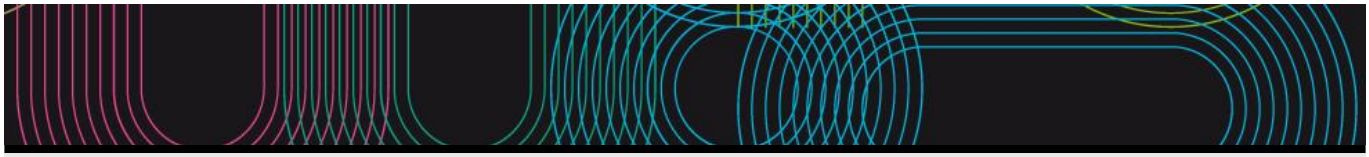

(*)Escola de Enxeñaría de Telecomunicación

(*)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

Director: Íñigo Cuíñas Gómez (teleco.direccion@uvigo.es)

Subdirección de Relaciones Internacionales: Enrique Costa Montenegro (teleco.subdir.internacional@uvigo.es)

Subdirección de Extensión: Francisco Javier Díaz Otero (teleco.subdir.extension@uvigo.es)

Subdirección de Organización Académica: Manuel Fernández Veiga (teleco.subdir.academica@uvigo.es)

Subdirección de Calidad: Loreto Rodríguez Pardo (teleco.subdir.calidade@uvigo.es)

Secretaría y Subdirección de Infraestruturas: Miguel Ángel Domínguez Gómez (teleco.subdir.infraestructuras@uvigo.es)

BACHELOR□S DEGREE IN TELECOMMUNICATION TECHNOLOGIES ENGINEERING

General coordinator: Rebeca Díaz Redondo (teleco.grao@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_grao.pdf

MASTER IN TELECOMMUNICATION ENGINEERING

General coordinator: Manuel Fernández Iglésias (teleco.master@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_master.pdf

MASTER IN CYBERSECURITY

General coordinator: Ana Fernández Vilas (camc@uvigo.es)

http://teleco.uvigo.es/images/stories/documentos/comisions/membros_comisions_master_ciberseguridade.pdf

MASTER IN INDUSTRIAL MATHEMATICS

General coordinator: Elena Vázquez Cendón (USC)

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

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

INTERNATIONAL MASTER 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 Cybersecurity

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

IDENTIFYING DATA				
Internship practice				
Subject	Internship practice			
Code	V05M175V01106			
Study programme	Master´s Degree in Cybersecurity			
Descriptors	ECTS Credits	Type	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.			

Competencies	
Code	
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.
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.
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.
CB4	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.
CB5	Students will apprehend the learning skills enabling them to study in a style that will be self-driven and autonomous to a large extent.
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.
CG2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.
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 communications.
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
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
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.
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.
CE2	Deep knowledge of cyberattack and cyberdefense techniques.
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.
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.
CE5	To design, deploy and operate a security management information system based on a referenced methodology.
CE6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.
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.
CE8	Skills for conceive, design, deploy and operate cybersecurity systems.
CE9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.
CE10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.
CE11	Ability to collect and interpret relevant data in the field of computer and communications security.
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.

CE13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.
CE14	Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards.
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.
CE16	Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization.
CE17	Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery.
CE18	Ability to correctly interpret the information sources in the discipline of criminal law (laws, doctrine, jurisprudence) both at the national and international levels.
CE19	To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector.
CE20	Knowledge about the firms specialized in cybersecurity in the region.
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.
CT2	Ability for oral and written communication in Galician language.
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.
CT4	Ability to ponder the importance of information security in the economic progress of society.
CT5	Ability for oral and written communication in English.

Learning outcomes

Learning outcomes	Competences
Experience in the practice of the cybersecurity profession and its usual functions in some real company environment	CB1 CB2 CB3 CB4 CB5 CG1 CG2 CG3 CG4 CG5 CG6 CE1 CE2 CE3 CE4 CE5 CE6 CE7 CE8 CE9 CE10 CE11 CE12 CE13 CE14 CE15 CE16 CE17 CE18 CE19 CE20 CT1 CT2 CT3 CT4 CT5

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	Evaluated Competencess			
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	CB1 CB2 CB3 CB4 CB5	CG1 CG2 CG3 CG4 CG5 CG6	CE1 CE2 CE3 CE4 CE5 CE6 CE7 CE8 CE9 CE10 CE11 CE12 CE13 CE14 CE15 CE16 CE17 CE18 CE19 CE20	CT1 CT2 CT3 CT4 CT5

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

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

IDENTIFYING DATA				
Master´s Thesis				
Subject	Master´s Thesis			
Code	V05M175V01107			
Study programme	Master´s Degree in Cybersecurity			
Descriptors	ECTS Credits	Type	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.			

Competencies	
Code	
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.
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.
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.
CB4	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.
CB5	Students will apprehend the learning skills enabling them to study in a style that will be self-driven and autonomous to a large extent.
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.
CG2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.
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 communications.
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
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
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.
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.
CE2	Deep knowledge of cyberattack and cyberdefense techniques.
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.
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.
CE5	To design, deploy and operate a security management information system based on a referenced methodology.
CE6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.
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.
CE8	Skills for conceive, design, deploy and operate cybersecurity systems.
CE9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.
CE10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.

CE11	Ability to collect and interpret relevant data in the field of computer and communications security.
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.
CE13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.
CE14	Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards.
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.
CE16	Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization.
CE17	Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery.
CE18	Ability to correctly interpret the information sources in the discipline of criminal law (laws, doctrine, jurisprudence) both at the national and international levels.
CE19	To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector.
CE20	Knowledge about the firms specialized in cybersecurity in the region.
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.
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.
CT4	Ability to ponder the importance of information security in the economic progress of society.
CT5	Ability for oral and written communication in English.

Learning outcomes

Learning outcomes	Competences
Capacity for planning and executing an original work in the cybersecurity field.	CB1 CB2 CB3 CB4 CB5
Capacity for finding relevant information in the cybersecurity field, for its study and analysis, and the retrieval of relevant results.	CG1 CG3 CG5 CG6 CT1 CT3 CT4 CT5

Resolution of original problems with real implications in the cybersecurity field.	CB1 CB2 CB3 CG1 CG2 CG3 CG4 CG5 CG6 CE1 CE2 CE3 CE4 CE5 CE6 CE7 CE8 CE9 CE10 CE11 CE12 CE13 CE14 CE15 CE16 CE17 CE18 CE19 CE20 CT1 CT3 CT4 CT5
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.	CB1 CB3 CB4 CG1 CG2 CG6
Presentation of a summary of the main results in front of a public jury.	CB4 CT1 CT4

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.

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.

Assessment

	Description	Qualification	Evaluated Competencess
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

Contingency plan

Description

=== EXCEPTIONAL PLANNING ===
Given the uncertain and unpredictable evolution of the health alert caused by COVID-19, the University of Vigo establishes an extraordinary planning that will be activated when the administrations and the institution itself determine it, considering safety, health and responsibility criteria both in distance and blended learning. These already planned measures guarantee, at the required time, the development of teaching in a more agile and effective way, as it is known in advance (or well in advance) by the students and teachers through the standardized tool.

=== ADAPTATION OF THE METHODOLOGIES ===
To public presentation will be performed using videoconferencing tools.

There are no other changes in the subject.