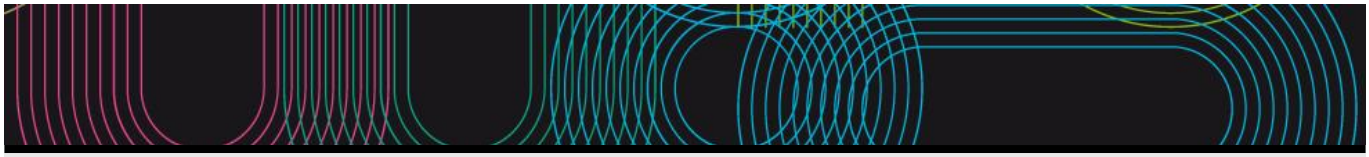

(*)Escola de Enxeñaría de Telecomunicación

(*)Páxina web

(*)

www.teleco.uvigo.es

(*)Presentación

(*)

A Escola Enxeñaría de Telecomunicación oferta para o curso académico 2017-18 un grao e dous másteres totalmente adaptados ao Espacio Europeo de Educación Superior, verificados pola ANECA axustándose á Orde Ministerial CIN/352/2009. A continuación indícanse os enlaces de acceso aos dípticos informativos dos tres títulos.

Grao en Enxeñaría de Tecnoloxías de Telecomunicación

http://teleco.uvigo.es/images/stories/documentos/gett/diptico-uvigo-eet-grao-gal.pdf

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

Máster en Enxeñaría de Telecomunicación

http://teleco.uvigo.es/images/stories/documentos/met/diptico-uvigo-eet-master-gal.pdf

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

Máster Interuniversitario en Matemática Industrial

http://teleco.uvigo.es/images/stories/documentos/promocion/M2i_Presentacion.pdf

www: http://m2i.es

(*)Equipo directivo

(*)

EQUIPO DIRECTIVO DEL CENTRO

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

Subdirección de Relaciones Internacionais: 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 Calidade: Loreto Rodríguez Pardo (teleco.subdir.calidade@uvigo.es)

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

COORDINACIÓN DEL GRADO

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

Coordinadora do Módulo de Formación Básica: Inés García-Tuñón Blanca (inesgt@com.uvigo.es)

Coordinadora do Módulo de Telecomunicación: Yolanda Blanco Fernández (Yolanda.Blanco@det.uvigo.es)

Coordinadora do Módulo de Sistemas Electrónicos: Lucía Costas Pérez (lcostas@uvigo.es)

Coordinador do Módulo de Sistemas de Telecomunicación: Marcos Curty Alonso (mcurty@com.uvigo.es)

Coordinador do Módulo de Sone Imaxe: Manuel Sobreira Seoane (msobre@gts.uvigo.es)

Coordinador do Módulo de Telemática : Raúl Rodríguez Rubio (rrubio@det.uvigo.es)

Coordinadora do Módulo de Optatividad: Ana Vázquez Alejos (analejos@uvigo.es)

Coordinador de Proxectos: Manuel Caeiro Seoane (manuel.caeiro@det.uvigo.es)

Coordinador de Mobilidade: Enrique Costa Montenegro (teleco.subdir.internacional@uvigo.es)

Coordinador de Prácticas Externas: Jorge Marcos Acevedo (teleco.practicas@uvigo.es)

Coordinador do TFG : Manuel Fernández Veiga (teleco.subdir.academica@uvigo.es)

Coordinador do Plan de Acción Titorial: Artemio Mojón Ojea (teleco.pat@uvigo.es)

COORDINACIÓN DO MESTRADO EN ENXEÑARÍA DE TELECOMUNICACIÓN

Coordinadora Xeral: María José Moure Rodríguez (teleco.master@uvigo.es)

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN MATEMÁTICA INDUSTRIAL

Coordinador Xeral: José Durany Castrillo (durany@dma.uvigo.es)

(*)Máster Universitario en Ciberseguridade

Subjects			
Year 2nd			
Code	Name	Quadmester	Total Cr.
V05M175V01106	Prácticas en empresa	1st	15
V05M175V01107	Traballo Fin de Máster	1st	15

IDENTIFYING DATA				
Internship practice				
Subject	Internship practice			
Code	V05M175V01106			
Study programme	(*)Máster Universitario en Ciberseguridade			
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	(*)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		Typology
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.	• Know be
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.	• Know be
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.	• Know be
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.	• Know be
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.	• Know be
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.	• Know be
CG2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.	• Know be
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.	• Know be
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	• Know be
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	• Know be
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.	• Know be
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.	• Know be
CE2	Deep knowledge of cyberattack and cyberdefense techniques.	• Know be
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.	• Know be
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.	• Know be
CE5	To design, deploy and operate a security management information system based on a referenced methodology.	• Know be
CE6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.	• Know be
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.	• Know be
CE8	Skills for conceive, design, deploy and operate cybersecurity systems.	• Know be
CE9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.	• Know be

CE10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.	• Know be
CE11	Ability to collect and interpret relevant data in the field of computer and communications security.	• Know be
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.	• Know be
CE13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.	• Know be
CE14	Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards.	• Know be
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.	• Know be
CE16	Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization.	• Know be
CE17	Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery.	• Know be
CE18	Ability to correctly interpret the information sources in the discipline of criminal law (laws, doctrine, jurisprudence) both at the national and international levels.	• Know be
CE19	To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector.	• Know be
CE20	Knowledge about the firms specialized in cybersecurity in the region.	• Know be
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.	• Know be
CT2	Ability for oral and written communication in Galician language.	• Know be
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.	• Know be
CT4	Ability to ponder the importance of information security in the economic progress of society.	• Know be
CT5	Ability for oral and written communication in English.	• Know be

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
(*)El alumno realizará una estancia en la empresa desarrollando funciones propias de un Master en Ciberseguridad

Planning

	Class hours	Hours outside the classroom	Total hours
External 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
External practices	Estancia en empresas desarrollando funciones propias de un Master en Ciberseguridad

Personalized assistance

Methodologies	Description
External practices	

Assessment

	Description	Qualification	Evaluated Competencess
External practices	(*)La evaluación la realizará el tutor en la Universidad en función de la memoria del trabajo realizado en la empresa y de la evaluación del alumno por parte del tutor en la empresa.	0	

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Master´s Thesis				
Subject	Master´s Thesis			
Code	V05M175V01107			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Type	Year	Quadmester
	15	Mandatory	2nd	1st
Teaching language				
Department				
Coordinator	Gil Castiñeira, Felipe José			
Lecturers	Gil Castiñeira, Felipe José			
E-mail	felipe@uvigo.es			
Web	http://munics.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		Typology
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.	• know
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.	• Know How
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.	• Know How
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.	• Know How
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.	• know • Know How
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.	• know • Know How
CG2	Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information, network or system security.	• know • Know How
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.	• know • Know How
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	• know • Know How
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	• know • Know How
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.	• know • Know How
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.	• know
CE2	Deep knowledge of cyberattack and cyberdefense techniques.	• know
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.	• know
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.	• know • Know How
CE5	To design, deploy and operate a security management information system based on a referenced methodology.	• Know How
CE6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.	• Know How
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.	• Know How

CE8	Skills for conceive, design, deploy and operate cybersecurity systems.	• Know How
CE9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.	• Know How
CE10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.	• know
CE11	Ability to collect and interpret relevant data in the field of computer and communications security.	• Know How
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.	• know
CE13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.	• Know How
CE14	Ability to develop a continuity business plan on the guidelines of commonly accepted norms and standards.	• Know How
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.	• Know How
CE16	Ability for envisioning and driving the business operations in areas related to cybersecurity, with feasible monetization.	• Know How
CE17	Ability to plan a time schedule containing the detection periods of incidents or disasters, and their recovery.	• Know How
CE18	Ability to correctly interpret the information sources in the discipline of criminal law (laws, doctrine, jurisprudence) both at the national and international levels.	• Know How
CE19	To learn how to identify the best professional profiles for an institution as a functions of its features and activity sector.	• know
CE20	Knowledge about the firms specialized in cybersecurity in the region.	• know
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.	• know • Know How
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.	• know • Know How
CT4	Ability to ponder the importance of information security in the economic progress of society.	• know
CT5	Ability for oral and written communication in English.	• Know How

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
he 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, http://www2.unavarra.es/gesadj/servicioBiblioteca/tutoriales/Citar_referenciar_(IEEE).pdf

Recommendations