



## (\*)Escola de Enxeñaría de Telecomunicación

### (\*)Páxina web

(\*)

[www.teleco.uvigo.es](http://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 indicanse 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](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](mailto:teleco.direccion@uvigo.es))

Subdirección de Relaciones Internacionais: Enrique Costa Montenegro ([teleco.subdir.internacional@uvigo.es](mailto:teleco.subdir.internacional@uvigo.es))

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

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

Subdirección de Calidade: Loreto Rodríguez Pardo ([teleco.subdir.calidade@uvigo.es](mailto:teleco.subdir.calidade@uvigo.es))

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

#### COORDINACIÓN DEL GRADO

Coordinadora General: Rebeca Díaz Redondo ([teleco.grao@uvigo.es](mailto: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 1st

Code	Name	Quadmester	Total Cr.
V05M175V01101	Xestión da seguridade da información	1st	6
V05M175V01102	Seguridade da información	1st	6
V05M175V01103	Seguridade en comunicacións	1st	6
V05M175V01104	Seguridade de aplicacións	1st	6
V05M175V01105	Redes Seguras	1st	6
V05M175V01201	Conceptos e leis en ciberseguridade	2nd	3
V05M175V01202	Fortificación de sistemas operativos	2nd	5
V05M175V01203	Tests de intrusión	2nd	5
V05M175V01204	Análise de malware	2nd	5
V05M175V01205	Seguridade como negocio	2nd	3
V05M175V01206	Seguridade en dispositivos móbiles	2nd	3
V05M175V01207	Análise forense de equipos	2nd	3
V05M175V01208	Seguridade ubicua	2nd	3
V05M175V01209	Ciberseguridade en contornas industriais	2nd	3
V05M175V01210	Xestión de incidentes	2nd	3

<b>IDENTIFYING DATA</b>				
<b>Management of Information Security</b>				
Subject	Management of Information Security			
Code	V05M175V01101			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Type	Year	Quadmester
	6	Mandatory	1st	1st
Teaching language	Spanish Galician			
Department				
Coordinator	Caeiro Rodríguez, Manuel			
Lecturers	Caeiro Rodríguez, Manuel Dafonte Vázquez, José Carlos Fernández Vilas, Ana			
E-mail	mcaeiro@det.uvigo.es			
Web	<a href="http://faitic.uvigo.es">http://faitic.uvigo.es</a>			
General description	This subject introduces the fundamental concepts related to the management of information security (e.g. vulnerability, threat, risk). It is devoted to the study of the methodologies, tools and specifications that deal with risk analysis and the development of information security management systems.			

<b>Competencies</b>	
Code	Typology
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.
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.
CE5	To design, deploy and operate a security management information system based on a referenced methodology.
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.
CE13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.
CT4	Ability to ponder the importance of information security in the economic progress of society.
CT5	Ability for oral and written communication in English.

<b>Learning outcomes</b>	
Learning outcomes	Competences
To know the fundamental concepts related to Information Security Management: vulnerability, threat, risk, countermeasure, security policy, security plan	CB2 CB3 CT4 CT5
To know the different Information Security Management methodologies, commonly accepted	CG1 CG2 CE5 CT5
To know the proper tools to carry out tasks related to risk analysis and security audit, as well as knowing which are the most appropriate for each environment	CG1 CG2 CE7 CE13 CT5

<b>Contents</b>
Topic

Foundations	Basic concepts: confidentiality, integrity, availability, threat, risk, etc. Legal framework of cybersecurity Standardization: standards and specifications Security operations centers
Risk analysis, management and certification	ISO 27005 and ISO 31000 Methodologies and risk analysis tools National Security Strategy
Information Security Management Systems	ISO27000, 27001 and 27002 National Scheme of Evaluation and Certification of Information Technologies Classification of information Training and awareness
Business impact	Cybersecurity roles Typical sequence of an attack Resilience Business continuity management Contingency plan
Security audit	Control objectives Frameworks and standards for the audit Audit of personal data security Delegate of data protection

### Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	19.5	39	58.5
Laboratory practical	18	57	75
Objective questions exam	1.5	3	4.5
Case studies	3	9	12

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

### Methodologies

	Description
Lecturing	Presentation by the faculty of the subject syllabus. This methodology will be used to work on competencies: CE5, CE7, CE13, CT4 and CT5.
Laboratory practical	In the lab, guided practices will be developed and practical case studies will be presented. This methodology will be used to work on competencies CB2, CB3, CG1, CG2, CE5, CE7, CE13 and CT5.

### Personalized assistance

Methodologies	Description
Lecturing	The teaching staff of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. The doubts will be answered in person or online (during the master's own session, or during the schedule established for the tutorials). The tutoring schedule will be established at the beginning of the course and will be published on the webpage of the subject.
Laboratory practical	The teachers of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. Likewise, the faculty will guide the students during the realization of the tasks assigned to them in the laboratory practices. The doubts will be answered in person (during the internships, or during the scheduled time for tutorials). The tutoring schedule will be established at the beginning of the course and will be published on the website of the subject.

### Assessment

	Description	Qualification	Evaluated Competences
Case studies	Exercises of practical cases on the risk analysis and the realization of security plans	30	CB2 CB3 CE5 CE7 CE13 CT5

Objective questions exam	Exam of theoretical knowledge and practical development	70	CG1 CG2 CE5 CE7 CE13 CT4 CT5
--------------------------	---	----	--

### Other comments on the Evaluation

Students can decide to be evaluated according to a continuous evaluation model or a single evaluation model. All students who submit the report of the first case study are opting for continuous assessment. Once the students choose the continuous assessment model, their grade can never be "Not Submitted".

The grade will be the result of applying the weighted average between results: (i) written exam (70%), and (ii) case studies (30%).

**Written exam:** will take place on the dates published in the official calendar.

#### Practical part:

1- Continuous evaluation model. A report 2 practical cases that will be delivered in the weeks indicated in the document that will be provided to the students on the first day of class. This is a group-based activity. All the students of the same group will receive the same mark.

2- Single evaluation model. Delivery of the the two case studies reports on the same date of the written exam published in the official calendar.

In the second-chance assessment, students will be evaluated using the single evaluation modality.

If plagiarism is detected in any of the assessment tests, the final grade of the subject will be "Suspense (0)", a fact that will be communicated to the school's management to adopt the appropriate measures.

### Sources of information

#### Basic Bibliography

Campbell, Tony, Practical Information Security Management: A Complete Guide to Planning and Implementation, Apress, 2016,

UNE-EN ISO, Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012)., AENOR, 2015,

UNE-EN ISO, Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices. (ISO 22313:2012)., AENOR, 2015,

UNE-EN ISO, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015), AENOR, 2017,

UNE-EN ISO, Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015)., AENOR, 2017,

ISO/IEC, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ISO/IEC 27000:2018), ISO/IEC, 2018,

ISO/IEC, Information technology -- Security techniques -- Information security management systems -- Guidance (ISO/IEC 27003:2017), ISO/IEC, 2017,

ISO/IEC, Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016), ISO/IEC, 2016,

ISO/IEC, Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005:2011), ISO/IEC, 2011,

#### Complementary Bibliography

Gómez Fernández, Luis y Fernández Rivero, Pedro Pablo, Como implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el ENS, AENOR, 2015,

Fernández Sánchez, Carlos Manuel y Piatini Velthuis, Mario, Modelo para el gobierno de las TIC basado en las normas ISO, AENOR, 2012,

ISO, Risk management -- Principles and guidelines (ISO/IEC 31000:2009), ISO, 2009,

Alan Calder Steve Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, 5, Kogan Page, 2012,

Alan Calder, Nine Steps to Success - North American edition: An ISO 27001:2013 Implementation Overview, 1, IT Governance Publishing, 2017,

Edward Humphreys, Implementing the ISO / IEC 27001 ISMS Standard, 2, Artech House, 2016,

### Recommendations

<b>IDENTIFYING DATA</b>				
<b>Information Security</b>				
Subject	Information Security			
Code	V05M175V01102			
Study programme	(*)Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Type	Year	Quadmester
	6	Mandatory	1st	1st
Teaching language	English			
Department				
Coordinator	Fernández Veiga, Manuel			
Lecturers	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
E-mail	mveiga@det.uvigo.es			
Web	<a href="http://fatic.uvigo.es">http://fatic.uvigo.es</a>			
General description	This course covers the fields of cryptography and cryptanalysis, generation of pseudorandom numbers and functions, message integrity, authenticated encryption, public key cryptography, privacy and anonymity in information systems, secure computations, steganography and watermarking.			

<b>Competencies</b>		
Code		Typology
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
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
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 • Know How
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
CE10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.	• know • Know How

<b>Learning outcomes</b>	
Learning outcomes	Competences
Understand the theoretical basis of encryption: Shannon ciphers, perfect security, semantic security, information-theoretic security	CE1 CE10
To know and be able to use stream ciphers	CE1 CE4 CE10
To know and be able to apply block ciphering tools, pseudorandom functions and the DES and AES ciphering standards	CE1 CE4 CE10
Knowledge about the construction, use and properties of hash functions, universal hashing and collision resistant hashing. Knowledge about message authentication codes. Case studies	CE1 CE4 CE10
Knowledge about public key cryptography and PK cryptographic schemes: RSA, ElGamal, Diffie-Hellman. Knowledge about digital signatures. Semantic security of public key cryptography	CE1 CE4 CE10
To know the basics of advanced cryptography: cryptography on elliptic curves. Lattice-based cryptography	CB2 CB5 CE1 CE4 CE10
To know and be able to use identification protocols, key interchange protocols and interactive communication protocols	CB5 CE1 CE4 CE10
To understand and have the ability to apply the basic techniques for steganography, watermarking and digital forensics	CB5 CE1 CE4 CE10

To know, understand and be able to use techniques for data anonymization	CB2 CB5 CE1 CE4 CE10
To know and understand the basic principles of distributed secure computation	CB2 CB5 CE1 CE4 CE10

## Contents

Topic	
1. Encryption	Shannon ciphers. Perfect security. Semantic security. Information-theoretic security: the wiretap channel
2. Stream ciphers	Pseudorandom generators. Composition of PRGs. Security. Attacks. Case studies
3. Block ciphers	Block ciphers. Security. DES & AES. Pseudorandom functions. Construction of PRFs and block ciphers
4. Message integrity	Authentication codes. Message integrity. Definition of security. Keyed MACs. PRFs and MAC. Hashing, hash functions. Universal hashing. Collision resistant hashing. Case studies
5. Authenticated encryption	Definition. Composition. Attacks, examples and case studies
6. Public key cryptography	Definition. Semantic security. One-way trapdoor functions. RSA, ElGamal, McEliece crypto systems. Diffie-Hellman key agreement. Digital signatures. Case studies
7. Advanced cryptography	Elliptic curve cryptography. Lattice-based cryptography. RLWE. Quantum-resistant cryptography. Homomorphic encryption
8. Identification protocols	Definitions. Passwords. Challenge-response. sigma-protocols. Okamoto and Schnorr protocols
9. Anonymization	Definitions. t-integrity and anonymity. Divergence. Analysis
10. Data hiding and steganography	Definitions. Spread-spectrum watermarking. Dirty paper coding. Digital forensics.
11. Secure computation	Computable functions. Fundamental limits. Two-way secure computation. Multiparty secure computation. Interactive communications. Homomorphic computations. Applications

## Planning

	Class hours	Hours outside the classroom	Total hours
Problem solving	0	24	24
Laboratory practical	18	36	54
Lecturing	17	51	68
Essay questions exam	2	0	2
Problem and/or exercise solving	1	0	1
Project	1	0	1

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

## Methodologies

	Description
Problem solving	Students are supposed to solve problems and exercises about the course contents. Written homework, with review and grading.  This methodology develops the competences CB2, CB4, CB5, CE1, CE44, CE10 and CT5.
Laboratory practical	Students are expected to work in the computer laboratory doing small programs on ciphering, and a programming assignment on ciphering, authentication, anonymity or digital forensics. The programming assignment will be supervised by the instructors.  This methodology develops the competences CB2, CB4, CB5, CE1, CE44, CE10 and CT4.
Lecturing	Lectures on the topics included in the course: definitions, concepts, main results, properties and applications.  This methodology develops the competences CB2, CB4, CB5, CE1, CE44, CE10 and CT5.

## Personalized assistance

Methodologies	Description
Lecturing	Individual office hours will be offered to the students who need guidance in the study, or further explanations on the course contents, clarification on the solutions to problems, etc.
Problem solving	Individual office hours will be offered to answer the questions about problems and exercises assigned to the students
Laboratory practical	Individual assistance will be given to the students who request guidance on the programming assignments or computer lab practice

<b>Assessment</b>			
	Description	Qualification	Evaluated Competences
Essay questions exam	Written exam. Questions, problems or exercises about the contents covered in the course	50	CB2 CB5 CE1 CE4 CE10
Problem and/or exercise solving	2-3 homework problem sets, to be worked out individually. Written submission	20	CB2 CB5 CE1 CE4 CE10
Project	Design and development of a programming assignment. Functional and performance tests will be run	30	CB2 CB5 CE1 CE4 CE10

### **Other comments on the Evaluation**

The student must choose between two alternative, mutually exclusive assessment method: continuous assessment or eventual assessment.

The continuous evaluation option consists in a final written exam (50% of the qualification), the completion of programming assignments (30% of the qualification) and homework (20%). These assignments will be due the last working day preceding the start of the examination period. The eventual assessment option consists in a final written exam (60% of the qualification) and in the completion of assignments (40% of the qualification). The assignments will be due the last working day preceding the start of the examination period. The examinations of the continuous and the eventual assessment options may not be equal.

The students can declare their preferred assessment type until the date of the written examination.

The students who fail the course will be given a second opportunity at the end of the academic year to do so. Their academic achievements will be re-evaluated, both with a written exam (theoretical knowledge) and a review of their engineering project looking for improvement or changes. The weights are the same they were committed to, according to their choice.

Any assigned grade will only be valid during the academic year where it is awarded.

### **Sources of information**

#### **Basic Bibliography**

D. Boneh, V. Shoup, A graduate course in applied cryptography, <http://toc.cryptobook.us>, 2018,

#### **Complementary Bibliography**

O. Goldreich, Foundation of cryptography, vol. I, Cambridge University Press, 2007,

O. Goldreich, Foundation of cryptography, vol. ii, Cambridge University Press, 2009,

J. Katz, Y. Lindell, Introduction to modern cryptography, 2, CRC Press, 2015,

A. Menezes, P. van Oorschot, S. Vanstone., Handbook of applied cryptography, CRC Press, 2001,

C. Dwork, A. Roth, The algorithmic foundations of differential privacy, NOW Publishers, 2014,

W. Mazurczyk, S. Wenzel, S. Zander, A. Houmansadr, K. Szczypiorski, Information hiding in communications networks: Fundamentals, mechanisms, applications, and countermeasures, Wiley, 2016,

I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kolker, Digital watermarking and steganography, 2, Morgan Kaufmann, 2008,

A. El-Gamal, Y. Kim, Network Information Theory, Cambridge University Press, 2011,



---

**Recommendations**

---

**Other comments**

---

The course is given in English. Ability for mathematical reasoning is highly recommended.

---

<b>IDENTIFYING DATA</b>				
<b>Secure Communications</b>				
Subject	Secure Communications			
Code	V05M175V01103			
Study programme	(*)Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Type	Year	Quadmester
	6	Mandatory	1st	1st
Teaching language	Spanish			
Department				
Coordinator	Rodríguez Rubio, Raúl Fernando			
Lecturers	Fernández Iglesias, Diego Rodríguez Pérez, Miguel Rodríguez Rubio, Raúl Fernando			
E-mail	rrubio@det.uvigo.es			
Web				
General description	This subject reviews the layers of the Internet communications architecture, showing its main weaknesses from a security point of view and providing the necessary techniques and tools to mitigate them. Students will acquire a detailed understanding of the network protocols that provide security for the transmission of information, and the implications derived from the place they occupy within the networking architecture.			

<b>Competencies</b>		Typology
Code		
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.	
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.	
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.	
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	
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.	
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.	
CE8	Skills for conceive, design, deploy and operate cybersecurity systems.	
CT4	Ability to ponder the importance of information security in the economic progress of society.	
CT5	Ability for oral and written communication in English.	

<b>Learning outcomes</b>		Competences
Learning outcomes		
To know in depth the network protocols that provide security to the transmission of information, and the implications derived from the place they occupy within the networking architecture		CB5 CG1 CE1 CT4 CT5
To understand that other protocols, being auxiliary (not related to the world of security), present exploitable vulnerabilities; and will be able to describe the most common attacks that try to take advantage of them, and some possible countermeasures		CB5 CE4 CT4 CT5

Knowing which solution / protocol is appropriate to ensure a specific scene	CB5 CG1 CG3 CG5 CE1 CE2 CE4 CT4 CT5
To know the solutions providing security to certain network services and/or universally used applications	CB5 CE2 CE8 CT4 CT5
To be able to configure the tools (software packages) that the different operating systems / platforms provide to secure communications.	CB2 CB5 CG5 CT4 CT5
To acquire the ability to write technical reports justifying the suitability of a cybersecurity solution for a given problem or scene	CB4 CG1 CG3

## Contents

Topic	
Internet architecture and protocols	Fundamental concepts
Link level security	Wired security/Ethernet networks: Access control and port-based authentication Confidentiality in Ethernet networks  Wireless Security/WiFi networks: IEEE 802.11i IEEE 802.11w Passpoint / HotSpot2.0
Network level security	IPsec security protocols IPsec dynamic key management IPsec authentication mechanisms IPsec and NAT
Securing Internet infrastructure	Routing protocols security DNS security TCP security
Data transmission security	The TLS protocol Cryptographic suites WebPKI infrastructure Certificate validation HTTP Public Key Pinning
Mobile networks security	LTE system architecture Association and authentication of the user/terminal Privacy

## Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	21	21	42
Laboratory practical	19	19	38
Autonomous practices through ICT	0	58	58
Essay questions exam	2	0	2
Practices report	0	10	10

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

## Methodologies

	Description
Lecturing	Master sessions follow the usual scheme for this type of teaching. In these sessions the CG3, CE1, CE2, CE4, CE8 competences are worked out

Laboratory practical	There will be several practical sessions guided by the teachers where the concepts learned in the theoretical classes will get entrenched. Such practices, will use network devices (routers and switches) and / or virtualization software that will allow students to learn and practice at home. The practices to be considered will be sized to be approachable during their respective classroom sessions; although any student that needs so will be able to reproduce them at home with free virtualization software that will allow them to virtualize the behaviour of the network hardware used in the laboratory. Optional exercises may also be proposed, which students can do during non-attendance hours, and may review individually during office hours. Students will acquire competencies CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
Autonomous practices through ICT	Beyond the guided practices, the student will have to deploy / configure / implement some specific solutions, for certain scenarios, in an autonomous way. In these activities CB2, CB4, CB5, CG1, CG3, CG5, CE1, CE4, CE8 are worked out.

### Personalized assistance

Methodologies	Description
Lecturing	During the office hours teachers will provide personalized attention to strengthen or guide students in the understanding of the theoretical concepts explained in the lectures or practical demonstration sessions; and to correct or reorient the small optional practical works derived from said laboratory classes.
Laboratory practical	This activity is interactive by definition, so it is expected that questions will flow naturally between teachers and students, and may involve other students in the answers.
Autonomous practices through ICT	Although the autonomous work is targeted to make students solve situations / challenges to be found in real systems on their own, during office hours, teachers will guide them by questioning the chosen solutions or suggesting alternative paths.

### Assessment

	Description	Qualification	Evaluated Competences
Laboratory practical	They will be qualified as apt / unfit. Students will pass them if they attend all sessions of this type. If for some reason they miss any, they must do some complementary practical that teachers will establish. In some of the sessions / activities the student may be asked for an additional autonomous work (and its associated report) that will be quantitatively evaluated within the more general element called "Autonomous practices through ICT".	0	CB2 CB4 CB5 CG5 CE4 CE8 CT4 CT5
Autonomous practices through ICT	Students must perform, in presence of the teachers, a practical demonstration showing the resolution of the different technical challenges posed, and face questions about the adopted solutions and their degree of completeness. This defense/interview will take place, in a general way, after the delivery deadline of the last ordered task, and before the beginning of the official exams period in the corresponding call, and its definite date will be agreed on time between students and teachers.  Every challenge or autonomous activity will require a written report, whose structure, composition and readability will affect final mark.	40	CB2 CB4 CB5 CG5 CE1 CE4 CE8 CT4 CT5
Practices report	The student's autonomous work should be reported appropriately with pertinent docs whose evaluation will be part of the more general evaluation of the documented task.	0	CB4 CG1 CG3 CT4 CT5
Essay questions exam	A written exam will be carried out at the end of the semester, where the theoretical concepts taught in the lectures are evaluated, as well as the practical foundations derived from the classes / practical work carried out.	60	CB4 CE1 CE2 CE4 CT4

### Other comments on the Evaluation

The evaluation of the subject can either follow a continuous assessment strategy (EC) or a single assessment one (EU). The students choose EC if they deliver the solution to the first challenge or autonomous work that they must attend during the course. The percentages expressed in the previous section only reflect the maximum mark obtainable in each type of test in the EC modality; and they are only indicative. The detailed evaluation form is expressed below:

For EC (first call), the final grade will be the weighted geometric mean between the autonomous work grade (TA, 40%) and the corresponding grade for the essay questions exam (E, 60%). The grade of TA will be the arithmetic mean of the marks obtained in each of the challenges / autonomous practical that students have to solve during the semester.

$$\text{FINAL GRADE (EC)} = (\text{TA} \wedge 0.4) \times (\text{E} \wedge 0.6)$$

If the laboratory practices assessment is unfit, the grade will be the minimum between the written test score (E) and 3.

Students who choose EU must take a final exam consisting of three parts: a written test analogous to the continuous assessment test (E), a proficiency test in the laboratory and one or more practical tasks (T). The final grade, in this case, is the weighted geometric mean between the theory grade (E, 80%) and practical work (T, 20%), with the condition that the aptitude test is passed. For any student that fails the aptitude test, the final grade will be the minimum between E and 3.

$$\text{FINAL GRADE (EU)} = (\text{T} \wedge 0.2) \times (\text{E} \wedge 0.8)$$

Finally, for the second call (June / July), students will be able to continue with the evaluation mode that they had already chosen (keeping the mark of the part -E or TA / T- that they had passed), facing only the failed part - though with possible modifications in the specifications of the practical works; or they may choose to follow EU doing just a final exam as the one just described. The aptitude test will only be necessary if they did not attend all laboratory sessions.

---

## Sources of information

### Basic Bibliography

I. Ristic, Bulletproof SSL and TLS, ser. Computers/Security, London: Fesity Duck, 2015,

A. Liska and G. Stowe, DNS Security: Defending the Domain Name System, Boston: Syngress, 2016,

Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya, RADIUS / AAA / 802.1x, RA-MA Editorial, 2008,

Graham Bartlett, Amjad Inamdar, IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS, CISCO PRESS, 2016,

### Complementary Bibliography

D. J. D. Touch, Defending TCP Against Spoofing Attacks, IETF, 2007, RFC 4953

R. R. Stewart, M. Dalal, and A. Ramaiah, Improving TCP's Robustness to Blind In-Window Attacks, IETF, 2010, RFC 5961

D. J. Bernstein, SYN cookies, <https://cr.yp.to/syncookies.html>

P. McManus, Improving syncookies, 2008, <https://lwn.net/Articles/277146/>

C. Pignataro, P. Savola, D. Meyer, V. Gill, and J. Heasley, The Generalized TTL Security Mechanism (GTSM), IETF, 2007, RFC 5082

D. J. D. Touch, R. Bonica, and A. J. Mankin, The TCP Authentication Option, IETF, 2010, RFC 5925

S. Rose, M. Larson, D. Massey, R. Austein, and R. Arends, DNS Security Introduction and Requirements, IETF, 2005, RFC 4033

R. Arends, R. Austin, M. Larson, D. Massey, S. Rose, Resource Records for the DNS Security Extensions, IETF, 2005, RFC 4034

R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, Protocol Modifications for the DNS Security Extensions, IETF, 2005, RFC 4035

Cloudflare Inc., How DNSSEC works, <https://www.cloudflare.com/dns/dnssec/how-dnssec-works/>

P. E. Hoffman and P. McManus, DNS Queries over HTTPS (DOH), IETF, 2018,

<https://datatracker.ietf.org/doc/html/draft-ietf-doh-dns-over-https-09>

E. Jones and O. L. Moigne, OSPF security vulnerabilities analysis, IETF, 2006, <https://datatracker.ietf.org/doc/html/draft-ietf-rpsec-ospf-vuln-02>

M. Khandelwal and R. Desetti, OSPF security: Attacks and defenses, 2016,

[https://www.sanog.org/resources/sanog28/SANOG28-Tutorial\\_OSPF-Security-Attacks-and-Defences-Manjul.pdf](https://www.sanog.org/resources/sanog28/SANOG28-Tutorial_OSPF-Security-Attacks-and-Defences-Manjul.pdf)

J. Durand, I. Pepelnjak, and G. Doering, BGP operations and security, IETF, 2015, RFC 7454

R. Kuhn, K. Sriram, and D. Montgomery, Border gateway protocol security, NIST, 2007,

C. Pelsser, R. Bush, K. Patel, P. Mohapatra, and O. Maennel, Making route flap damping usable, IETF, 2014, RFC 7196

Y. Rekhter, J. Scudder, S. S. Ramachandra, E. Chen, and R. Fernando, Graceful restart mechanism for BGP, IETF, 2007, RFC 4724

IEEE 802.1 Working Group, IEEE Std 802.1X - 2010. Port-Based Network Access Control, IEEE Computer Society, 2010,

Security Task group of IEEE 802.1, IEEE Std 802.1AE. Medium Access Control Security, IEEE Computer Society, 2018,

S. Kent, K. Seo, Security Architecture for the Internet Protocol, IETF, 2005, RFC 4301

S. Kent, IP Authentication Header, IETF, 2005, RFC 4302

S. Kent, IP Encapsulating Security Payload, IETF, 2005, RFC 4303

C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, Internet Key Exchange Protocol Version 2 (IKEv2), IETF, 2014, RFC 7296

J. Cichonski, J. M. Franklin, M. Bartock, Guide to LTE Security, NIST Special Publication 800-187,

<https://doi.org/10.6028/NIST.SP.800-187>

---

## Recommendations

<b>IDENTIFYING DATA</b>			
<b>Applications Security</b>			
Subject	Applications Security		
Code	V05M175V01104		
Study programme	(*)Máster Universitario en Ciberseguridade		
Descriptors	ECTS Credits	Type	Year
	6	Mandatory	1st
Teaching language	Spanish		
Department			
Coordinator	López Nores, Martín Bellas Permuy, Fernando		
Lecturers	Bellas Permuy, Fernando López Nores, Martín Losada Pérez, José		
E-mail	mlnores@det.uvigo.es fbellas@udc.es		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530005&amp;any_academic=2018_19&amp;idioma_assig=cast">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530005&amp;any_academic=2018_19&amp;idioma_assig=cast</a>		
General description	Developing secure applications is not an easy task. Knowledge of the vulnerabilities that usually affect applications, the techniques of authentication, authorization and access control, as well as the incorporation of security into the development life cycle, is essential to be able to build and maintain applications successfully. In this course, all these aspects are studied in a practical way, with special emphasis on the development of web applications and services.		

<b>Competencies</b>	
Code	Typology

<b>Learning outcomes</b>	
Learning outcomes	Competences

<b>Contents</b>	
Topic	

<b>Planning</b>			
	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

<b>Methodologies</b>	
	Description

<b>Personalized assistance</b>	

<b>Assessment</b>		
Description	Qualification	Evaluated Competences

<b>Other comments on the Evaluation</b>	

<b>Sources of information</b>	
<b>Basic Bibliography</b>	
<b>Complementary Bibliography</b>	

<b>Recommendations</b>	

<b>IDENTIFYING DATA</b>			
<b>Secure Networks</b>			
Subject	Secure Networks		
Code	V05M175V01105		
Study programme	(*)Máster Universitario en Ciberseguridade		
Descriptors	ECTS Credits	Type	Year
	6	Mandatory	1st
Teaching language	Spanish		
Department			
Coordinator	Rodríguez Pérez, Miguel Nóvoa de Manuel, Francisco Javier		
Lecturers	Nóvoa de Manuel, Francisco Javier Rodríguez Pérez, Miguel Rodríguez Rubio, Raúl Fernando		
E-mail	fjnovoa@udc.es miguel@det.uvigo.gal		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530006&amp;any_academic=2018_19&amp;idioma_assig=cast">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530006&amp;any_academic=2018_19&amp;idioma_assig=cast</a>		
General description	(*)A materia Redes Seguras ten como obxectivo principal que os estudantes aprendan a deseñar e implementar infraestruturas de rede capaces de proporcionarlos servizos de seguridade precisos nun contorno corporativo moderno. Deberán coñecer as arquitecturas de seguridade de referencia e seren quen de configuralas en mantelas, utilizando para iso tecnoloxías como VPN, IDS/IPS e Firewalls entre outros. A materia esta concebida para que as prácticas de laboratorio, con equipos físicos e virtuais teñan unha importancia capital no proceso de aprendizaxe		

<b>Competencies</b>	
Code	Typology

<b>Learning outcomes</b>	
Learning outcomes	Competences

<b>Contents</b>	
Topic	

<b>Planning</b>			
	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

<b>Methodologies</b>	
	Description

<b>Personalized assistance</b>	

<b>Assessment</b>		
Description	Qualification	Evaluated Competences

<b>Other comments on the Evaluation</b>	

<b>Sources of information</b>	
<b>Basic Bibliography</b>	
<b>Complementary Bibliography</b>	

<b>Recommendations</b>	

<b>IDENTIFYING DATA</b>				
<b>Principles and Law in Cybersecurity</b>				
Subject	Principles and Law in Cybersecurity			
Code	V05M175V01201			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Type	Year	Quadmester
	3	Mandatory	1st	2nd
Teaching language	Spanish Galician English			
Department				
Coordinator	Rodríguez Vázquez, Virgilio			
Lecturers	Faraldo Cabana, Patricia Rodríguez Vázquez, Virgilio			
E-mail	virxilio@uvigo.es			
Web				
General description	This subject will address the rules relating to cybersecurity. A criminological study of the main computing crimes will be carried out. The central block consists of a systematic review of the regulation of the computing crimes contained in the Spanish Criminal Code. Analysis will also be made of the case law existing in this subject.			

<b>Competencies</b>		Typology
Code		
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 • Know How
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
CE8	Skills for conceive, design, deploy and operate cybersecurity systems.	• know • Know How • 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 How • Know be
CT5	Ability for oral and written communication in English.	• Know How

<b>Learning outcomes</b>		Competences
Learning outcomes		
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.		CB3
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.		CE3
Skills for conceive, design, deploy and operate cybersecurity systems.		CE8
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.		CT1
Ability for oral and written communication in English.		CT5

<b>Contents</b>	
Topic	
1. Introduction to the law on cybersecurity. Review of the rules on computer and risk management.	1.1. EU regulations. 1.2. The Law of National Security: the strategy of national security and the diagram of national security. 1.3. Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation. The Organic Law of Data Protection and the developmental Regulation. 1.4. Computing crimes in the Criminal Code.
2. Criminological approach to computing.	2.1. Statistical sources: main national and international organisms, crimes. 2.2. Analysis of the main reports on cybersecurity. 2.3. Identification of the main technological resources used.



3. Cybersecurity breaches through criminal conduct.	<p>3.1. Definition: computing crimes and cybercrime.</p> <p>3.2. The use of ICT to commit crimes and when ICT is the goal of the crime.</p> <p>3.3. The Spanish Criminal Code, LO 10/1995, of 23 November, European Directive 2013/40/UE of the European Parliament and of the Council, of 12 August 2013, on attacks against information systems, Agreement on cybersecurity or Agreement of Budapest, of the Council of Europe, of 23 November 2001.</p>
4. The main crimes that affect cybersecurity.	<p>4.1. Crimes of discovering and disclosing secrets (I). Frequent risks: ransomware and the theft of information.</p> <p>4.2. Crimes of discovering and disclosing secrets (II). Access and interception. The access to files or computer, electronic or telematic media. Special attention to the manager of the files or media. The interception of transmissions of computing data. The use of malware (virus, spyware...).</p> <p>4.3. Crimes of discovering and disclosing of secrets (III). Producing, purchasing, importing or facilitating programs to commit the crimes listed above, or computer passwords or access codes.</p> <p>4.4. Crimes against privacy and an individual's right to their own image: the undue use of cookies.</p> <p>4.5. Crimes against property (I). Scams committed via computer. Producing, possessing or facilitating computer programs used for this purpose.</p> <p>4.6. Crimes against property (II). Fraud using a third-party telecommunication signal. Use of telecommunication terminal without the owner's consent.</p> <p>4.7. Crimes against property (III). Damages to computing data, computing programs or electronic documents. Damages to computing systems. Damages to computing systems of a critical infrastructure (brief reference to the operators of critical infrastructure, to the operator's security plans and to the of specific protection plans). Hindering or interrupting the functioning of a third-party computing system. Manufacturing, possessing or facilitating to third parties computing programs to be used for this purpose. Special reference to the criminal liability of legal persons.</p> <p>4.8. Crimes against intellectual and industrial property. Through the provision of information society services or through an Internet access portal.</p> <p>4.9. Crimes relating to the market and to consumers. Discovering company secrets through the use of ICT. Intelligible access to a radio or television broadcast, to remote interactive services via electronic channels.</p> <p>4.10. Crimes against public faith: electronic lies.</p>
5. Crimes committed against persons using communication techniques.	<p>5.1. Crimes against freedom. Threats using social networks or other ICT. Cyber stalking.</p> <p>5.2. Crimes against the sexual freedom and indemnity. Child grooming and child pornography.</p> <p>5.3. Crimes against intimacy and privacy.</p> <p>5.4. Crimes against honour. Harming a person's digital reputation.</p>
6. Cyberterrorism.	<p>6.1. Concept.</p> <p>6.2. Computing crimes carried out with the specific purpose of art. 573 of the Criminal Code.</p> <p>6.3. Crime of collaborating with a terrorist group or organisation through the provision of technological services.</p>
7. Crimes relating to national Defence and others.	Brief approximation.
8. Analysis of Spanish caselaw in relation to computing crimes.	<p>8.1. Special attention to the caselaw of the Supreme court.</p> <p>8.2. Agreements of the non-jurisdictional plenary of the Second Chamber of the Supreme Court relating to computing crimes.</p> <p>8.3. The Prosecution Service and the Prosecutor's Office specialising in computer criminality.</p>

## Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	13	32	45
Laboratory practical	5	22	27
Objective questions exam	2	0	2
Problem and/or exercise solving	1	0	1

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

<b>Methodologies</b>	
	Description
Lecturing	Presentation by the teacher of the contents of the subject under study, theoretical and / or guidelines for the work, exercise or project to be developed by the student.
Laboratory practical	Activities to apply knowledge to specific situations and basic skills acquisition and procedures related to the matter to be studied. Special areas are developed with specialized equipment (scientific and technical laboratories, computer rooms, etc.).

<b>Personalized assistance</b>	
Methodologies	Description
Lecturing	The students will have lectures as shown on the timetable published on the website for the Master's Degree.
Laboratory practical	The students will have practical classes as shown on the timetable published on the website for the Master's Degree.

<b>Assessment</b>			
	Description	Qualification	Evaluated Competences
Objective questions exam	<p>The continuous assessment system will consist of three written examinations first two will focus on partial objective tests (objective questions exam, multiple choice, referred to in this part of the Guide), and the third, will focus on "problem solving" (referred to in the following part of the guide).</p> <p>The multiple choice "objective questions" exam:</p> <ul style="list-style-type: none"> <li>- will be held throughout the course, during the lecture timetable.. The timetable for the different intermediate assessment tests will be approved by the Comisión Académica de Máster Interuniversitario (CAMI) and will be available at the beginning of each academic term.</li> <li>- each examination will comprise the part of the program that is indicated at the start of the term by the subject coordinator.</li> <li>- they will consist of a multiple choice test, with 0 to 2.5 points for each of them. Correct answers will be worth 0.1 and 0.05 will be deducted for each incorrect answer. Answers left blank will not score anything.</li> <li>- Both exams together will be worth 50% of the final mark, with the remaining 50% corresponding to the "problem solving" (described in the following section).</li> </ul> <p>To pass the subject under the continuous assessment system the mark from the three exams, based on the weighting above, needs to be equal to or greater than 5. Those who attend the first partial test (the first multiple choice objective questions exam), thereby expressing their interest in being included in the continuous assessment system, will be assessed according to the criteria stated above and will not be entitled to be assessed by the final exam system that corresponds to 100% of the marks for the subject. Therefore, if a student takes the first partial exam, it is not possible to abandon the continuous assessment system. If a student takes the first partial exam and then does not take the next partial exam(s), they will score 0 points for this/these exam(s).</p>	50	CB3 CE3 CE8 CT1

Problem and/or exercise solving	<p>The continuous assessment system will consist of three written examinations: the first two will focus on partial objective tests (objective questions exam, multiple choice, referred to in the previous part of the guide exercise, and the third will focus on "problem solving" (referred to in this part of the guide).</p> <p>The examination corresponds to "problem solving":</p> <ul style="list-style-type: none"> <li>- it will be held on the official date of the ordinary announcement of the final exam: first opportunity, according to the official schedule approved by the Academic Commission of the Master's Degree for the 2019-2020 academic year</li> <li>- It will consist of solving one or several practical cases and will be marked with a score of 0 to 5 points</li> <li>- The problems posed by the practical cases may affect the issues covered in the course syllabus.</li> <li>- It will be worth 50% of the final mark, with the remaining 50% corresponding to the two multiple choice objective questions exams.</li> </ul> <p>To pass the subject under the continuous assessment system, the mark from the three exams, based on the weighting above, needs to be equal to or greater than 5. Those who attend the first partial test (the first multiple choice objective questions exam), thereby expressing their interest in being included in the continuous assessment system, will be assessed according to the criteria stated above and will not be entitled to be assessed by the final exam system that corresponds to 100% of the marks for the subject. Therefore, if a student takes the first partial exam, it is not possible to abandon the continuous assessment system. If a student takes the first partial exam and then does not take the next partial exam(s), they will score 0 points for this/these exam(s).</p>	50	CB3 CE3 CE8 CT1 CT5
---------------------------------	---	----	---------------------------------

---

### Other comments on the Evaluation

---

#### 1. FIRST OPPORTUNITY

a) **CONTINUOUS ASSESSMENT SYSTEM** described in the sections above.

b) **FINAL EXAM SYSTEM**

For those who do not choose the continuous assessment system, the subject assessment will consist of a single final exam, on the date established in the official schedule approved by the Academic Commission of the Master's Degree for the 2019-2020 academic year.

The exam will cover the whole syllabus and will be worth 100% of the mark for the subject. It will consist of two parts, a theory part and a practical part, which will both be worth 0 to 5 points each. The theory part will consist of a multiple choice test, in which correct answers will be worth twice as much as the points deducted for incorrect answers. Any answers left blank will not score anything. The practical part will consist of solving one or several practical cases. The final mark for the exam will be obtained by adding together the marks obtained in each of the parts. To pass the subject students must obtain a minimum of 5 points after adding the marks from both parts together.

#### 2. SECOND OPPORTUNITY AND EXTRAORDINARY EXAM

The subject assessment will consist of a single final exam, on the date established in the official schedule approved by the Academic Commission of the Master's Degree for the 2019-2020 academic year.

The exam will cover the whole syllabus and will be worth 100% of the mark for the subject. It will consist of two parts, a theory part and a practical part, which will both be worth 0 to 5 points each. The theory part will consist of a multiple choice test, in which correct answers will be worth twice as much as the points deducted for incorrect answers. Any answers left blank will not score anything. The practical part will consist of solving one or several practical cases. The final mark for the exam will be obtained by adding together the marks obtained in each of the parts. To pass the subject students must obtain a minimum of 5 points after adding the marks from both parts together.

---

### Sources of information

#### Basic Bibliography

DE LA CUESTA ARZAMANDI, José Luis (dir.), Derecho penal informático, 1.ª, Civitas, 2010, Madrid

LUZÓN PEÑA, Diego-Manuel (dir.), Código Penal, 5.ª, Reus, 2017, Madrid

#### Complementary Bibliography

BARONA VILAR, Silvia, Justicia civil y penal en la era global, 1.ª, Tirant lo Blanch, 2017, Valencia

BARRIO ANDRÉS, Moisés, Cibercriminología : amenazas criminales del ciberespacio : adaptado reforma Código Penal 2015, 1.ª, Reus, 2017, Madrid

CRESPO SANCHÍS, Carolina (coord.), Fraude electrónico : panorámica actual y medios jurídicos para combatirlo, 1.ª, Civitas, 2013, Madrid

CRUZ DE PABLO, José Antonio, Derecho penal y nuevas tecnologías : aspectos sustantivos : adaptado a la reforma operada en el Código penal por la Ley orgánica 15-2003 de 25 de noviembre, especial referencia al artículo 286 CP, 1.ª, Difusión Jurídica y Temas de actualidad, 2006, Madrid

CUERDA ARNAU, María Luisa (coord.), Menores y redes sociales : cyberbullying, cyberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia en la red, 1.ª, Tirant lo Blanch, 2016, Valencia

DAVARA RODRÍGUEZ, Miguel Ángel, Manual de derecho informático, 11.ª, Thomson-Aranzadi, 2015, Cizur Menor (Navarra)

DE NOVA LABIÁN, Alberto José, Delitos contra la propiedad intelectual en el ámbito de Internet : especial referencia a los sistemas de intercambio de archivos, 1.ª, Dykinson, 2010, Madrid

DE URBANO CASTRILLO, Eduardo et al., Delincuencia informática : tiempos de cautela y amparo, 1.ª, Aranzadi, 2012, Cizur Menor (Navarra)

FARALDO CABANA, Patricia, Las Nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, 1.ª, Tirant lo Blanch, 2009, Valencia

FERNÁNDEZ TERUELO, Javier Gustavo, Cibercrimen, los delitos cometidos a través de Internet : estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y ot, 1.ª, Constitutio Criminalis Carolina, 2017, Madrid

FLORES PRADA, Ignacio, Criminalidad informática : (aspectos sustantivos y procesales), 1.ª, Tirant lo Blanch, 2012, Valencia

GALÁN MUÑOZ, Alfonso, El Fraude y la estafa mediante sistemas informáticos : análisis del artículo 248.2 C.P, 1.ª, Tirant lo Blanch, 2005, Valencia

GIANT, Nikki, Ciberseguridad para la i-generación : usos y riesgos de las redes sociales y sus aplicaciones, 1.ª, Narcea, 2016, Madrid

GÓMEZ RIVERO, M.ª del Carmen (dir.), Nociones fundamentales de Derecho penal. Parte especial. Volumen I, 2.ª, Tecnos, 2015, Madrid

GÓMEZ RIVERO, M.ª del Carmen (dir.), Nociones fundamentales de Derecho penal. Parte especial. Volumen II, 2.ª, Tecnos, 2015, Madrid

GÓMEZ TOMILLO, Manuel, Responsabilidad penal y civil por delitos cometidos a través de Internet : especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces, 2.ª, Thomson-Aranzadi, 2006, Cizur Menor (Navarra)

GONZÁLEZ CUSSAC, José Luis (coord.), Derecho penal. Parte especial, 5.ª, Tirant lo Blanch, 2016, Valencia

GONZÁLEZ CUSSAC, José Luis/CUERDA ARNAU, M.ª Luisa (dirs.), Nuevas amenazas a la seguridad nacional : terrorismo, criminalidad organizada y tecnologías de la información y la comunicación, 1.ª, Tirant lo Blanch, 2013, Valencia

GOODMAN, Marc, Future crimes : inside the digital underground and the battle for our connected world, 1.ª, Pegasus Books, 2016, New York

HILGENDORF, Eric, Computer- und Internetstrafrecht : ein Grundriss, 1.ª, Springer, 2005, Berlin

Instituto Español de Estudios Estratégicos, Grupo de Trabajo número 03/10, Ciberseguridad : retos y amenazas a la seguridad nacional en el ciberespacio, 1.ª, Ministerio de Defensa, Dirección General de Relaci, 2011, Madrid

LUZÓN PEÑA, Diego-Manuel, Lecciones de Derecho penal. Parte general, 3.ª, Tirant lo Blanch, 2016, Valencia

MARZILLI, Alan, The Internet and crime, 1.ª, Chelsea House, 2010, New York

MATA Y MARTÍN, Ricardo M., Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago : el uso fraudulento de tarjetas y otros instrumentos de pago, 1.ª, Thomson-Aranzadi, 2007, Thomson-Aranzadi,

MORÓN LERMA, Esther, Internet y derecho penal : "hacking" y otras conductas ilícitas en la red, 2.ª, Aranzadi, 2002, Cizur Menor (Navarra)

MUÑOZ CONDE, Francisco/GARCÍA ARÁN, Mercedes, Derecho penal. Parte general, 9.ª, Tirant lo Blanch, 2015, Valencia

ORENES, Eduardo, Ciberseguridad familiar : cyberbullying, hacking y otros peligros en Internet, 1.ª, Círculo Rojo, 2013, El Ejido (Almería)

ORTS BERENQUER, Enrique/ROIG TORRES, Margarita, Delitos informáticos y delitos comunes cometidos a través de la informática, 1.ª, Tirant lo Blanch, 2001, Valencia

QUERALT JIMÉNEZ, Joan Josep, Derecho penal español. Parte especial, 7.ª, Tirant lo Blanch, 2015, Valencia

QUINTERO OLIVARES, Gonzalo (dir.), Comentarios a la Parte especial del Derecho penal, 10.ª, Aranzadi, 2016, Cizur Menor (Navarra)

RALLO LOMBARTE, Artemi, El derecho al olvido en Internet : Google, 1.ª, Centro de Estudios Políticos y Constitucionales, 2014, Madrid

RODRÍGUEZ MESA, M.ª José, Los delitos de daños, 1.ª, Tirant lo Blanch, 2017, Valencia

ROMEO CASABONA, Carlos M.ª (coord.), El Cibercrimen : nuevos retos jurídico-penales, nuevas respuestas político-criminales, 1.ª, Comares, 2006, Granada

RUEDA MARTÍN, M.ª Ángeles, Protección penal de la intimidad personal e informática : (los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal), 1.ª, Atelier, 2004, Barcelona

SAIN, Gustavo, Delitos informáticos : investigación criminal, marco legal y peritaje, 1.ª, B de f, 2017, Montevideo

SÁINZ PEÑA, Rosa M.ª (coord.), Ciberseguridad, la protección de la información en un mundo digital, 1.ª, Fundación Telefónica, Ariel, 2016, Madrid, Barcelona

SEGURA SERRANO, Antonio/GORDO GARCÍA, Fernando (coords.), Ciberseguridad global : oportunidades y compromisos en el uso del ciberespacio, 1.ª, Universidad de Granada, 2013, Granada

SILVA SÁNCHEZ, Jesús María (dir.)/RAGUÉS I VALLÉS, Ramón (coord.), Lecciones de Derecho penal: Parte especial, 5.ª, Atelier, 2018, Barcelona

SINGER, Peter Warren, Cybersecurity and cyberwar : what everyone needs to know, 1.ª, Oxford University Press, 2014, Oxford

TOURIÑO, Alejandro, El derecho al olvido y a la intimidad en Internet, 1.ª, Los Libros de la Catarata, 2014, Madrid

VALLS PRIETO, Javier, Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial, 1.ª, Dykinson, 2017, Madrid

VELASCO NÚÑEZ, Eloy (dir.), Delitos contra y a través de las nuevas tecnologías : ¿cómo reducir su impunidad?, 1.ª, Consejo General del Poder Judicial, Centro de Docu, 2006, Madrid

VELASCOS SAN MARTÍN, Cristos, La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet, 1.ª, Tirant lo Blanch, 2012, Valencia

WALDEN, Ian, Computer crimes and digital investigations, 1.ª, Oxford University Press, 2007, Oxford

---

## **Recommendations**

---

### **Subjects that it is recommended to have taken before**

---

Management of Information Security/V05M175V01101

---

**IDENTIFYING DATA****Hardening of Operating Systems**

Subject	Hardening of Operating Systems		
Code	V05M175V01202		
Study programme	(*)Máster Universitario en Ciberseguridade		
Descriptors	ECTS Credits	Type	Year
	5	Mandatory	1st
Teaching language	Spanish		
Department			
Coordinator	Lorenzo Veiga, Beatriz Yáñez Izquierdo, Antonio Fermín		
Lecturers	Lorenzo Veiga, Beatriz Yáñez Izquierdo, Antonio Fermín		
E-mail	antonio.yanez@udc.es b.lorenzo.es@ieee.org		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530007&amp;any_academic=2018_19&amp;idioma_assig=eng">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530007&amp;any_academic=2018_19&amp;idioma_assig=eng</a>		
General description	A newly installed Operating system is inherently insecure. It has a certain number of vulnerabilities, depending on such things such as the age of the O.S., the amount of services it provides, the existence of initial backdoors not already patched, and the use of default policies designed without security in mind. By Hardening Operating Systems we refer to the act of configuring an operating system with the aim of making it as secure as possible, so that we minimize the risk of getting it compromised. This usually implies applying patches, changing default O.S. policies, and removing (or disabling) non-essential applications and/or services. In this course we'll try to identify common O.S. vulnerabilities and how to defend the O.S. against them. Both UNIX (linux) and Windows type O.S. will be considered.		

**Competencies**

Code	Typology
------	----------

**Learning outcomes**

Learning outcomes	Competences
-------------------	-------------

**Contents**

Topic
-------

**Planning**

	Class hours	Hours outside the classroom	Total hours
--	-------------	-----------------------------	-------------

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

**Methodologies**

Description
-------------

**Personalized assistance****Assessment**

Description	Qualification	Evaluated Competences
-------------	---------------	-----------------------

**Other comments on the Evaluation****Sources of information****Basic Bibliography****Complementary Bibliography****Recommendations**

**IDENTIFYING DATA****Intrusion tests**

Subject	Intrusion tests			
Code	V05M175V01203			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Type	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Costa Montenegro, Enrique Carballal Mato, Adrián			
Lecturers	Carballal Mato, Adrián Costa Montenegro, Enrique			
E-mail	adrian.carballal@udc.es kike@gti.uvigo.es			
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530008&amp;any_academic=2018_19&amp;idioma_assig=cast">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530008&amp;any_academic=2018_19&amp;idioma_assig=cast</a>			
General description	No hay una mejor forma de probar la fortaleza de un sistema que atacarlo. Los Test de Intrusión sirven para reproducir intentos de acceso de un atacante valiéndose de las vulnerabilidades que puedan existir en una determinada infraestructura. En este curso se cubrirán los temas fundamentales orientados a los test de intrusión (pentesting) cubriendo las distintas fases de un ataque y explotación (desde el reconocimiento y el control de acceso hasta el borrado de huellas)			

**Competencies**

Code	Typology
------	----------

**Learning outcomes**

Learning outcomes	Competences
-------------------	-------------

**Contents**

Topic
-------

**Planning**

	Class hours	Hours outside the classroom	Total hours
--	-------------	-----------------------------	-------------

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

**Methodologies**

Description
-------------

**Personalized assistance****Assessment**

Description	Qualification	Evaluated Competences
-------------	---------------	-----------------------

**Other comments on the Evaluation****Sources of information****Basic Bibliography****Complementary Bibliography****Recommendations**

**IDENTIFYING DATA****Malware Analysis**

Subject	Malware Analysis			
Code	V05M175V01204			
Study programme	(*)Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Type	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	English			
Department				
Coordinator	Burguillo Rial, Juan Carlos			
Lecturers	Burguillo Rial, Juan Carlos			
E-mail	jrial@uvigo.es			
Web	http://http://faiitc.uvigo.es			
General description	Malware uses the systems and the communication networks to disseminate virus, hijack devices or steal confidential data. The aim of this subject is to provide the student the capability to analyze, detect and erase malware. To achieve that, we will explore and evaluate, practically and with case studies, the techniques used nowadays to hide malware, together with the new tendencies to detect it and eliminate it.			

**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
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 How
CE8	Skills for conceive, design, deploy and operate cybersecurity systems.	• Know How
CE11	Ability to collect and interpret relevant data in the field of computer and communications security.	• Know How
CE13	Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks.	• 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
The student will learn to analyze, detect and erase malware in systems and networks.	CG1 CE11 CE13 CT5
The student will learn to detect and fight against techniques used to hide and to provide persistence to malware in systems and networks.	CB1 CG1 CE8 CE11 CE13 CT5
The student will analyze systems and networks to detect and correct vulnerabilities that can be used by malware.	CG1 CE8 CE11 CE13 CT5
The student will learn the malware nowadays trends and the experience obtained from relevant case studies.	CB1 CG1 CT4 CT5

**Contents**

Topic	
Introduction to malware analysis and engineering.	a) What is malware? b) How to detect and erase it? c) What is malware engineering?
Malware types and definitions.	a) Estructure. b) Components. c) Infection vectors.



Malware Engineering.	a) Propagation techniques. b) Infection processes. c) Malware persistence. d) Hiding techniques.
Reverse malware engineering.	a) How to analyze and infer malware behavior? b) Understanding how new malware types work.
Tools for malware analysis.	a) Tools for malware detection. b) Tools for malware erasing.

### Planning

	Class hours	Hours outside the classroom	Total hours
Introductory activities	2	2	4
Lecturing	10	30	40
Laboratory practical	15	40	55
Discussion Forum	0	2	2
Case studies	5	4	9
Objective questions exam	2	4	6
Problem and/or exercise solving	3	6	9

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

### Methodologies

	Description
Introductory activities	We start doing a general introduction to the aims, the global contents of the subject and the expected outcomes. This activity will be performed individually.
Lecturing	We describe the different subject topics, giving the teaching material needed to follow them.  Through this methodology the competencies CB1, CG1, CE8, CE11, CE13, CT4 and CT5 are developed. This activity will be performed individually.
Laboratory practical	Students must perform a set of practices in the lab to better understand the contents explained along the master lessons.  Through this methodology the competencies CG1, CE8, CE11, CE13 and CT5 are developed. Some practices will be performed individually and others in groups (depending on the number of students).
Discussion Forum	Students must participate in the subject forum within TEMA at FAITIC.  Through this methodology the competencies CE8, CE11, CE13 and CT5 are developed. This activity will be performed individually.
Case studies	Along master lessons students will present case studies about threads, security problems already known and nowadays technologies.  Through this methodology the competencies CG1, CE11, CE13 and CT5 are developed. This activity can be performed individually or in groups of two people.

### Personalized assistance

Methodologies	Description
Introductory activities	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.
Lecturing	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.
Case studies	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.

Laboratory practical	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.
Discussion Forum	In the practical formative activities and tutoring, the professors of the subject will offer personal guidance to each student in the tasks to be performed, with the aim to orient the approach and the methodology. Also they will offer coordination information with other contents and subjects of the study program. It is recommended to consult the doubts with the teachers along the course in order to improve the understanding of the basic concepts, and for performing the tasks and activities to be evaluated.

<b>Assessment</b>			
	Description	Qualification	Evaluated Competences
Case studies	Students will provide presentations about case studies, selected by them, in order to analyze nowadays threads.	15	CG1 CE11 CE13 CT5
Laboratory practical	Students will perform a set of practices at the lab, where they work with the concepts studied along the master lessons.	45	CB1 CG1 CE8 CE11 CE13 CT5
Discussion Forum	Students must participate in the subject forum available at TEMA in FAITIC.	5	CB1 CG1 CE11 CE13 CT4 CT5
Objective questions exam	Two evaluation tests will be performed along the subject for the partial contents provided in the subject. Tests will be filled individually and time limited	30	CB1 CG1 CE11 CE13 CT5
Problem and/or exercise solving	Along master lessons, the teacher will ask questions to the students to test their knowledge level in the discussed topics.	5	CB1 CE11 CE13 CT5

### **Other comments on the Evaluation**

The elements that are part of the evaluation of the subject are the following:

- **Questionnaires:** along the course the student will fill two questionnaires that will contribute 15% to the final mark (each one).
- **Presentation of case studies:** each student has to provide an original presentation, which contributes with a 15% to the final mark.
- **Laboratory practice:** each student will have to perform a set of practical tasks/quizzes in the laboratory that will contribute 45% to the final mark.
- **Class participation:** students will discuss in class about expositions done by the professor, and this contributes up to a 5% to the final mark.
- **Forum participation:** students should interact individually in the forum of the subject to achieve up to a 5% to the final

mark. To achieve such percentage the student should provide at least two relevant contributions.

Therefore, we have:

**Final Mark** = Questionnaires (2\*x15% = 30%) + Case Study Presentation (15%) + Lab. Tasks (45%) + Class participation (5%) + Forum (5%) = 100%.

The students need to pass the questionnaires and the practical task with at least 4 points over 10 to calculate the average final mark. If any of the marks is below 4, then the final mark will never be higher than 4 points over 10.

The schedule of the midterm/intermediate exams will be approved in the Comisión Académica de Grado (CAG) and will be available at the beginning of each academic semester.

Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

Following the degree guidelines, the students that will follow this subject can choose between two possibilities: continuous assessment and final evaluation at the end of the semester.

**Continuous assessment:** the student follows the continuous assessment since the moment he/she fulfills the two questionnaires. From that moment we assume that he/she will participate in the subject, independently of the assistance to the first call.

**First Call:** if the continuous evaluation is not performed, then the student will have to perform a final exam that substitutes the questionnaires done along the course, in addition to provide the practical tasks and the equivalent work to be done as part of the continuous assessment.

**Second Call:** the student will have to perform the part not passed previously.

**The questionnaires and tasks, proposed and performed along the module, are only valid for the current course.**

---

### Sources of information

#### Basic Bibliography

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, 1, John Wiley & Sons Inc, 2014,

Michael Sikorski / Andrew Honig, Practical Malware Analysis, 1, William Pollock, 2012, San Francisco, CA (USA)

#### Complementary Bibliography

---

### Recommendations

#### Subjects that are recommended to be taken simultaneously

Forensic Analysis/V05M175V01207

Hardening of Operating Systems/V05M175V01202

Security in Mobile Devices/V05M175V01206

#### Subjects that it is recommended to have taken before

Applications Security/V05M175V01104

<b>IDENTIFYING DATA</b>			
<b>Security as a Business</b>			
Subject	Security as a Business		
Code	V05M175V01205		
Study programme	(*)Máster Universitario en Ciberseguridade		
Descriptors	ECTS Credits	Type	Year
	3	Mandatory	1st
Teaching language	Spanish		
Department			
Coordinator	Fernández Vilas, Ana Carneiro Díaz, Victor Manuel		
Lecturers	Carneiro Díaz, Victor Manuel Fernández Vilas, Ana		
E-mail	victor.carneiro@udc.es avilas@det.uvigo.es		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530010&amp;any_academic=2018_19&amp;idioma_assig=cast">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530010&amp;any_academic=2018_19&amp;idioma_assig=cast</a>		
General description	(*)Seguridade como negocio aborda as competencias necesarias para comprender o funcionamento dun Security Operation Centre (SOC), desde o punto de vista tecnolóxico, operacional e de intelixencia. Profundarase na infraestrutura, organización, operación e mecanismos de métrica necesarios para a explotación empresarial dos servizos asociados a un SOC. Estudaranse diferentes contornas de especialización como o sector bancario, administración pública ou o ámbito militar.		

<b>Competencies</b>	
Code	Typology

<b>Learning outcomes</b>	
Learning outcomes	Competences

<b>Contents</b>	
Topic	

<b>Planning</b>			
	Class hours	Hours outside the classroom	Total hours
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

<b>Methodologies</b>	
	Description

<b>Personalized assistance</b>	

<b>Assessment</b>		
Description	Qualification	Evaluated Competences

<b>Other comments on the Evaluation</b>	

<b>Sources of information</b>	
<b>Basic Bibliography</b>	
<b>Complementary Bibliography</b>	

<b>Recommendations</b>	

**IDENTIFYING DATA****Security in Mobile Devices**

Subject	Security in Mobile Devices			
Code	V05M175V01206			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Type	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish Galician			
Department				
Coordinator	López Bravo, Cristina			
Lecturers	Fernández Caramés, Tiago Manuel López Bravo, Cristina			
E-mail	clbravo@det.uvigo.es			
Web	<a href="http://faitic.uvigo.es">http://faitic.uvigo.es</a>			
General description	This course presents a general view of security in mobile devices with different characteristics. Based on the study of the architecture of these devices, we will discover their internal operation and which are the main security tools that they include, along with the risks and threats they suffer. We will study how to find, analyze and mitigate the vulnerabilities that affect mobile devices, using forensic analysis tools, secure application development and device management in business environments.			

The documentation of this course will be in English.

**Competencies**

Code		Typology
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 • 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 • 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
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 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
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
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
CE6	To develop and apply forensic research techniques for analysing incidents or cybersecurity threats.	• know • Know How
CE9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.	• know • 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
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
Knowing the fundamental concepts associated with security in mobile operating systems and the development of secure apps.	CB2 CG1 CE4 CE15 CT4 CT5

Identifying an app with malicious behavior and vulnerabilities in operating systems and apps	CB4 CG2 CE4 CT4 CT5
Being able to perform a forensic analysis of a mobile device	CB3 CG2 CE6 CT5
Knowing the fundamentals of mobile device management systems	CB2 CG1 CG2 CG5 CE9 CT5

## Contents

Topic	
Introduction: Threats and vulnerabilities that affect mobile devices	
Mobile devices architectures	
Security models in mobile devices	
Writing secure Applications	Permissions Packages management Users management APIs
Data assurance	
Devices assurance	
Network assurance	
Vulnerabilities, exploits and malicious applications	
Forensic analysis of mobile operating systems	
Mobile Device Management Systems	

## Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	9	9	18
Computer practices	10	10	20
Objective questions exam	2	14	16
Problem and/or exercise solving	0	11	11
Practices report	0	10	10

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

## Methodologies

	Description
Lecturing	The professors of the course present the main theoretical contents related to security in mobile devices. Through this methodology competencies CB3, CG1, CE4, CE15, and CT4 get developed.
Computer practices	Students will complete guided and supervised practices in the laboratory. Through this methodology the competencies CG2, CG5, CB2, CB4, CE4, CE6, and CE9 get developed.

## Personalized assistance

Methodologies	Description
Computer practices	The professors of the course will provide individual attention to the students during the course, solving their questions. Questions will be answered during the lab sessions or during tutorial sessions. Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the course website.
Lecturing	The professors of the course will provide individual attention to the students during the course, solving their questions. Questions will be answered during the master sessions or during tutorial sessions (also virtually). Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the course website.

## Assessment

Description	Qualification	Evaluated Competences
Objective questions exam	50	CB3 CB4 CE4
Problem and/or exercise solving	20	CB2 CB4 CG1 CG2 CE4
Practices report	30	CB4 CG5 CE4 CE6 CE9 CE15 CT4

### Other comments on the Evaluation

#### FIRST CALL

Following the guidelines of the degree, two evaluation systems will be offered to students attending this course: continuous assessment and eventual assessment.

Before the end of the second week of the course, students must declare if they opt for the continuous assessment or the eventual assessment. Those who opt for the continuous assessment system may not be listed as "not presented" if they make a delivery or an assessment test after the communication of their decision.

#### Continuous assessment system

The final grade of the course will be equal to the weighted arithmetic average of the tests previously indicated. To pass the course the final grade must be greater or equal to five.

#### Eventual assessment system

The final grade of the course will be equal to the weighted arithmetic average of the tests previously indicated. In this case, the problem-solving test (troubleshooting) will be done in a single test at the end of the bimester. To pass the course the final grade must be greater or equal to five.

#### SECOND CALL

The assessment will consist in an objective questions exam, a problem-solving exam and delivering the practice reports of all the practices carried out throughout the course.

#### OTHER COMMENTS

The obtained grades are only valid for the current academic year.

The use of any material during the tests will have to be explicitly authorized.

Plagiarism is regarded as serious dishonest behavior. If any form of plagiarism is detected in any of the tests or exams, the final grade will be FAIL (0), and the incident will be reported to the corresponding academic authorities for prosecution.

#### Sources of information

##### Basic Bibliography

Dominic Chell, *The mobile application hacker's handbook, 1*, John Wiley & Sons, 2015, Indianapolis

##### Complementary Bibliography

Joshua Drake, *Android hacker's handbook, 1*, John Wiley & Sons, 2014, Indianapolis

Charles Miller, *iOS hacker's handbook, 1*, John Wiley & Sons, 2012, Indianapolis

Abhishek Dubey, Anmol Misra, *Android security: attacks and defenses, 1*, CRC Press, 2013, Boca Ratón, Florida

David Thiel, iOS application security: the definitive guide for hackers and developers, 1, No Starch Press, 2016, San Francisco, California

---

Nikolay Elenkov, Android security internals: an in-depth guide to Android's security architecture, 1, No Starch Press, 2015, San Francisco, California

---

Andrew Hoog, iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices, 1, Syngress/Elsevier, 2011, Waltham, MA

---

Andrew Hoog, iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices, 1, Syngress/Elsevier, 2011, Waltham, MA

---

---

## **Recommendations**

---

### **Other comments**

---

It is recommended to have Linux OS and Java programming skills. It is also recommended, but not indispensable, to have Android programming skills.

---



<b>IDENTIFYING DATA</b>			
<b>Forensic Analysis</b>			
Subject	Forensic Analysis		
Code	V05M175V01207		
Study programme	(*)Máster Universitario en Ciberseguridade		
Descriptors	ECTS Credits	Type	Year
	3	Optional	1st
Teaching language	Spanish		
Department			
Coordinator	Suárez González, Andrés Vázquez Naya, José Manuel		
Lecturers	Suárez González, Andrés Vázquez Naya, José Manuel		
E-mail	asuarez@det.uvigo.es jose.manuel.vazquez.naya@udc.es		
Web	<a href="http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530012&amp;any_academic=2019_20&amp;idioma=cast&amp;idioma_assig=cast">http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530012&amp;any_academic=2019_20&amp;idioma=cast&amp;idioma_assig=cast</a>		
General description	El análisis forense de equipos consiste en la aplicación de técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. La materia "Análisis Forense de Equipos" tiene una fuerte componente práctica. Se comenzará con una introducción a este campo, explicando conceptos clave. A continuación, se estudiarán fundamentos y metodologías de análisis forense desde un punto de vista genérico y aplicable a nuevos casos, pero también se estudiarán ejemplos concretos basados en casos reales. Paralelamente, en las prácticas de laboratorio el/la alumno/a aprenderá a manejar diferentes herramientas de análisis forense y realizará prácticas simulando problemas reales.		

<b>Competencies</b>	
Code	Typology

<b>Learning outcomes</b>	
Learning outcomes	Competences
New	

<b>Contents</b>	
Topic	

<b>Planning</b>			
	Class hours	Hours outside the classroom	Total hours

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

<b>Methodologies</b>	
	Description

<b>Personalized assistance</b>	

<b>Assessment</b>		
Description	Qualification	Evaluated Competences

<b>Other comments on the Evaluation</b>	

<b>Sources of information</b>	
<b>Basic Bibliography</b>	
<b>Complementary Bibliography</b>	

<b>Recommendations</b>	

<b>IDENTIFYING DATA</b>				
<b>Ubiquitous Security</b>				
Subject	Ubiquitous Security			
Code	V05M175V01208			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Type	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish Galician			
Department				
Coordinator	Gil Castiñeira, Felipe José			
Lecturers	Gil Castiñeira, Felipe José Rabuñal Dopico, Juan Ramón			
E-mail	felipe@uvigo.es			
Web	<a href="http://faitic.uvigo.es">http://faitic.uvigo.es</a>			
General description	Intelligent devices are providing new services and we are almost unaware of their presence: our car is not anymore a mechanical machine, as it became a connected device where electronics suppose an important part; in hotels, we no longer use a key as we can open our room with a card or with our mobile phone; our home thermostats can be connected to a weather forecasting service to take advantage of the temperature of the environment. Those are all examples of the applications that allow embedded technologies, wireless communication networks, and in summary, the "Internet of Things" (IoT). This subject analyzes the problems and the best practices to make this kind of systems secure.			

<b>Competencies</b>		
Code		Typology
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 • 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 • 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 • 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
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 How
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
CE9	Ability to write clear, concise and motivated projects and work plans in the field of cybersecurity.	• 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 • Know How

<b>Learning outcomes</b>	
Learning outcomes	Competences
Gain knowledge of the security in the different layers of an ubiquitous system and the used technologies.	CB2 CB3 CB4 CG1 CG2 CG5 CE4 CE9 CT4 CT5

Understand the security problems related to the ubiquitous field.

CB2  
CB3  
CB4  
CG1  
CG2  
CG5  
CE4  
CE9  
CT4  
CT5

To know real cases of attacks to ubiquitous systems.

CB2  
CB3  
CB4  
CG5  
CE4  
CT4  
CT5

## Contents

Topic

Physical security	Hardware components. - Communication buses. - Interfaces. - Cryptographic hardware. Attacks.
Middleware security	Security during the startup process. Security in the operating system. Access control. Cyphering. Firmware updates.
Communication security	Wireless communications. Risks and threats for communications.
Security in the perception of the environment	Attacks in the positioning system. Attacks to sensor measurements. Privacy.

## Planning

	Class hours	Hours outside the classroom	Total hours
Project based learning	10	35	45
Lecturing	10	20	30

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

## Methodologies

	Description
Project based learning	Work in groups in the design, implementation and validation of an IoT system, with a special emphasis in the security.  Perform attacks to the security of the systems implemented by the other groups or implemented by third parties.  This methodology will contribute to acquire competences CB2, CB3, CB4, CG1, CG2, CG5, CE4, CE9, CT4 and CT5.
Lecturing	Professors will present the main theoretical contents related to the security for ubiquitous systems (security for embedded systems, communications and backends).  This methodology will contribute to the acquisition of competences CB2, CB3, CB4, CG1, CG2, CE4 and CE9.

## Personalized assistance

Methodologies	Description
Lecturing	The professors of the course will provide individual attention to the students during the course, solving their doubts and questions. Questions will be answered during the master sessions or during tutorial sessions. Professors will establish timetables for this purpose at the beginning of the course. This schedule will be published on the subject website.

Project based learning	The professors of the course will provide individual attention to the students during the course, solving their doubts and questions. The professors will guide and help the students to complete the assigned project. Questions will be answered during the supervising sessions, group supervising sessions, or during tutorial sessions. Teachers will establish timetables for this purpose at the beginning of the course. This schedule will be published on the subject website.
------------------------	--

<b>Assessment</b>			
	Description	Qualification	Evaluated Competences
Lecturing	Students will complete one or several exams to assess what they have learned in master lessons. In case there is more than one exam, the result will be the arithmetic mean of the different tests.	20	CB2 CB3 CB4 CG1 CG2 CE4 CE9
Project based learning	The students will work in groups in the design, implementation and proof of an IoT, with a special emphasis in security.  The same group of students will perform attacks to the security of the systems implemented by other groups or by third parties.  The results (project and reports containing the outcomes of the attacks) will be evaluated after the delivery, having into account key aspects such as the correction, the quality, the performance and the functionalities. It will be mandatory to deliver the code, prototypes and documentation. It will be also necessary make a public presentation of the results.  In addition, during the implementation of the project, the design and the evolution of the development will be evaluated. If the intermediate results are not satisfactory, a penalization of the 20% of the grade could be applied. The evaluation will be by group and by person: each one of the members of a team must document his/her tasks and answer the questions related to them.	80	CB2 CB3 CB4 CG1 CG2 CG5 CE4 CE9 CT4 CT5

### **Other comments on the Evaluation**

In order to pass the course it is necessary to complete the different parts of the subject (exam or exams about the master sessions and project). The final grade will be the **weighted geometric mean** of the grades of the different parts. For example, if "NT" is the grade obtained for the master sessions and "NP" for the project, the final grade will be:

$$\text{Grade} = \text{NT}^{0.2} \times \text{NP}^{0.8}$$

During the first month, students must provide a written declaration to opt for single evaluation. In other case, it will be considered that they opt for continuous evaluation. Students who select continuous evaluation and submit the first task or questionnaire may not be listed as "Absent".

Students who opt for the final assessment procedure have to submit also a dossier that must be defended in-person in front of the professors, with detailed information about the events and issues that arose during the execution of the different tasks, and especially the project. In addition, during the first month of the course, professors will notify students who opted for final assessment if they have to do the tutored work individually.

### **Second call to pass the course**

Students can opt to the second call only if they didn't pass the first call (at the end of the semester).

The evaluation procedure is the presented in the previous sections, but it will be necessary to submit an additional dossier that must be defended in-person in front of the professors, with detailed information about the events and issues that arose during the execution of the different tasks, and especially the project.

Students that have opted by the continuous evaluation procedure, can decide to maintain the grades of the different parts of the subject obtained in the first call or discard them.

### **Other comments**

Although the project will be completed (if possible) in groups, each student should keep a record of his or her activities. In the case in which the performance of a member of the group wouldn't be adequate compared with the performance of his or her team mates, he or she could be excluded from the group and/or qualified individually.

The use of any material during the tests will have to be explicitly authorized.

In case of detection of plagiarism or unethical behavior in any of the tasks/tests done, the final grade will be "failed (0)" and the professors will communicate the incident to the academic authorities to take the appropriate measures.

---

## **Sources of information**

### **Basic Bibliography**

Brian Russell, Drew Van Duren, Practical Internet of Things Security, 1, Packt Publishing, 2016,

### **Complementary Bibliography**

Houbing Song, Glenn A. Fink, Sabina Jeschke, Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications., 1, Wiley, 2018,

Bruce Schneider, Applied Cryptography: Protocols, Algorithms and Source Code in C, 2, Wiley, 2015,

Adam Shostack, Threat Modeling. Designing for Security., 1, Wiley, 2014,

---

## **Recommendations**

### **Subjects that it is recommended to have taken before**

Hardening of Operating Systems/V05M175V01202

Secure Networks/V05M175V01105

Applications Security/V05M175V01104

Information Security/V05M175V01102

Secure Communications/V05M175V01103

Intrusion tests/V05M175V01203

---

**IDENTIFYING DATA****Cybersecurity in Industrial Environments**

Subject	Cybersecurity in Industrial Environments		
Code	V05M175V01209		
Study programme	(*)Máster Universitario en Ciberseguridad		
Descriptors	ECTS Credits	Type	Year
	3	Optional	1st
Teaching language	Spanish		
Department			
Coordinator	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel		
Lecturers	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel		
E-mail	tiago.fernandez@udc.es mcacho@uvigo.es		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530014&amp;any_academic=2019_20">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530014&amp;any_academic=2019_20</a>		
General description	The Industry 4.0 paradigm derived into the proliferation of industrial devices connected to networks and physical processes. This subject, besides reviewing traditional industrial systems (i.e., industrial control systems, access controls, communication and information management systems) is focused on the security of the Industry 4.0 technologies: IoT/IIoT, robotics, cloud/edge computing, augmented reality, blockchain or AGVs.		

**Competencies**

Code	Typology
------	----------

**Learning outcomes**

Learning outcomes	Competences
-------------------	-------------

**Contents**

Topic	
(*)Introducción	(*)Políticas de seguridad industrial Implicaciones de la ciberseguridad industrial y de infraestructuras críticas Casos prácticos
(*)Sistemas de control de acceso físico a dependencias industriales	(*)Sistemas de proximidad Sistemas de acceso remoto Sistemas biométricos
(*)Sistemas de control industrial	(*)Arquitecturas de comunicaciones Sistemas tradicionales Sistemas ciberfísicos
(*)Sistemas de la Industria 4.0	(*)Introducción a la Industria 4.0 Sistemas IoT/IIoT Seguridad en otras tecnologías 4.0 (e.g., realidad aumentada, cloud/edge computing, blockchain, AGVs)
(*)Sistemas de gestión de información en entornos industriales	(*)Bases de datos tradicionales ERPs PLMs Sistemas MES

(\*)Sistemas de comunicaciones industriales

(\*)Arquitectura de comunicaciones

Tecnologías de comunicación cableadas

Tecnologías de comunicación inalámbricas

## Planning

	Class hours	Hours outside the classroom	Total hours
Autonomous practices through ICT	10	10	20
Mentored work	0	20	20
Lecturing	9	9	18
Objective questions exam	1	15	16

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

## Methodologies

	Description
Autonomous practices through ICT	(*)Realización por parte del alumnado de prácticas guiadas y supervisadas.
Mentored work	(*)Realización por parte del alumnado de trabajos de componente tanto teórica como práctica.
Lecturing	(*)Exposición por parte del profesorado de los principales contenidos teóricos relacionados con la ciberseguridad en contornos industriales.

## Personalized assistance

Methodologies	Description
Autonomous practices through ICT	

## Assessment

	Description	Qualification	Evaluated Competences
Autonomous practices through ICT	(*)Resolución de prácticas y realización de informes con los resultados obtenidos.	30	
Mentored work	(*)Realización de un trabajo con parte teórica y parte práctica.	30	
Objective questions exam	(*)Examen escrito sobre los contenidos teóricos y prácticos impartidos durante el curso.	40	

## Other comments on the Evaluation

### Sources of information

#### Basic Bibliography

Eric Knapp, Joel Thomas Langill, Industrial Network Security., Elsevier, 2014,

Junaid Ahmed Zubairi, Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies., IGI Global, 2012,

Tyson Macaulay, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS., Auerbach Publications, 2012,

Josiah Dykstra, Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems., O'Reilly, 2015,

Pascal Ackerman, Industrial Cybersecurity, Packt, 2017,

#### Complementary Bibliography

Peng Cheng, Heng Zhang, Jiming Chen, Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop., CRC Press, 2016,

## Recommendations

**IDENTIFYING DATA****Cybersecurity Incident Management**

Subject	Cybersecurity Incident Management		
Code	V05M175V01210		
Study programme	(*)Máster Universitario en Ciberseguridade		
Descriptors ECTS Credits	Type	Year	Quadmester
3	Optional	1st	2nd
Teaching language	Spanish		
Department			
Coordinator	Álvarez Sabucedo, Luis Modesto Dafonte Vázquez, José Carlos		
Lecturers	Álvarez Sabucedo, Luis Modesto Dafonte Vázquez, José Carlos Gómez García, Ángel		
E-mail	lsabucedo@det.uvigo.es carlos.dafonte@udc.es		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530015&amp;any_academic=2018_19&amp;idioma_assig=cast&amp;idioma_assig=cast">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530015&amp;any_academic=2018_19&amp;idioma_assig=cast&amp;idioma_assig=cast</a>		
General description	La gestión de incidentes de ciberseguridad se centra en manejar la proactividad para prevenir y atenuar posibles consecuencias. Se obtendrá el conocimiento necesario sobre herramientas que pueden facilitar la gestión de los incidentes y las recuperaciones, la justificación de los planes propuestos para recuperación y resiliencia, la identificación y clasificación de los posibles incidentes y la definición de los cauces para su gestión y resolución.		

**Competencies**

Code	Typology
------	----------

**Learning outcomes**

Learning outcomes	Competences
-------------------	-------------

**Contents**

Topic
-------

**Planning**

	Class hours	Hours outside the classroom	Total hours
--	-------------	-----------------------------	-------------

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

**Methodologies**

Description
-------------

**Personalized assistance****Assessment**

Description	Qualification	Evaluated Competences
-------------	---------------	-----------------------

**Other comments on the Evaluation****Sources of information****Basic Bibliography****Complementary Bibliography****Recommendations**