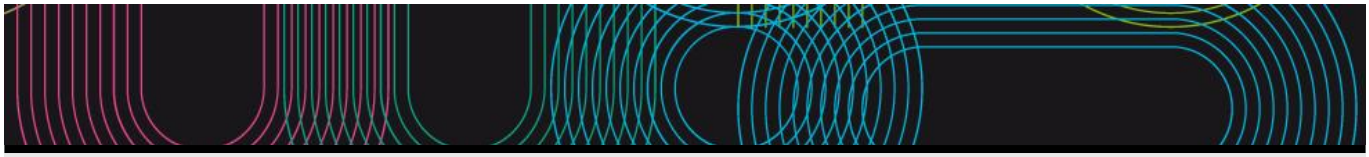

(*)Escola de Enxeñaría de Telecomunicación

(*)Páxina web

(*)

www.teleco.uvigo.es

(*)Presentación

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

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

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

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

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

Master in Telecommunication Engineering

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

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

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

Interuniversity Masters

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

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

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

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

(*)Equipo directivo

MANAGEMENT TEAM

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

Secretaría e Subdirección de Novas Titulacións: Pedro Rodríguez Hernández

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

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

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

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

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

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

BACHELOR□SDEGREE IN TELECOMMUNICATION TECHNOLOGIES ENGINEERING

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

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

MASTER IN TELECOMMUNICATION ENGINEERING

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

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

MASTER INCYBERSECURITY

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

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

MASTER ININDUSTRIAL MATHEMATICS

Generalcoordinator: Elena Vázquez Cendón (USC)

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

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

INTERNATIONALMASTER IN COMPUTER VISION

General coordinator: Xose Manuel Pardo López (USC)

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

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

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

General coordinator: Javier Mas (USC)

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

https://quantummastergalicia.es/info

Máster Universitario en Ciberseguridad

Subjects			
Year 1st			
Code	Name	Quadmester	Total Cr.
V05M175V11108	Information Security	1st	5
V05M175V11109	malware analysis	1st	5
V05M175V11110	Privacy and anonymity	1st	5
V05M175V11111	Application security	1st	5
V05M175V11112	Secure networks	1st	5

V05M175V11113	Distributed ledger and Blockchain technologies	1st	5
V05M175V11211	Communications security	2nd	5
V05M175V11212	Systems Fortification	2nd	5
V05M175V11213	Industrial cybersecurity and IoT	2nd	5
V05M175V11214	Ethical Hacking and Intrusion Test	2nd	5
V05M175V11215	Business in cybersecurity and entrepreneurship	2nd	4
V05M175V11216	Forensic analysis	2nd	3
V05M175V11217	Data center security	2nd	3
V05M175V11218		2nd	3
V05M175V11219	Smart Contracts and dApps	2nd	3

Year 2nd

Code	Name	Quadmester	Total Cr.
V05M175V11301	Information security management	1st	5
V05M175V11302	Concepts and laws	1st	4
V05M175V11303	Business practice	1st	9
V05M175V11304	Final Master's Project	1st	12

IDENTIFYING DATA				
Information Security				
Subject	Information Security			
Code	V05M175V11108			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	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	http://moovi.gal			
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.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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. Quantumresistant 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	2	0	2

*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 curse contents. Written homework, with review and grading.
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.
Lecturing	Lectures on the topics included in the course: definitions, concepts, main results, properties and applications.

Personalized assistance	
Methodologies	**Description**
Problem solving	Individual office hours will be offered to answer the questions about problems and exercises assigned to the students. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Laboratory practical	Individual assistance will be given to the students who request guidance on the programming assignments or computer lab practice. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
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. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga

Assessment			
	Description	Qualification	Training and Learning Results
Problem solving	4 homework problem sets, to be worked out individually. Written submission	30	
Laboratory practical	Design and development of programming assignments. Functional and performance tests will be run	30	
Essay questions exam	Written exam. Questions, problems or exercises about the contents covered in the course	40	

Other comments on the Evaluation

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

The continuous evaluation option consists in a final written exam (40% of the qualification), the completion of programming assignments (30% of the qualification) and homework (30%). The global assessment option consists in a final written exam (40% of the qualification) and in the completion of assignments (two, 30% of the qualification each one). 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 an extraordinary 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, 2021

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**, 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.

IDENTIFYING DATA				
malware analysis				
Subject	malware analysis			
Code	V05M175V11109			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	English			
Department				
Coordinator	Burguillo Rial, Juan Carlos			
Lecturers	Burguillo Rial, Juan Carlos Hernández Pereira, Elena María Rivas López, Jose Luis			
E-mail	jrial@uvigo.es			
Web	http://https://moovi.uvigo.gal			
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. This course will be taught in English. However, students have the possibility to interact with teachers in Spanish or Galician if necessary. All the documentation needed for the course will be provided in English.			

Training and Learning Results	
Code	
B2	To learn about malware stealth and persistence techniques, as well as current malware trends through the study of real cases.
C2	Detect and eliminate vulnerabilities susceptible to malware, as well as malware, in communication systems and networks, as well as evade malware stealth and persistence techniques.
D3	Work as a malware analyst, to protect applications, as well as analyse their security in any application area.
D6	Identify vulnerabilities in a real system, as well as vary its parameters and configure it to protect against them, thus limiting exposure to known threats.

Expected results from this subject	Training and Learning Results
To provide the student the capability to analyze, detect and erase malware.	B2 C2
To explore and evaluate, practically and with case studies, the techniques used nowadays to hide malware.	D3
Learn the new tendencies to find vulnerabilities in real systems, and how to protect and limit the exposure to known threats.	D6

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) Structure. 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 knowledge B2, skill C2 and competence D6 are achieved. 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 knowledge B2, skill C2 and competencies D3 and D6 are achieved. 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 the MOOVI platform. Through this methodology the knowledge B2 and the competence D6 are achieved. This activity will be performed individually.
Case studies	Along master lessons students will present case studies about threats, security problems already known and nowadays technologies. Through this methodology the knowledge B2 and competencies D3 and D6 are achieved. 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. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
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. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
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. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
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. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).
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. Students can request tutoring support through the Moovi platform (https://moovi.uvigo.gal).

Assessment			
	Description	Qualification	Training and Learning Results
Laboratory practical	Students will perform a set of practices (3 x 15% = 45%) at the lab, where they work with the concepts studied along the master lessons.	45	
Discussion Forum	Students must participate in the subject forum available at Moovi.	5	
Case studies	Students will provide presentations about case studies, selected by them, in order to analyse nowadays threats.	15	
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	
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	

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 (individually or in a group) 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 practices (by defect 3 practices with a weight of 15% each) 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 Score = Questionnaires (2*x15% = 30%) + Case Study Presentation (15%) + Lab. Tasks (45%) + Class participation (5%) + Forum (5%) = 100%.

The students need to pass the questionnaires, the case studies and the practical tasks 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 4.9 points over 10.

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

Following the degree guidelines, the students that will follow this subject can choose between two possibilities: continuous or final assessment (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 presentation at the first call.

Global assessment: if the continuous assessment 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.

Extraordinary assessment: the student will have to perform the part not passed previously.

End-of-program assessment: the student will have to perform the part not passed previously.

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.

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

Complementary Bibliography

Recommendations

Subjects that are recommended to be taken simultaneously

Forensic analysis/V05M175V11216

IDENTIFYING DATA				
Privacy and anonymity				
Subject	Privacy and anonymity			
Code	V05M175V11110			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	#EnglishFriendly Spanish			
Department				
Coordinator	Pérez González, Fernando			
Lecturers	Hernández Pereira, Elena María Pérez González, Fernando			
E-mail	fperez@gts.uvigo.es			
Web	http://http://moovi.gal			
General description	This subject presents the main techniques to provide privacy and anonymity in networks, systems and applications. It covers concepts and methods of differential privacy, privacy enhancing technologies (PET), geolocation privacy, machine learning privacy, and anonymity techniques. The implications of privacy by design, and ethical and legal aspects of privacy are also explored.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Introduction. Attacks.	Introduction to privacy and anonymity. Inference attacks. Traffic analysis attacks. Online tracking.
Differential privacy.	Differential privacy. Differential privacy mechanisms. Composition theorems.
Privacy preserving and enhancing techniques.	Privacy-preserving primitives: information retrieval, set intersection. Privacy enhancement techniques with homomorphic encryption and secure multi-party computing. Bloom filters.
Anonymity.	Basic concepts. K-anonymity, l-diversity and t-proximity.
Applications in privacy and anonymity.	Geolocation privacy. Anonymous communications. Onion routing. Mixes. Anonymous authentication. Privacy in machine learning.

Planning			
	Class hours	Hours outside the classroom	Total hours
Laboratory practical	19	38	57
Lecturing	19	38	57
Problem solving	2	0	2
Objective questions exam	2	0	2
Report of practices, practicum and external practices	0	3	3
Report of practices, practicum and external practices	0	4	4
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies	
	Description
Laboratory practical	Students will develop privacy and anonymity projects in the laboratory as applications of the techniques presented in the master classes. The practices or projects will be supervised by the teachers.
Lecturing	Systematic presentation of the course contents: concepts, results, algorithms, examples and use cases.
Problem solving	Solving problems in the classroom by teachers.

Personalized assistance

Methodologies	Description
Laboratory practical	Questions related to laboratory practices and the development of the project will be answered individually. Office hours will be established at the beginning of the course and will be published on the subject's website.
Lecturing	Individual attention will be given to students who require orientation for the study, additional explanation on the contents of the discipline, clarification or guidance on problem solving. Office hours will be established at the beginning of the course and will be published on the subject's website.
Problem solving	Queries about solving problems and exercises raised in class or worked independently will be addressed individually. Office hours will be established at the beginning of the course and will be published on the subject's website.

Assessment

	Description	Qualification	Training and Learning Results
Objective questions exam	Written exam. Resolution of questions, problems or exercises.	40	
Report of practices, practicum and external practices	Reports on the practices corresponding to the first half of the course carried out individually or in pairs.	30	
Report of practices, practicum and external practices	Reports on the practices corresponding to the first half of the course carried out individually or in pairs.	30	

Other comments on the Evaluation

It is necessary to achieve a minimum of 4.00 in the written exam to pass the subject.

In the practice reports, it will be necessary to indicate if generative AI tools were used and, if so, explicitly state which elements of the report were produced with them. In case of detection of plagiarism or unjustified use of these tools, the professors may grade the deliverable with 0 points.

The grade of the tests/reports will only be valid in the academic year in which they are obtained.

Sources of information

Basic Bibliography

C. Dwork, **The Algorithmic Foundations of Differential Privacy**, Now Publishers Inc., 2013

J. Morris Chang, Di Zhuang, and G. Dumindu Samaraweer, **Privacy-preserving Machine Learning**, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, GCATI, 2020

Complementary Bibliography

Katharine Jarmul, **Practical Data Privacy**, O'Reily Media, 2023

Nishant Bhajaria, **Data Privacy**, Manning Publications, 2022

PALISADE, **PALISADE HOMOMORPHIC ENCRYPTION SOFTWARE LIBRARY**,

Ilaria Chillotti, **TFHE Deep Dive**, https://www.zama.ai/post/tfhe-deep-dive-part-1,

Daniele Micciancio, and Oded Regev, **Lattice-based cryptography**, https://cseweb.ucsd.edu/%7Edaniele/papers/PostQuantum.pdf, Springer, 2009

Recommendations

IDENTIFYING DATA				
Application security				
Subject	Application security			
Code	V05M175V11111			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	Spanish			
Department				
Coordinator	Fernández Vilas, Ana			
Lecturers	Bellas Permuy, Fernando Losada Pérez, José			
E-mail	avilas@uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530104&idioma=cast&any_academic=2024_25			
General description	Developing secure applications is not a trivial task. Knowing the most common vulnerabilities that affect the applications, the mechanisms of authentication, authorization and access control, as well as the incorporation of the security to the software life cycle, is essential to build secure applications. This course addresses all of these aspects, with special emphasis in the development of applications and web services.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA

Secure networks

Subject	Secure networks			
Code	V05M175V11112			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language				
Department				
Coordinator	Rodríguez Rubio, Raúl Fernando			
Lecturers	Nóvoa de Manuel, Francisco Javier Rodríguez Rubio, Raúl Fernando			
E-mail	rrubio@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530105&fitxa_apartat=3&any_academic=2024_25&idioma_assig=&any_academic=2024_25			
General description	The main objective of Secure Networks is for students to learn how to design and implement network infrastructures that are capable of providing the necessary security services in a modern corporate environment. They must know the reference security architectures and be able to configure and manage them, using technologies such as IDS / IPS and Firewalls, among others. The subject is conceived so that laboratory practices, with physical and virtual equipment, have a major importance in the learning process.			

Training and Learning Results

Code

Expected results from this subject

Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Distributed ledger and Blockchain technologies				
Subject	Distributed ledger and Blockchain technologies			
Code	V05M175V11113			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language				
Department				
Coordinator	Fernández Iglesias, Manuel José			
Lecturers	Álvarez Sabucedo, Luis Modesto Fernández Caramés, Tiago Manuel Fernández Iglesias, Manuel José			
E-mail	manolo@uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530106&any_academic=2024_25			
General description	In this course, the basic concepts about distributed ledger and blockchain technologies are introduced.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Communications security				
Subject	Communications security			
Code	V05M175V11211			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Rodríguez Rubio, Raúl Fernando			
Lecturers	Fernández Iglesias, Diego Rodríguez Rubio, Raúl Fernando Suárez González, Andrés			
E-mail	rrubio@det.uvigo.es			
Web	http://https://moovi.uvigo.gal			
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.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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: WPA/2/3: Personal & Enterprise security
Network level security	IPsec security protocols IPsec dynamic key management IPsec authentication mechanisms
Securing Internet infrastructure	Routing protocols security DNS security TCP security
Data transmission security	The TLS protocol Cryptographic suites WebPKI infrastructure Certificate validation
Mobile networks security	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
Practices through ICT	0	58	58
Essay questions exam	2	0	2
Report of practices, practicum and external practices	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. Students will acquire competencies CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
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. Office hours: Raúl Rodríguez Rubio https://moovi.uvigo.gal/user/profile.php?id=11315 Andrés Suárez González https://moovi.uvigo.gal/user/profile.php?id=11340 Diego Fernández Iglesias https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614
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.
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	Training and Learning Results
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	
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.	60	
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.	40	
Report of practices, practicum and external practices	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	

Other comments on the Evaluation

The evaluation of the subject can either follow a continuous assessment strategy (EC) or a general assessment one (EG). 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, 60%) and the corresponding grade for the essay questions exam (E, 40%). 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, which will never be less than two.
FINAL GRADE (EC) = (TA ^ 0.6) × (E ^ 0.4)
If the laboratory practices assessment is unfit, the grade will be the minimum between the written test score (E) and 3.
Students who choose EG 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.
FINAL GRADE (EU) = (T ^ 0.2) × (E ^ 0.8)
Finally, for the extra 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

Madhusanka Liyanage, Ijaz Ahmad, Ahmed Abro, Andrei Gurtov, Mika Ylianttila, **A Comprehensive Guide to 5G Security**, Wiley, 2018

Complementary Bibliography

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

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

D. J. Bernstein, **SYN cookies**,

P. McManus, **Improving syncookies**, 2008

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

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

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

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

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

Cloudflare Inc., **How DNSSEC works**,

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

E. Jones and O. L. Moigne, **OSPF security vulnerabilities analysis**, IETF, 2006

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

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

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

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

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

S. Kent, **IP Authentication Header**, IETF, 2005

S. Kent, **IP Encapsulating Security Payload**, IETF, 2005

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

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

Recommendations

IDENTIFYING DATA				
Systems Fortification				
Subject	Systems Fortification			
Code	V05M175V11212			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Blanco Fernández, Yolanda			
Lecturers	Blanco Fernández, Yolanda Yáñez Izquierdo, Antonio Fermín			
E-mail	yolanda@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530108&any_academic=2024_25			
General description	A newly installed operating system is inherently insecure. It presents certain vulnerabilities based on factors such as the age of the OS, the presence of backdoors, the services it provides, and the use of default policies that do not prioritize security. When we refer to the fortification of an operating system, we mean the act of configuring this OS with the intention of making it as secure as possible, aiming to minimize the risk of it being compromised and exploited by any vulnerabilities. This typically involves applying security patches, changing certain default OS policies, and removing (or deactivating) non-essential applications and services. The document of the teaching guide can be consulted at the UDC link specified above.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Ciberseguridade industrial e IoT				
Subject	Ciberseguridade industrial e IoT			
Code	V05M175V11213			
Study programme	Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1	2c
Teaching language	Castelán Galego			
Department	Dpto. Externo Enxeñaría de sistemas e automática Enxeñaría telemática			
Coordinator	Diaz-Cacho Medina, Miguel Ramón			
Lecturers	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel Gil Castiñeira, Felipe José			
E-mail	mcacho@uvigo.es			
Web	http://www.moovi.gal			
General description	Os dispositivos intelixentes están a prestarnos cada vez máis servizos case sen que nos deamos conta da súa presenza: o coche deixou de ser unha simple máquina mecánica para converterse nun sistema conectado cun enorme control electrónico; nos hoteis xa non usamos chave, senón que podemos abrir a nosa habitación cun cartón ou o noso teléfono móbil; Os nosos *termostatos domésticos pódense conectar a un servizo de prognóstico do tempo e axustarse ao clima nas próximas horas. As contornas industriais son casos de uso particularmente importantes, xa que a conexión en rede de dispositivos que miden e controlan procesos permite a Industria 4.0. Todos son exemplos das aplicacións habilitadas por tecnoloxías "integradas", redes de comunicacións inalámbricas e, en última instancia, "Internet das cousas" (IoT). Esta materia analiza os problemas e as mellores prácticas para facer que este tipo de sistemas sexan seguros, con especial énfase na seguridade das tecnoloxías da Industria 4.0, como os sistemas *IoT/*IioT, os sistemas *robóticos, a *computación na nube/bordo, a realidade aumentada, a cadea de bloques ou os AGV.			

Resultados de Formación e Aprendizaxe	
Code	
B9	Identificar a arquitectura dos sistemas IoT, a súa complexidade e vulnerabilidades, así como comprender a seguridade no ámbito dos sistemas embebidos e dos sistemas de comunicación IoT.
C9	Analizar as implicacións do nivel de seguridade das tecnoloxías relacionadas coa dixitalización dos sectores produtivos, así como avaliar e modelar as ameazas e executar ataques co obxectivo de deseñar sistemas de IoT seguros.
D2	Demostrar autonomía e iniciativa para resolver problemas complexos que impliquen múltiples tecnoloxías no ámbito das redes ou sistemas de comunicación, e desenvolver solucións innovadoras no ámbito das comunicacións e informática distribuídas privadas.
D5	Analizar a seguridade dos protocolos de comunicación na capa física; ligazón; de rede e transporte, así como avaliar nunha rede corporativa as medidas de seguridade que se deben implantar para protexer os seus bens internos e comunicacións.
D7	Aplicar políticas de seguridade e implementar as diferentes técnicas de protección baseadas na comprensión dos ataques a sistemas industriais para minimizar os problemas de seguridade e os ataques ás redes de control industrial.

Resultados previstos na materia	
Expected results from this subject	Training and Learning Results
RA01. Comprender a execución de políticas de seguridade e as súas implicacións en contornas industriais.	B9 C9 D7
RA02. Comprender as diferentes técnicas de protección e ataque en sistemas industriais e saber como se poden implementar.	B9 C9 D2 D5 D7
RA03. Entender as problemáticas de seguridade e os ataques a redes de control industrial e coñecer os mecanismos que permiten minimizalos.	B9 C9 D5 D7

RA04. Coñecer e identificar a arquitectura dos sistemas IoT, a súa complexidade e as súas vulnerabilidades	B9
RA05. Comprender a seguridade no ámbito dos sistemas embebidos.	B9 C9 D2 D5 D7
RA06. Comprender a seguridade no ámbito dos sistemas de comunicación IoT.	B9 C9 D5
RA07. Coñecer casos reais de ataques a sistemas IoT.	B9 D7
RA08. Ser capaz de comprender as implicacións a nivel de seguridade de tecnoloxías relacionadas con conceptos como a Industria 4.0/5.0.	B9 C9 D5 D7
RA09. Ser capaz de valorar e modelar ameazas e executar ataques sobre un sistema IoT	B9 C9 D2
RA10. Ser capaz de deseñar sistemas IoT seguros	B9 C9 D2 D5 D7

Contidos	
Topic	
Introdución á ciberseguridade industrial.	Introdución á ciberseguridade industrial.
Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud	Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud
Ciberseguridade de sistemas de control e comunicacións industriais.	Ciberseguridade de sistemas de control e comunicacións industriais.
Ciberseguridade de tecnoloxías da Industria 4.0/5.0.	Ciberseguridade de tecnoloxías da Industria 4.0/5.0.
Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.	Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.
Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.	Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.
Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.	Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.

Planificación			
	Class hours	Hours outside the classroom	Total hours
Aprendizaxe baseado en proxectos	5	45	50
Lección maxistral	14	20	34
Prácticas con apoio das TIC	15	25	40
Exame de preguntas obxectivas	1	0	1
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Metodoloxía docente	
	Description
Aprendizaxe baseado en proxectos	Implementación grupal do deseño, implementación e probas dun sistema IoT, con especial énfase na seguridade. Realizar ataques grupales á seguridade dos sistemas implementados por outros compañeiros ou terceiros.
Lección maxistral	Presentación, por parte do profesorado, dos principais contidos teóricos relacionados coa seguridade industrial e IoT (seguridade embebida, en comunicacións e backends, con especial foco en contornas industriais)
Prácticas con apoio das TIC	Realización por parte dos alumnos de prácticas guiadas e supervisadas.

Atención personalizada	
Methodologies	**Description**

Aprendizaxe baseado en proxectos	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará ao alumnado durante a realización do proxecto. As dúbidas resolveranse durante as titorías en grupo, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Lección maxistral	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. As dúbidas resolveranse durante a propia sesión maxistral, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Prácticas con apoio das TIC	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que lles foron asignadas, tanto nas prácticas. As dúbidas resolveranse ben durante as propias clases ou ben no horario establecido para as titorías.

Avaliación

	Description	Qualification	Training and Learning Results		
Aprendizaxe baseado en proxectos	O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, pondo unha énfase especial na seguridade e/ou realizará ataques á seguridade dos sistemas implementados por outros compañeiros/as ou por terceiros. O proxecto realizado, e o informe que contén o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como a corrección, a calidade, as prestacións e as funcionalidades. Deberase entregar o código, prototipos e documentación realizados. Así mesmo, será necesario realizar unha presentación dos resultados. Durante a realización do proxecto realizarase un seguimento continuo do deseño e da evolución da implementación. Si os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de até o 20% da nota. O seguimento será grupal e individual: cada un do membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas.	40	B9	C9	D2 D5 D7
Prácticas con apoio das TIC	Resolución de prácticas e realización de informes cos resultados obtidos.	30	B9	C9	D2 D5 D7
Exame de preguntas obxectivas	Exame escrito sobre os contidos teóricos e prácticos impartidos durante o curso.	30	B9	C9	D2 D5 D7

Other comments on the Evaluation

Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exámenes acerca dos contidos expostos na sesión maxistral e o proxecto). A nota final será o resultado de aplicar a **media xeométrica ponderada** da nota de cada unha das partes.

Así, se a nota das sesións maxistrais é NT, a nota do proxecto é NP e a nota das prácticas é NL, a nota final será:

Nota = NT^0.3 × NP^0.4 × NL^0.3

Durante o primeiro mes, o estudiantado deberá indicar explícitamente e por escrito o seu desexo de cursar a materia seguindo a evaluación global. Noutro caso se considerará que seguen a availiación continua. Quen sigan a avaliación continua non se podrán considerar "non presentados" así que realicen a entrega do primeiro cuestionario ou tarefa.

O alumnado que opte pola avaliación global deberá presentar adicionalmente un *dossier* que deberá defender presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, e moi especialmente o proxecto. No caso de seguir a avaliación global, os alumnos/as deberán realizar o traballo de forma individual, salvo que o profesorado comuníquelles explícitamente a autorización para realizalo en grupo.

Avaliación extraordinaria

Só podrán optar á avaliación extraordinaria quen non supere a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.

Quen seguise a avaliación continua pode optar por manter as notas obtidas na primeira oportunidade para as distintas partes da materia ou descartalas.

Outros comentarios

As puntuacións obtidas só son válidas para o curso académico en vigor. Aínda que o proxecto se desenvolverá (na medida do posible) en grupos, o alumnado debe gardar evidencias do seu traballo individual dentro do grupo. No caso no que o rendemento dun alumno ou alumna non sexa acorde ao dos seus compañeiros de grupo, se considerará a súa expulsión do mesmo e/ou podrá ser avaliado/a de forma completamente individual nesta parte.

O uso de calquera material durante a realización dos exámenes tendrá que ser autorizado explícitamente polo profesorado.

En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a calificación da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tomen as medidas oportunas.

Na realización das actividades académicas desta materia permítese o uso de intelixencia artificial xenerativa (IAX). O seu uso debe realizarse de forma ética, crítica e responsable. No caso de utilizar IAX, debe avaliarse de forma crítica calquera resultado que proporcione, e verificar de forma coidadosa calquera cita ou referencia xerada. Así mesmo, recoméndase declarar o uso das ferramentas utilizadas.

Bibliografía. Fontes de información

Basic Bibliography

Brian Russell, Drew Van Duren,, **Practical Internet of Things Security**, 978-1788625821, 2, Packt Publishing, 2018

Eric Knapp, Joel Thomas Langill, **Industrial Network Security**, 978-0-12-420114-9, 2, Elsevier, 2015

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, 978-1609608514, GI Global, 2012

Tyson Macaulay,, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.,**, 978-1439801963, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems**, 978-1491920947, O'Reilly, 2016

Pascal Ackerman, **Industrial Cybersecurity,**, 978-1788395151, Packt, 2017

Complementary Bibliography

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 978-1-119-22604-8, 1, Wiley, 2015

Adam Shostack, **Threat Modeling. Designing for Security**, 978-1118809990, 1, Wiley, 2014

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, 978-1498734738, CRC Press, 2016

Recomendacións

IDENTIFYING DATA				
Ethical Hacking and Intrusion Test				
Subject	Ethical Hacking and Intrusion Test			
Code	V05M175V11214			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Costa Montenegro, Enrique			
Lecturers	Carballal Mato, Adrián Costa Montenegro, Enrique			
E-mail	kike@gti.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530110&any_academic=2024_25&idioma=cast			
General description	There is no better way to prove the strength of a system than to attack it. The Intrusion Tests serve to reproduce access attempts of an attacker using the vulnerabilities that may exist in a given infrastructure. In this course the fundamental topics oriented to the intrusion tests (pentesting) will be covered, covering the different phases of an attack and exploitation (from the recognition and control of access to the erasure of tracks).			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA

Business in cybersecurity and entrepreneurship

Subject	Business in cybersecurity and entrepreneurship			
Code	V05M175V11215			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	4	Mandatory	1st	2nd
Teaching language				
Department				
Coordinator	Fernández Vilas, Ana			
Lecturers	Carneiro Díaz, Victor Manuel Fernández Vilas, Ana			
E-mail	avilas@uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530111&any_academic=2024_25&idioma=cast&any_academic=2024_25			
General description	In the subject Business in cybersecurity and entrepreneurship, security is approached as a transversal element in the organization, from the strategic and business generation point of view. Different approaches to the monetization of data and their security are presented, as well as the different professional profiles present in the organization, focusing on the operation of a Security Operation Center (SOC) and its associated tools. Finally, different cases of success and business opportunities oriented to different productive sectors are addressed, with special attention to entrepreneurship.			

Training and Learning Results

Code

Expected results from this subject

Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Forensic analysis				
Subject	Forensic analysis			
Code	V05M175V11216			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Suárez González, Andrés			
Lecturers	Suárez González, Andrés Vázquez Naya, José Manuel			
E-mail	asuarez@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530112&any_academic=2024_25			
General description	Computer forensic analysis is the application of scientific and analytical techniques to identify, preserve, analyse and present data that is valid in legal proceedings. This subject has a strong practical component. It will begin with an introduction to computer forensics, explaining key concepts. Next, the fundamentals and methodologies of forensic analysis will be studied from a generic point of view and applicable to new cases, but also specific examples based on real cases will be studied. In the laboratory practicals, students will learn how to use different forensic analysis tools and will carry out practices simulating real problems.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Data center security				
Subject	Data center security			
Code	V05M175V11217			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Suárez González, Andrés			
Lecturers	Dafonte Vázquez, José Carlos López Rivas, Antonio Daniel Suárez González, Andrés			
E-mail	asuarez@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530113&any_academic=2024_25			
General description	Security in a data processing centre involves the implementation of a variety of physical and logical measures to protect the infrastructure and the data stored in the DPC, with the aim of guaranteeing the availability, confidentiality and integrity of the information and systems critical to an organisation. This course will introduce the different architectures of data centres as well as the auxiliary physical facilities that are necessary for their operation.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

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	Training and Learning Results

Other comments on the Evaluation

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
(*)Seguridade en dispositivos móviles				
Subject	(*)Seguridade en dispositivos móviles			
Code	V05M175V11218			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish Galician English			
Department				
Coordinator	López Bravo, Cristina			
Lecturers	Fernández Caramés, Tiago Manuel López Bravo, Cristina Rivas López, Jose Luis			
E-mail	clbravo@det.uvigo.es			
Web	http://http://moovi.uvigo.gal			
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.			

Training and Learning Results	
Code	
B14	Distinguish the fundamental concepts associated with security in mobile operating systems and the development of secure apps, as well as mobile device management systems.
C14	Identificar vulnerabilidades nos sistemas operativos e aplicacións dos dispositivos móbiles, así como realizar unha análise forense e definir a política de seguridade que afecta ás comunicacións e aos sistemas móbiles dunha organización.
D3	Work as a malware analyst, to protect applications, as well as analyse their security in any application area.
D8	Perform penetration testing in complex practical environments to identify vulnerabilities, as well as to perform attacks in controlled environments with critical and ethical judgement.
D9	Apply forensic investigation methods for the analysis of cybersecurity incidents or risks using scientific and analytical techniques to identify, preserve, analyse and present data that are valid within a legal process.

Expected results from this subject	
Expected results from this subject	Training and Learning Results
Know the fundamental concepts associated with the security in the operative systems mobiles and development of apps safe.	B14 C14
Identify an app with malicious behavior and vulnerabilities in operative systems and apps	C14 D3
Be able to realize a forensic analysis of a mobile device	C14 D8 D9
Know the systems of management of the mobile devices	B14 C14

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 security
Devices security
Network security
Vulnerabilities, exploits and malicious applications
Forensic analysis of mobile operating systems
Enterprise Mobile Management Systems (EMM)

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	9	9	18
Practices through ICT	12	12	24
Objective questions exam	2	14	16
Problem and/or exercise solving	0	5	5
Report of practices, practicum and external practices	0	12	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	The professors of the course present the main theoretical contents related to security in mobile devices. Through this methodology competencies B14 and C14 get developed.
Practices through ICT	Students will complete guided and supervised practices. Through this methodology the competencies C14, D3, D8 and D9 get developed.

Personalized assistance	
Methodologies	**Description**
Practices through ICT	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. The tutorial sessions could also be agreed with the teacher by appointment.
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. The tutorial sessions could also be agreed with the teacher by appointment.

Assessment			
	Description	Qualification	Training and Learning Results
Objective questions exam	Short-questions exam on the theoretical and practical contents reviewed throughout the course, both in the lectures and in the laboratory practices. This exam will be done at the end of the term.	40	
Problem and/or exercise solving	Problem-solving tests where students make use of the acquired knowledge, in both theoretical and practical sessions. This test will be carried out throughout the term, with partial deliveries on the dates indicated by teachers.	25	
Report of practices, practicum and external practices	Students will individually fill questionnaires and/or write practice reports, where the right development and understanding of the practice get probed.	35	

Other comments on the Evaluation

ORDINARY EXAM

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

Before the end of the fourth week of the course, students must declare if they opt for the continuous assessment or the global 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.

Global 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 term. To pass the course the final grade must be greater or equal to five.

EXTRAORDINARY EXAM

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, Jonh Wiley & Sons, 2015
Complementary Bibliography
Joshua Drake, **Android hacker's handbook**, 1, Jonh Wiley & Sons, 2014
Charles Miller, **iOS hacker's handbook**, 1, Jonh Wiley & Sons, 2013
Abhishek Dubey, Anmol Misra, **Android security: attacks and defenses**, 1, CRC Press, 2013
David Thiel, **iOS application security: the definitive guide for hackers and developers**, 1, No Starch Press, 2016
Nikolay Elenkov, **Android security internals: an in-depth guide to Android's security architecture**, 1, No Starch Press, 2015
Andrew Hoog, **iPhone and iOS forensics: investigation, analysis, and mobile security for Apple iPhone, iPad, and iOS devices**, 1, Syngress/Elsevier, 2011

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.

IDENTIFYING DATA				
Smart Contracts and dApps				
Subject	Smart Contracts and dApps			
Code	V05M175V11219			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd
Teaching language	Spanish			
Department				
Coordinator	Fernández Iglesias, Manuel José			
Lecturers	Álvarez Sabucedo, Luis Modesto Fernández Iglesias, Manuel José			
E-mail	manolo@uvigo.es			
Web				
General description	This course offers students an introductory understanding of the concepts and practices related to the development and deployment of secure smart contracts and decentralized applications. Students will explore the specificities of smart contract programming, and examine various security vulnerabilities and threats specific to smart contracts and decentralized applications. Through hands-on exercises, real-world case examples and classroom discussions, students will learn how to employ best practices to mitigate risks and protect against attacks in the blockchain ecosystem. By the end of the course, students will be equipped with the knowledge and skills to develop secure smart contracts and design resilient decentralized applications that can withstand the challenges of these technologies.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Basic concepts	Discussion of the basic concepts related to the development of smart contracts and decentralized applications.
Design and development of smart contracts	The development of smart contracts is addressed, taking into account the most relevant security aspects.
Peer-to-peer file systems	The basic characteristics of peer-to-peer networks are presented, followed by a description of the essential elements of decentralized file systems and their relationship with blockchain technologies. IPFS is presented as a case study.
Non-fungible tokens	A specific use case very popular in the world of smart contracts and decentralized applications is discussed: non-fungible tokens or NFTs.
Oracles. Good practices	Oracles are presented as third-party services that provide external data or events to a smart contract in a blockchain. Best practices for their development and use are identified.
Cybersecurity aspects	A recap of the key elements for designing secure smart contracts, oracles and decentralized applications is offered.

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	11.5	24.5	36
Practices through ICT	2.5	6	8.5
Practices through ICT	4	9	13
Practices through ICT	4	9	13
Objective questions exam	1.5	3	4.5
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies
Description

Lecturing	Theoretical concepts and their practical application will be presented in class. Students will be encouraged to participate in the resolution of practical cases (case studies), in such a way that in each class session the teacher's presentation will be combined with the students' participation.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.
Practices through ICT	Small projects or programming exercises of smart contracts or decentralized applications will be proposed, to be carried out in the laboratory and/or through autonomous work, under the supervision of the teacher. Reference platforms and languages in the field of blockchain will be utilized.

Personalized assistance

Methodologies	Description
Lecturing	Students will have the opportunity to attend personalized tutorial sessions in accordance with the procedure that will be established for this purpose at the beginning of the semester. This procedure will be published on the course website.
Practices through ICT	Students will have the opportunity to attend personalized tutorial sessions in accordance with the procedure that will be established for this purpose at the beginning of the semester. This procedure will be published on the course website.

Assessment

	Description	Qualification	Training and Learning Results
Practices through ICT	The solution offered to the first course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	10	
Practices through ICT	The solution offered to the second course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	25	
Practices through ICT	The solution offered to the third course assignment will be evaluated, taking into account the correctness of the proposed solution, the quality of the code, the efficiency of the code, the problem-solving skills and the documentation of the code.	25	
Objective questions exam	Each student will sit, individually and without any supporting material, a classroom exam at the end of the semester (the exact date will be published at the beginning of the semester at the course web) on the totality of the course syllabus.	40	

Other comments on the Evaluation

There are two assessment modalities, continuous assessment (CA) and global assessment (GA), which must be chosen by the students considering the following conditions:

- Both the classroom and lab parts will be evaluated according to the same mechanism, CA or GA, as selected by the student.
- CA includes the exams described in the previous section: one classroom exam, and design and development of three programming assignments.
- Students will confirm the final evaluation modality (CA or GA) when submitting lab deliverables, depending on the submission date.
- Regardless of the chosen evaluation modality, lab assignments will always be carried out individually.
- A minimum grade of 2 points in both theory/classroom (out of 4) and lab parts (out of 6) is required to pass the course.
- If the grade resulting from adding the classroom and lab grades is equal or higher than 5 points, but the student does not reach the minimum grade required in any of them, his/her final grade will be Fail (4.5).
- If a student attends any of the evaluation tests of the course, he/she will not be able to appear in transcripts as "no-show".
- The CA tests will only take place on the dates established by the lecturers, and cannot be resit or delayed.

- 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.

Assessment procedure for the ordinary call for students who opt for Continuous Assessment (CA)

- **Theory/classroom part (40%)**: The grade of this part (4 points) corresponds to an individual exam without any type of supporting material at the end of the academic semester (on the date approved by the school).
- **Lab part (60%)**: The grade for this part depends on the grades obtained in each lab assignment (up to 1, 2,5 and 2,5 points respectively, up to 6 points in total).

Students who do not pass the course in the ordinary opportunity, may redeem the grade obtained in both theory and lab for the extraordinary opportunity, as long as they have achieved the minimum grade required in the part they wish to keep (2 points out of 4 and 2 points out of 6 respectively).

Assessment procedure for the ordinary call for students who opt for Global Assessment (GA):

- **Classroom part (40%)**: The grade of this part (4 points) corresponds to an individual exam without any type of supporting material at the end of the academic semester (on the date approved by the school).
- **Lab part (60%)**: The grade for this part depends on the grades obtained in the three assignments (up to 1, 2,5 and 2,5 points respectively, up to 6 points in total). The deliverables may be identical to those required in CA or include modifications in the functionalities to be developed. They will be delivered in digital format and will be evaluated by lecturers outside lab sessions.

Assessment procedure for the extraordinary call and end-of-program call:

- **Classroom part (40%)**. Individual exam on the date to be approved by the school, requiring a minimum grade of 2 points (out of 4).
- **Lab part (60%)**. The corresponding assignments must be submitted in digital. Assignments may be the same CA/GA assignments or may include modifications in functionality and/or scoring. As there is no CA, assessment procedures are the same as as ordinary call's GA.

Sources of information

Basic Bibliography

Lorne Lantz e Daniel Cawrey, **Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications**, O□Reilly Media., 2020

Daniel Drescher, **Blockchain Basics:A Non-Technical Introduction in 25 Steps**, Apress, 2017

Don Tapscott e Alex Tapscott, **Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World**, New enlarged edition, Penguin Publishing Group, 2018

Paul Vigna e Michae lJ. Case, **The Truth Machine: The Blockchain and the Future of Everything**, Harper Collins, 2019

Manuel J. Fernández Iglesias, **Introduction to Blockchain, Smart Contracts and Decentralized Applications**, 2023

Complementary Bibliography

Andreas M. Antonopoulos, **The Internet of Money**, CreateSpace Independent Publishing Platform, 2016

Ethereum.org, **Ethereum Development Tutorials**, 2023

Bina Ramamurthy, **Blockchain Basics**, Coursera, 2023

Mark Parzygnat, **IBM Blockchain 101: Quick-start guide for developers**, IBM Developer, 2023

Recommendations

Subjects that it is recommended to have taken before

Distributed ledger and Blockchain technologies/V05M175V11113

IDENTIFYING DATA				
Information security management				
Subject	Information security management			
Code	V05M175V11301			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	2nd	1st
Teaching language	#EnglishFriendly Spanish Galician			
Department				
Coordinator	Caeiro Rodríguez, Manuel			
Lecturers	Caeiro Rodríguez, Manuel Fernández Vilas, Ana			
E-mail	mcaeiro@det.uvigo.es			
Web	http://http://moovi.uvigo.es			
General description	In this subject enter the fundamental concepts related with the management of the security of the information (and.G. Vulnerability, threat, risk) and study the methodologies, tools and specifications that occupy of the analysis of risks and of the development of systems of management of security of the information. They treat also the systems of answer to incidents, recovery of disasters and continuity of business.			

Training and Learning Results	
Code	
B16	Describe the fundamental concepts and technical regulations related to Information Security Management, Risk Analysis methodologies, as well as the tools to carry out risk analysis tasks, security auditing, incident management, business continuity management and recoveries.
C16	Manage information security, use risk analysis tools and security auditing, proactively identify and classify possible incidents and define the channels for their management and resolution.
D11	Design, implement and maintain an information security management system using reference methodologies, analyse risks, plan incident or disaster detection and recovery periods, develop a business continuity plan, certify secure systems and perform security auditing of systems and facilities.
D14	Project, model, calculate and design technical and management solutions for information security, networks and/or communications systems in all fields of application, with ethical criteria of responsibility and professional ethics.

Expected results from this subject	Training and Learning Results
Know the fundamental concepts related with Information security management: vulnerability, threat, risk, control, politics of security, plan of security, audit	B16
Know the different methodologies of Information Security Management commonly accepted	C16 D11
Know the own tools to carry out tasks related with the risk analysis and the audit of security, as well as know which are the most adapted to each context	C16 D11
Develop and evaluate incident response, disaster response and business continuity.	D14

Contents	
Topic	
Foundations	Basic concepts Legal Frame Normalisation Relevant entities
Analysis of risks, management and certification:	Methodologies Tools for risk analysis
Information Security Management Systems	ISO 27000 Family Esquema Nacional de Seguridad Audit
Business continuity	Roles Typical Sequence of an attack Resilience Contingency plans

Incident detection and response management	Intrusion detection and prevention system Incident response Incident notification
Disaster recovery	Disaster recovery plan Technological architectures for disaster recovery

Planning			
	Class hours	Hours outside the classroom	Total hours
Lecturing	19.5	28	47.5
Mentored work	0.5	5	5.5
Laboratory practical	15	20	35
Objective questions exam	2	20	22
Case studies	5	10	15

*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 of subject topics during the A sessions. With this methodology work the competitions: B16, C16, D11 and D14
Mentored work	Each student individually will make a report on one of the topics of the subject. With this methodology will work the competitions B16 and C16
Laboratory practical	In the laboratory students working in groups will develop lab practices. With this methodology will work the competitions D11 and D14

Personalized assistance

Methodologies	Description
Mentored work	Teachers of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. The doubts will attend of face-to-face form or on line (during lecture hours, or during the time established for the tutoring sessions). The schedule of tutoring sessions will be established at the beginning of the course and will be published in the web page of the subject.
Laboratory practical	Teachers of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. The doubts will attend of face-to-face form or on line (during lab hours, or during the time established for the tutoring sessions). The schedule of tutoring sessions will be established at the beginning of the course and will be published in the web page of the subject.
Tests	**Description**
Case studies	Teachers of the subject will provide individual and personalized attention to the students during the course, solving their doubts and questions. The doubts will attend of face-to-face form or on line (during lab hours, or during the time established for the tutoring sessions). The schedule of tutoring sessions will be established at the beginning of the course and will be published in the web page of the subject.

Assessment

	Description	Qualification	Training and Learning Results		
Mentored work	Each student individually will make a work on one of the subjects of the subject to present it during the lecture session.	10	B16	C16	
Laboratory practical	Students will develop at least two practices, one on the development of a ISMS including an analysis of risks and another on management of incidents.	40			D11 D14
Objective questions exam	Examination of theoretical knowledge and of practical development	40	B16	C16	D11 D14
Case studies	Students will develop a practical case in the part of laboratory in relation with the management of incidents and business continuity	10			D11 D14

Other comments on the Evaluation

Sources of information

Basic Bibliography

Cess van der Wens, **ISO 27001 ISMS Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses**, 979-8852486288, 2023

Ester Chicano Tejada, **Gestión de incidentes de seguridad informática**, 9788411036191, IC Editorial, 2023

Complementary Bibliography

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements, ISO, 2022

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls, ISO, 2022

ISO 22301:2019 Security and resilience Business continuity management systems Requirements, ISO, 2019

Recommendations

Subjects that are recommended to be taken simultaneously

Concepts and laws/V05M175V11302

IDENTIFYING DATA				
Concepts and laws				
Subject	Concepts and laws			
Code	V05M175V11302			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	4	Mandatory	2nd	1st
Teaching language	Spanish Galician English			
Department				
Coordinator	Rodríguez Vázquez, Virgilio			
Lecturers	Rodríguez Vázquez, Virgilio			
E-mail	virxilio@uvigo.es			
Web	http://moovi.uvigo.gal/			
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.			

Training and Learning Results	
Code	
B17	Analyse the technical and legal regulations applicable to cybersecurity, their implications in the design of systems, in the use of security tools and in the protection of information.
C17	Analyse and communicate the legal regulations related to cybersecurity, its ethical-legal issues and cybercrime in the national, European and international context.
C18	Know how to apply acquired knowledge and problem-solving skills in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of study.
C19	Know how to communicate their conclusions - and the ultimate knowledge and rationale behind them - to specialised and non-specialised audiences in a clear and unambiguous way.
D15	Communicate knowledge and findings, and the ultimate reasons behind them, to specialist and non-specialist audiences in a clear and unambiguous way.
D19	Apply the gender perspective in the different fields of knowledge and in professional practice with the aim of achieving a fairer and more egalitarian society.

Expected results from this subject	
Expected results from this subject	Training and Learning Results
Analyse the technical and legal regulations applicable to cybersecurity, their implications in the design of systems, in the use of security tools and in the protection of information.	B17
Analyse and communicate the legal regulations related to cybersecurity, its ethical-legal issues and cybercrime in the national, European and international context.	C17
Know how to apply acquired knowledge and problem-solving skills in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of study.	C18
Know how to communicate their conclusions - and the ultimate knowledge and rationale behind them - to specialised and non-specialised audiences in a clear and unambiguous way.	C19
Communicate knowledge and findings, and the ultimate reasons behind them, to specialist and non-specialist audiences in a clear and unambiguous way.	D15
Apply the gender perspective in the different fields of knowledge and in professional practice with the aim of achieving a fairer and more egalitarian society.	D19

Contents	
Topic	
1. Introduction to Cybersecurity Law. Review of regulations regarding computer security and risk management.	1.1. EU regulations. 1.2. The National Security Law: the national cybersecurity strategy and the national security scheme.
2. Ethical-legal issues related to cybersecurity.	2.1. Legal limits on the use of information technologies in cybersecurity matters. Rights that may be affected: freedom, privacy, dignity. 2.2. Ethical limits in cybersecurity. 23. Problems related to the use of new technologies: facial recognition, blockchain, web crawling.

3. Special problems of computer crimes in the context of the general part of criminal law.	3.1. The place of commission of the crime. 3.2. The moment of commission of the crime. 3.3. The plurality of subjects. 3.4. Testing problems. 3.5. The difficulties in their investigation and prosecution. Brief reference to extradition.
4. The violation of cybersecurity through criminal conduct.	4.1. Terminological precisions: computer crimes and cybercrime. 4.2. The use of ICT to commit crimes and when ICT is the object of the crime. 4.3. The Spanish Penitentiary Code, LO 10/1995, of November 23, the European Directive 2013/40/EU of the European Parliament and of the Council, of August 12, 2013, relating to attacks against information systems, Convention on cybercrime o Budapest Convention, of the Council of Europe, of November 23, 2001.
5. Cybercrimes of discovery and disclosure of secrets	5.1. Crimes of discovering and disclosing secrets (I). Frequent risks: ransomware and the theft of information. 5.2. 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...). 5.3. 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. 5.4. Crimes against privacy and an individuals right to their own image: the undue use of cookies
6. Cybercrimes against property.	6.1. Crimes against property (I). Scams committed via computer. Producing, possessing or facilitating computer programs used for this purpose. 6.2. Crimes against property (II). Fraud using a third-party telecommunication signal. Use of telecommunication terminal without the owners consent. 6.3. 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 operators 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.
7. Cybercrimes against collective rights.	7.1. Crimes against intellectual and industrial property. Through the provision of information society services or through an Internet access portal. 7.2. 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. 7.3. Crimes against public faith: electronic lies.
8. Crimes committed against persons using communication techniques.	8.1. Crimes against freedom. Threats using social networks or other ICT. Cyber stalking. 8.2. Crimes against the sexual freedom and indemnity. Child grooming and child pornography. 8.3. Crimes against intimacy and privacy. 8.4. Crimes against honour. Harming a persons digital reputation.
9. Cyberterrorism.	9.1. Concept. 9.2. Computing crimes carried out with the specific purpose of art. 573 of the Criminal Code. 9.3. Crime of collaborating with a terrorist group or organisation through the provision of technological services.
10. Crimes relating to national Defence and others.	Brief approximation.
11. Criminological approach to computing.	11.1. Statistical sources: main national and international organisms, crimes. 11.2. Analysis of the main reports on cybersecurity. 11.3. Identification of the main technological resources used.

12. Analysis of Spanish caselaw in relation to computing crimes.	12.1. Special attention to the caselaw of the Supreme court. 12.2. Agreements of the non-jurisdictional plenary of the Second Chamber of the Supreme Court relating to computing crimes. 12.3. The Prosecution Service and the Prosecutor□s Office specialising in computer criminality.
13. Protection of personal data	13.1. EU regulation. Regulation (EU) 2016/679 of April 27, 2016, General Data Protection Regulation (RGPD). 13.2. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation). 13.3. The Organic Law of Data Protection and the Development Regulation. 13.4. The personal data protection agency. 13.5. Compliance programs in the field of personal data protection.

Planning

	Class hours	Hours outside the classroom	Total hours
Lecturing	12	32	44
Laboratory practical	13	22	35
Objective questions exam	3	0	3
Problem and/or exercise solving	2	0	2

*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 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.).

Personalized assistance

Methodologies	Description
Lecturing	The students will have lectures as shown on the timetable published on the website for the Master□s Degree. It will be able to attended, previous appointment -by email-, or well through email or well through virtual dispatch in the remote campus.
Laboratory practical	The students will have lectures as shown on the timetable published on the website for the Master□s Degree. It will be able to attended, previous appointment -by email-, or well through email or well through virtual dispatch in the remote campus.

Assessment

Description	Qualification	Training and Learning Results

Objective questions exam	The continuous assessment system will consist of three written exams. 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). The multiple choice objective questions exam: - 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. - each examination will comprise the part of the program that is indicated at the start of the term by the subject coordinator. - 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. - 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). 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), he/she will score 0 points for this/these exam(s).	50	B17 C17 D15 C18 D19 C19
Problem and/or exercise solving	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). The examination corresponds to problem solving: - 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 2022-2023 academic year - It will consist of solving one or several practical cases and will be marked with a score of 0 to 5 points - The problems posed by the practical cases may affect the issues covered in the course syllabus. - It will be worth 50% of the final mark, with the remaining 50% corresponding to the two multiple choice objective questions exams. 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), he/she will score 0 points for this/these exam(s).	50	B17 C17 D15 C18 D19 C19

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.

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 deduced 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.

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 subtracted 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

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

Complementary Bibliography

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

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

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

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 arículo 286 CP**, 1.ª, Difusión Jurídica y Temas de actualidad, 2006

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

DAVARA RODRÍGUEZ, Miguel Ángel, **Manual de derecho informático**, 11.ª, Thomson-Aranzadi, 2015

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

DE URBANO CASTRILLO, Eduardo et al., **Delincuencia informática : tiempos de cautela y amparo**, 1.ª, Aranzadi, 2012

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MORÓN LERMA, Esther, **Internet y derecho penal : "hacking" y otras conductas ilícitas en la red**, 2.ª, Aranzadi, 2002

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

ORENES, Eduardo, **Ciberseguridad familiar : cyberbullying, hacking y otros peligros en Internet**, 1.ª, Círculo Rojo, 2013

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

QUERALT JIMÉNEZ, Joan Josep, **Derecho penal español. Parte especial**, 7.ª, Tirant lo Blanch, 2015
QUINTERO OLIVARES, Gonzalo (dir.), **Comentarios a la Parte especial del Derecho penal**, 10.ª, Aranzadi, 2016
RALLO LOMBARTE, Artemi, **El derecho al olvido en Internet : Google**, 1.ª, Centro de Estudios Políticos y Constitucionales, 2014
RODRÍGUEZ MESA, M.ª José, **Los delitos de daños**, 1.ª, Tirant lo Blanch, 2017
ROMEO CASABONA, Carlos M.ª (coord.), **El Cibercrimen : nuevos retos jurídico-penales, nuevas respuestas político-criminales**, 1.ª, Comares, 2006
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
SAIN, Gustavo, **Delitos informáticos : investigación criminal, marco legal y peritaje**, 1.ª, B de f, 2017
SÁINZ PEÑA, Rosa M.ª (coord.), **Ciberseguridad, la protección de la información en un mundo digital**, 1.ª, Fundación Telefónica, Ariel, 2016
SEGURA SERRANO, Antonio/GORDO GARCÍA, Fernando (coords.), **Ciberseguridad global : oportunidades y compromisos en el uso del ciberespacio**, 1.ª, Universidad de Granada, 2013
SILVA SÁNCHEZ, Jesús María (dir.)/RAGUÉS I VALLÉS, Ramón (coord.), **Lecciones de Derecho penal: Parte especial**, 5.ª, Atelier, 2018
SINGER, Peter Warren, **Cybersecurity and cyberwar : what everyone needs to know**, 1.ª, Oxford University Press, 2014
TOURIÑO, Alejandro, **El derecho al olvido y a la intimidad en Internet**, 1.ª, Los Libros de la Catarata, 2014
VALLS PRIETO, Javier, **Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial**, 1.ª, Dykinson, 2017
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
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
WALDEN, Ian, **Computer crimes and digital investigations**, 1.ª, Oxford University Press, 2007

Recommendations

Subjects that are recommended to be taken simultaneously

Information security management/V05M175V11301

IDENTIFYING DATA				
Business practice				
Subject	Business practice			
Code	V05M175V11303			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	9	Mandatory	2nd	1st
Teaching language	Spanish			
Department				
Coordinator	Marcos Acevedo, Jorge			
Lecturers	Marcos Acevedo, Jorge			
E-mail	acevedo@uvigo.es			
Web	http://www.munics.es/			
General description	(*)La misión del máster es formar profesionales de alta cualificación en todos los procesos técnicos, organizativos, operativos y forenses relativos a la seguridad digital. El profesorado pertenece a las áreas de Ingeniería Telemática, Teoría de la Señal y Comunicaciones, Ciencias de la Computación e Inteligencia Artificial, Ingeniería de Sistemas y Derecho Penal de las dos universidades, y se complementa con la contribución de destacados profesionales de empresas del sector en Galicia y el compromiso de éstas en apoyar las prácticas de los estudiantes.			

Training and Learning Results	
Code	
B1	Knowledge of the basic methods and techniques of classical cryptography, cryptographic security standards and protocols, steganography and post-quantum encryption.
B2	To learn about malware stealth and persistence techniques, as well as current malware trends through the study of real cases.
B3	Identify privacy attack methods and the concepts of privacy preservation and anonymity: differential privacy, homomorphic encryption and secure multi-party computing.
B4	Distinguish the main vulnerabilities suffered by applications, as well as the main authentication, authorisation and access control mechanisms, with special emphasis on web applications and web services.
B5	Knowledge of vulnerabilities in network access devices and technologies, tools to scan for them and protective measures for secure communications networks, as well as understanding the concept of security policy as applied to networks, perimeter security and firewalls.
B6	Understand the basic concepts and general functioning of distributed log-based technologies; as well as their assessment in terms of confidentiality, integrity and availability; and their main applications and use cases.
C1	Determine the degree of security of a cryptographic solution, choose the most appropriate one for an information or communications system, as well as implement and adapt its elements.
C2	Detect and eliminate vulnerabilities susceptible to malware, as well as malware, in communication systems and networks, as well as evade malware stealth and persistence techniques.
C3	Choosing the most appropriate privacy and anonymisation solution for an information or communications system, as well as knowing how to apply and adapt privacy and anonymisation elements to a product, service or information and communications system according to the needs and taking into account the trade-off between information utility and data privacy.
C4	Preventing, identifying and correcting the main vulnerabilities suffered by applications, as well as incorporating authentication, authorisation and access control mechanisms for applications.
C5	Design and implement secure networks, selecting and configuring the appropriate devices for each section of the network and proactively using network monitoring so that the organisation is correctly implemented.
C6	Apply distributed logging technologies to specific use cases, as well as design, develop and deploy a solution based on these technologies, optimising its essential parameters and applying protection mechanisms to prevent and mitigate attacks.
C7	Decide on the appropriate solution/protocol to ensure end-to-end communications security, as well as configure the different tools provided by the different operating systems/platforms to activate communications security.
C8	Identify the vulnerabilities of an OS in a specific usage environment, modify the configuration to minimise its exposure and test its security level.
C9	Analyse the security implications of technologies related to the digitisation of production sectors, as well as assess and model threats and execute attacks in order to design secure IoT systems.
C10	Identify and exploit, in an analytical and practical way, vulnerabilities in information systems, as well as identify possible attack vectors and innovate in techniques and processes related to ethical hacking.
C11	Assessing a company in the field of security and even more specific sectors within this field, as well as defining the necessary profiles, whether in-house or external, associated with cybersecurity.
C12	Identify, preserve and analyse evidence, perform forensic analysis of an information system, and generate reports that are clear, concise and intelligible to experts and non-experts alike.

C13	Apply infrastructure virtualisation tools in Data Processing Centres, as well as use tools for monitoring their infrastructures and services.
C14	Identificar vulnerabilidades nos sistemas operativos e aplicacións dos dispositivos móbiles, así como realizar unha análise forense e definir a política de seguridade que afecta ás comunicacións e aos sistemas móbiles dunha organización.
C15	Apply smart contracts to the development of decentralised systems, assess whether a development is appropriate to the problem and use appropriate development tools to programme, deploy and interact with smart contracts, as well as use oracles under robust and secure conditions.
C16	Manage information security, use risk analysis tools and security auditing, proactively identify and classify possible incidents and define the channels for their management and resolution.
C17	Analyse and communicate the legal regulations related to cybersecurity, its ethical-legal issues and cybercrime in the national, European and international context.
C18	Know how to apply acquired knowledge and problem-solving skills in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of study.
C19	Know how to communicate their conclusions - and the ultimate knowledge and rationale behind them - to specialised and non-specialised audiences in a clear and unambiguous way.
D1	Solve problems related to the use of encrypted information and have the autonomy and initiative to develop innovative solutions in the fields of cryptography, cryptanalysis, anonymisation and privacy.
D2	Demonstrate autonomy and initiative to solve complex problems involving multiple technologies in the field of communications networks or systems, and develop innovative solutions in the field of private communications and distributed computing.
D3	Work as a malware analyst, to protect applications, as well as analyse their security in any application area.
D4	Applying blockchain technology to the verifiable decentralised protection of information, be it digital information assets or digital assets representing goods of use.
D5	Analyse the security of communication protocols at the physical, link, network and transport layers, as well as evaluate the security measures that need to be implemented in a corporate network to protect its internal assets and communications.

Expected results from this subject

Expected results from this subject	Training and Learning Results
Experience in the practice of the cybersecurity profession and its usual functions in some real company environment.	B1 B2 B3 B4 B5 B6 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 D1 D2 D3 D4 D5

Contents

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

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

Planning

	Class hours	Hours outside the classroom	Total hours
Practicum, External practices and clinical practices	220	5	225

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

Methodologies

	Description
Practicum, External practices and clinical practices	Stay in a company developing functions of a Master Degree in Cybersecurity so that they can put into practice the knowledge and skills acquired, to complete their academic training.

Personalized assistance

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

Assessment

	Description	Qualification	Training and Learning Results		
Practicum, External practices and clinical practices	(*)Prácticum, Practicas externas y clínicasPrácticas externas La evaluación se realizará en función de: 1) La memoria de actividades 2) La evaluación del tutor en la empresa	100	B1 B2 B3 B4 B5 B6	C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19	D1 D2 D3 D4 D5

Other comments on the Evaluation

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

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

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

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

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

Sources of information
Basic Bibliography
Complementary Bibliography

Recommendations

IDENTIFYING DATA				
Final Master's Project				
Subject	Final Master's Project			
Code	V05M175V11304			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	12	Mandatory	2nd	1st
Teaching language	Spanish Galician			
Department				
Coordinator	Caeiro Rodríguez, Manuel			
Lecturers	Caeiro Rodríguez, Manuel			
E-mail	mcaeiro@det.uvigo.es			
Web	http://moovi.uvigo.es			
General description	(*)O Traballo Fin de Máster (TFM) é un traballo académico, persoal e orixinal que se debe presentar en público e que é avaliado por un tribunal. Trátase dun proxecto no que o estudante ten que mostrar os coñecementos adquiridos durante o mestrado. Debe concluir coa redacción por escrito dun conxunto de explicacións, teorías, ideas, razoamentos, descrición de desenvolvementos ou deseños, etc. sobre unha temática elixida polo alumno, e supervisada por un titor ou titores, que velarán pola súa progresión e polo nivel de calidade. Non obstante, o Traballo Fin de Máster é responsabilidade única do aspirante ao título de máster.			

Training and Learning Results
Code

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
The Master's Thesis is an academic, personal and original work in which the student has to show the knowledge obtained during the master. Therefore, the content of each work must be unique. Nevertheless, it must show the ability of the student to analyze a problem in a systematic way, propose solutions, analyze the results obtained and expose them clearly.	1. Objectives 2. Methodology and planning 3. Previous work (current situation, standards, etc.) 4. Results and technical-scientific contributions 5. Conclusions 6. Bibliography 7. Drafting of the report 8. Oral presentation

Planning			
	Class hours	Hours outside the classroom	Total hours
Mentored work	0	275	275
Presentation	1	24	25
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

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

Personalized assistance	
Methodologies	**Description**

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

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

Assessment

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

Other comments on the Evaluation

Sources of information

Basic Bibliography

Complementary Bibliography

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

Recommendations