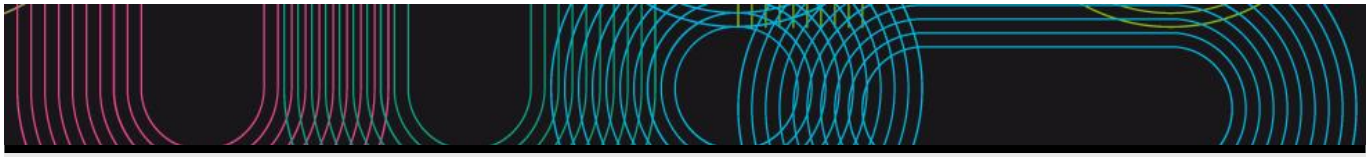

Escola de Enxeñaría de Telecomunicación

(*)Páxina web

(*)

www.teleco.uvigo.es

(*)Presentación

The School of Telecommunication Engineering (EET) is a higher education school of the University of Vigo that offers Bachelor's degrees, Master's degrees and Doctoral programs in the fields of Telecommunications Engineering.

Bachelor's Degree in Telecommunication Technologies Engineering (EUR-ACE®).

The mail goal of the Bachelor's Degree in Telecommunication Technologies Engineering is to form professionals at the forefront of technological knowledge and professional competences in telecommunication engineering. This Bachelor has been recognized with the best quality seals, like the EUR-ACE's. **It has a bilingual option: up to 80% of the degree credits can be taken in English**.

http://teleco.uvigo.es/images/stories/documentos/gett/degree_telecom.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/gett

Master in Telecommunication Engineering

The Master in Telecommunication Engineering is a Master's degree that qualifies to exercise the profession of Telecommunication Engineer, in virtue of the established in the Order CIN/355/2009 of 9 of February.

http://teleco.uvigo.es/images/stories/documentos/met/master_telecom_rev.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/mit

Interuniversity Masters

The current academic offer includes interuniversity master's degrees that are closely related to the business sector:

Master in Cybersecurity: www: https://www.munics.es/

Master in Industrial Mathematics: www: http://m2i.es

International Master in Computer Vision: www: https://www.imcv.eu/

(*)Equipo directivo

MANAGEMENT TEAM

Directora: Rebeca Pilar Díaz Redondo (teleco.direccion@uvigo.gal)

Secretaría e Subdirección de Novas Titulacións: Pedro Rodríguez Hernández

(teleco.subdir.secretaria@uvigo.gal;teleco.subdir.novastitulacions@uvigo.gal)

Subdirección de Organización Académica: Pedro Comesaña Alfaro (teleco.subdir.academica@uvigo.gal)

Subdirección de Relaciones Internacionais e Subdirección de Infraestructuras: María Verónica Santalla del

Río (teleco.subdir.internacional@uvigo.gal; teleco.subdir.infraestructuras@uvigo.gal)

Subdirección Difusión e Captación: Laura Docio Fernández (teleco.subdir.captacion@uvigo.gal)

Subdirección de Calidade: Ana María Cao Paz(teleco.subdir.calidade@uvigo.gal)

BACHELOR□SDEGREE IN TELECOMMUNICATION TECHNOLOGIES ENGINEERING

Generalcoordinator: Lucía Costas Pérez (teleco.grao@uvigo.gal)

https://teleco.uvigo.es/es/documentos/acordos-es/comisions-academicas-es/miembros-de-la-comision-academica-del-gett/

MASTER IN TELECOMMUNICATION ENGINEERING

Generalcoordinator: Manuel García Sánchez (teleco.master@uvigo.gal)

https://teleco.uvigo.es/es/documentos/acordos-es/comisions-academicas-es/miembros-de-la-comision-academica-del-met/

MASTER INCYBERSECURITY

General coordinator:Ana Fernández Vilas (teleco.munics@uvigo.gal)

https://teleco.uvigo.es/es/documentos/acordos-es/comisions-academicas-es/miembros-de-la-comision-academica-del-munics/

MASTER ININDUSTRIAL MATHEMATICS

Generalcoordinator: Elena Vázquez Cendón (USC)

UVigo coordinator:José Durany Castrillo (durany@dma.uvigo.es)

http://www.m2i.es/?seccion=coordinacion

INTERNATIONALMASTER IN COMPUTER VISION

General coordinator: Xose Manuel Pardo López (USC)

UVigo coordinator:José Luis Alba Castro (jalba@gts.uvigo.es)

https://www.imcv.eu/legal-notice/

MASTER'S DEGREE IN QUANTUM INFORMATION SCIENCE AND TECHNOLOGIES (MQIST)

General coordinator: Javier Mas (USC)

Coordinador UVIGO: Manuel Fernández Veiga(teleco.mqist@uvigo.es)

https://quantummastergalicia.es/info

Máster Universitario en Ciberseguridad (en extinción)

Subjects			
Year 2nd			
Code	Name	Quadmester	Total Cr.
V05M175V01106	Internships	1st	15
V05M175V01107	Master´s Thesis	1st	15

IDENTIFYING DATA				
Internships				
Subject	Internships			
Code	V05M175V01106			
Study programme	Máster Universitario en Ciberseguridad (en extinción)			
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	The master's degree mission is to train highly qualified professionals in all technical, organizational, operational and forensic processes related to digital security. All teachers belong to the areas of Telematics Engineering, Signal Theory and Communications, Computer Science and Artificial Intelligence, Systems Engineering and Criminal Law from two universities, and are complemented by the contribution of prominent professionals from companies in this sector in Galicia and their commitment to support students' internships.			

Training and Learning Results	
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.

Expected results from this subject

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	
General content	To be defined by both the tutor in the company and the academic tutor.
Integration in the company and in his surroundings of work	During his internship the student will be integrated into the company organization and collaborate with the members of their work team.

Development of his professional activity	The student will carry out the assigned tasks in accordance with his knowledges and competences.

Planning

	Class hours	Hours outside the classroom	Total hours
Practicum, External practices and clinical practices	370	5	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 a company developing functions of a Master Degree in Cybersecurity so that they can put into practice the knowledge and skills acquired, to complete their academic training.

Personalized assistance

Methodologies	Description
Practicum, External practices and clinical practices	The student will have a tutor in the company that will guide and supervise him in the specific tasks to be carried out; and an academic tutor -professor of the EET. of the University of Vigo or de la FIC of the Universidad da Coruña- who will define, together with the company tutor, the general framework of the student activity to guarantee that it is appropriate for student profile.

Assessment

	Description	Qualification	Training and Learning Results			
Practicum, External practices and clinical practices	The assessment will take into account: (1) The report of activities and (2) The assessment of the company tutor.	100	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

Other comments on the Evaluation

REPORT OF ACTIVITIES: The student must submit a report explaining the activities undertaken during practices, specifying its duration, departments of the company that were conducted, training received (courses, software, etc.), the level of integration within the company and personal relationships.

The report must also include a section of conclusions, containing a reflection on the adequacy of the lessons learned during the university studies to performance practice (negative and positive aspects significant related to the development of practices). It also assessed the inclusion of information on the professional and personal experience with the practices (personal assessment of learning achieved over practices or own contributions and suggestions on the structure and operation of the company visited).

The assessment of memory will be 60% of the final qualification.

COMPANY TUTOR EVALUATION: The company tutor will submit a report assessing aspects with the practices carried out by students: punctuality, attendance, responsibility, teamwork ability and integration in the enterprise, quality of work done,

etc.

The assessment of the tutor in the company will be 40% of the final qualification.

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Master´s Thesis				
Subject	Master´s Thesis			
Code	V05M175V01107			
Study programme	Máster Universitario en Ciberseguridad (en extinción)			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	15	Mandatory	2nd	1st
Teaching language	Spanish Galician English			
Department				
Coordinator	Caeiro Rodríguez, Manuel			
Lecturers	Caeiro Rodríguez, Manuel			
E-mail	mcaeiro@det.uvigo.es			
Web	http://moovi.uvigo.es			
General description	The Master Thesis (TFM) is an academic work, personal and original that is presented in public and that is evaluated by a panel. It is a project where the student has to show the knowledge acquired during the master studies. It must conclude with a written dissertation including explanations, theories, ideas, reasonings, description of developments or designs, etc. It should address a topic chosen by the student, and supervised by a director or directors, that will care for its progression and its quality. Nonetheless, the Master Thesis is the responsibility of the aspirant to the title of Master.			

Training and Learning Results	
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.
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.

Expected results from this subject

Expected results from this subject	Training and Learning Results
Capacity for planning and executing an original work in the cybersecurity field.	A1 A2 A3 A4 A5
Capacity for finding relevant information in the cybersecurity field, for its study and analysis, and the retrieval of relevant results.	B1 B3 B5 B6 D1 D3 D4 D5

Resolution of original problems with real implications in the cybersecurity field.	A1 A2 A3 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 D3 D4 D5
Elaboration of a project report that summarizes the state of the art, the analyzed problematic, the objectives, the completed work, the conclusions and the future lines.	A1 A3 A4 B1 B2 B6
Presentation of a summary of the main results in front of a public jury.	A4 D1 D4

Contents

Topic
The Master's Thesis is an academic, personal and original work in which the student has to show the knowledge obtained during the master. Therefore, the content of each work must be unique. Nevertheless, it must show the ability of the student to analyze a problem in a systematic way, propose solutions, analyze the results obtained and expose them clearly.

Planning

	Class hours	Hours outside the classroom	Total hours
Mentored work	0	350	350
Presentation	1	24	25

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

Methodologies

	Description

Mentored work	The student will complete an academic, personal and original work in which he will have to show the knowledge obtained during the master. It must conclude with a set of written explanations, theories, ideas, reasoning, description of developments or designs, etc. on a subject chosen by the student, and supervised by a tutor or tutors, who will ensure the correct progression and the quality level.

Personalized assistance

Methodologies	Description
Mentored work	During the Master's Thesis there will be periodic meetings between the student and the tutors to define, orient, supervise and delimit the work, as well as to orient the writing of the dissertation. The TFMcoordinator will establish tutoring hours at the beginning of the term. These hours could be checked at the subject web page https://moovi.uvigo.gal/.

Tests	Description
Presentation	The directors of the work will guide the student in the preparation of the presentation of the work at the end of the master's degree. The TFM coordinator will establish tutoring hours at the beginning of the term. These hours could be checked at the subject web page https://moovi.uvigo.gal/.

Assessment

	Description	Qualification	Training and Learning Results
Mentored work	The work will be evaluated by a panel. The student will provide a written dissertation, and will make a public presentation. The panel will use a rubric that will be publicly available.	100	

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Manuel Ruiz-de-Luzuriaga-Peña, **Guía para citar y referenciar. Estilo IEEE**, Universidad Pública de Navarra, 2016

Recommendations