



## (\*)Escola de Enxeñaría de Telecomunicación

### (\*)Páxina web

(\*)

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

Secretaría e Subdirección de Novas Titulacións: Pedro Rodríguez Hernández

([teleco.subdir.secretaria@uvigo.gal](mailto:teleco.subdir.secretaria@uvigo.gal);[teleco.subdir.novastitulacions@uvigo.gal](mailto: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'S DEGREE 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 IN CYBERSECURITY

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 IN INDUSTRIAL MATHEMATICS

Generalcoordinator: Elena Vázquez Cendón (USC)

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

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

#### INTERNATIONAL MASTER IN COMPUTER VISION

General coordinator: Xose Manuel Pardo López (USC)

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

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

#### MASTER'S DEGREE IN 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<br>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 |                                                                                                                                                                                                          |
| B1   | Knowledge of the basic methods and techniques of classical cryptography, cryptographic security standards and protocols, steganography and post-quantum encryption.                                      |
| 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.                  |
| 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. |
| D13  | Apply acquired knowledge and problem-solving skills in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of study.                                     |

### Expected results from this subject

| Expected results from this subject                                                                                                                 | Training and Learning Results |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Understand and be able to apply the fundamental cryptographic primitives                                                                           | B1                            |
| Understand and be able to apply the main standards in symmetric, asymmetric, and post-quantum cryptography, as well as digital signature standards | B1                            |
| Be able to apply the concepts of semantic security to specific use cases across different environments                                             | C1<br>D1                      |
| Learn to develop methods and algorithms for information protection                                                                                 | D1<br>D13                     |

### Contents

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

| <b>Planning</b>                 |             |                             |             |
|---------------------------------|-------------|-----------------------------|-------------|
|                                 | Class hours | Hours outside the classroom | Total hours |
| Problem solving                 | 0           | 24                          | 24          |
| Laboratory practical            | 19          | 23                          | 42          |
| Lecturing                       | 19          | 36                          | 55          |
| 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.

| <b>Methodologies</b> |                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Description                                                                                                                                                                                                                                              |
| Problem solving      | Students are supposed to solve problems and exercises about the course 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. <a href="https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga">https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga</a>                                                                   |
| Laboratory practical | Individual assistance will be given to the students who request guidance on the programming assignments or computer lab practice. <a href="https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga">https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga</a>                                                        |
| 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. <a href="https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga">https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga</a> |

| <b>Assessment</b>    |                                                                                                 |               |                               |
|----------------------|-------------------------------------------------------------------------------------------------|---------------|-------------------------------|
|                      | 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.

For every assessment type and opportunity, a minimum grade of 3 over a scale of 10 points in the written exam is mandatory for passing the course. Should the student not achieve this grade, his/her final grade in the course will be Fail (3.0)

---

### 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.

Use of generative AI tools in the coursework will be especially monitored and controlled by the instructors.

| 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                                                                                                                                                                                                     | #EnglishFriendly<br>Spanish                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
| Department                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |      |            |
| Coordinator                                                                                                                                                                                                           | Burguillo Rial, Juan Carlos                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
| Lecturers                                                                                                                                                                                                             | Burguillo Rial, Juan Carlos<br>Mikic Fonte, Fernando Ariel<br>Rivas López, Jose Luis                                                                                                                                                                                                                                                                                                                                            |           |      |            |
| E-mail                                                                                                                                                                                                                | jrial@uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                  |           |      |            |
| Web                                                                                                                                                                                                                   | http://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

| Expected results from this subject                                                                                            | Training and Learning Results |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| To provide the student the capability to analyze, detect and erase malware.                                                   | B2<br>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?<br>b) How to detect and erase it?<br>c) What is malware engineering?                  |
| Malware types and definitions.                    | a) Structure.<br>b) Components.<br>c) Infection vectors.                                                  |
| Malware Engineering.                              | a) Propagation techniques.<br>b) Infection processes.<br>c) Malware persistence.<br>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.<br>b) Tools for malware erasing.                                          |

### Planning

|                                 | Class hours | Hours outside the classroom | Total hours |
|---------------------------------|-------------|-----------------------------|-------------|
| Introductory activities         | 2           | 2                           | 4           |
| Lecturing                       | 15          | 25                          | 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 ( <a href="https://moovi.uvigo.gal">https://moovi.uvigo.gal</a> ). |
| 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 ( <a href="https://moovi.uvigo.gal">https://moovi.uvigo.gal</a> ). |
| 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 ( <a href="https://moovi.uvigo.gal">https://moovi.uvigo.gal</a> ). |
| 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 ( <a href="https://moovi.uvigo.gal">https://moovi.uvigo.gal</a> ). |
| 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 ( <a href="https://moovi.uvigo.gal">https://moovi.uvigo.gal</a> ). |

| 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 ( $2 \times 15\% = 30\%$ ) + 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.

After any assessment, teaching staff may call students for oral verification interviews, either at random or where there are indications of cheating, unauthorized use of artificial intelligence, or other fraudulent means in completing the exam. Grades

for the assessments shall remain provisional until any such interviews have been completed. During these interviews, students must demonstrate that they possess the knowledge and skills needed to adequately justify the solutions they submitted.

**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

| <b>IDENTIFYING DATA</b>      |                                                                                                                                                                                                                                                                                                                                                                                             |           |      |            |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Privacy and anonymity</b> |                                                                                                                                                                                                                                                                                                                                                                                             |           |      |            |
| 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<br>Spanish                                                                                                                                                                                                                                                                                                                                                                 |           |      |            |
| Department                   |                                                                                                                                                                                                                                                                                                                                                                                             |           |      |            |
| Coordinator                  | Pérez González, Fernando                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| Lecturers                    | Pedrouzo Ulloa, Alberto<br>Pérez González, Fernando                                                                                                                                                                                                                                                                                                                                         |           |      |            |
| E-mail                       | fperez@gts.uvigo.es                                                                                                                                                                                                                                                                                                                                                                         |           |      |            |
| Web                          | 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. |           |      |            |

| <b>Training and Learning Results</b> |                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Code                                 |                                                                                                                                                                                                                                                                                                                                                                      |
| B3                                   | Identify privacy attack methods and the concepts of privacy preservation and anonymity: differential privacy, homomorphic encryption and secure multi-party computing.                                                                                                                                                                                               |
| 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. |
| 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.                                                                                                                                                             |
| 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.                                                                                                                              |

| <b>Expected results from this subject</b>                                        |                               |
|----------------------------------------------------------------------------------|-------------------------------|
| Expected results from this subject                                               | Training and Learning Results |
| To know the different technical alternatives for improving privacy and anonymity | B3<br>C3<br>D1                |
| To design, implement, and validate algorithms to improve privacy and anonymity   | B3<br>C3<br>D14               |

| <b>Contents</b>                              |                                                                                                                                                                                     |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                         |

| <b>Planning</b>      |             |                             |             |
|----------------------|-------------|-----------------------------|-------------|
|                      | 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. The practical results from the first opportunity (within the same academic year) will be maintained, as practices are part of the continuous assessment of the course and, therefore, cannot be retaken.

### 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 Samaraweera, **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'Reilly Media, 2023  
Nishant Bhajaria, **Data Privacy**, Manning Publications, 2022  
PALISADE, **PALISADE HOMOMORPHIC ENCRYPTION SOFTWARE LIBRARY**,  
Ilaria Chillotti, **TFHE Deep Dive**,  
Daniele Micciancio, and Oded Regev, **Lattice-based cryptography**, Springer, 2009

Recommendations

| IDENTIFYING DATA            |                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|
| <b>Application security</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |      |
| Subject                     | Application security                                                                                                                                                                                                                                                                                                                                                                                                                       |           |      |
| Code                        | V05M175V11111                                                                                                                                                                                                                                                                                                                                                                                                                              |           |      |
| Study programme             | Máster Universitario en Ciberseguridad                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |
| Descriptors                 | ECTS Credits                                                                                                                                                                                                                                                                                                                                                                                                                               | Choose    | Year |
|                             | 5                                                                                                                                                                                                                                                                                                                                                                                                                                          | Mandatory | 1st  |
| Teaching language           | Spanish                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |
| Department                  |                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |      |
| Coordinator                 | López Nores, Martín                                                                                                                                                                                                                                                                                                                                                                                                                        |           |      |
| Lecturers                   | López Nores, Martín                                                                                                                                                                                                                                                                                                                                                                                                                        |           |      |
| E-mail                      | mlnores@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                       |           |      |
| Web                         | <a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530104&amp;id_ioma=cast&amp;any_academic=2024_25">http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614530&amp;assignatura=614530104&amp;id_ioma=cast&amp;any_academic=2024_25</a>                                                                                                                  |           |      |
| 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       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |      |            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Secure networks</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |      |            |
| 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              | Rodríguez Rubio, Raúl Fernando                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |      |            |
| E-mail                 | rrubio@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |      |            |
| Web                    | <a href="http://academica.udc.gal/doa/consultaPublica/look%5bconpub%5dMostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202743&amp;idiomaPais=es.ES">http://academica.udc.gal/doa/consultaPublica/look%5bconpub%5dMostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202743&amp;idiomaPais=es.ES</a>                                                                                                                                                                                                            |           |      |            |
| 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                                      |                               |
| <b>Expected results from this subject</b> |                               |
| 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

| <b>IDENTIFYING DATA</b>                               |                                                                                                                                                                                                                                                                     |           |      |            |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Distributed ledger and Blockchain technologies</b> |                                                                                                                                                                                                                                                                     |           |      |            |
| 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                                     | Spanish                                                                                                                                                                                                                                                             |           |      |            |
| Department                                            |                                                                                                                                                                                                                                                                     |           |      |            |
| Coordinator                                           | Fernández Iglesias, Manuel José                                                                                                                                                                                                                                     |           |      |            |
| Lecturers                                             | Álvarez Sabucedo, Luis Modesto<br>Fernández Iglesias, Manuel José                                                                                                                                                                                                   |           |      |            |
| E-mail                                                | manolo@uvigo.es                                                                                                                                                                                                                                                     |           |      |            |
| Web                                                   | <a href="http://academica.udc.gal/doa/consultaPublica/look[conpub]MostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202744">http://academica.udc.gal/doa/consultaPublica/look[conpub]MostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202744</a> |           |      |            |
| General description                                   | In this course, the basic concepts about distributed ledger and blockchain technologies are introduced.                                                                                                                                                             |           |      |            |

### Training and Learning Results

| Code                                      |                               |
|-------------------------------------------|-------------------------------|
| <b>Expected results from this subject</b> |                               |
| 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

| <b>IDENTIFYING DATA</b>        |                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |      |            |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Communications security</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |      |            |
| 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                      | Rodríguez Rubio, Raúl Fernando<br>Suárez González, Andrés                                                                                                                                                                                                                                                                                                                                                                                |           |      |            |
| E-mail                         | rrubio@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                      |           |      |            |
| Web                            | http://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. |           |      |            |

| <b>Training and Learning Results</b> |                                                                                                                                                                                                                                                                                       |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Code                                 |                                                                                                                                                                                                                                                                                       |
| B7                                   | To know in detail the network protocols that provide security for the transmission of information, and to understand which other protocols, being auxiliary (not related to the world of security), present exploitable vulnerabilities and possible countermeasures against 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.                                                         |
| 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.                                  |
| 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.                                  |
| D10                                  | Design and manage infrastructure security to perform infrastructure security auditing and ensure business continuity under reference norms and standards.                                                                                                                             |

| <b>Expected results from this subject</b>                                                                                                                                                                                                                                                                                       |                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Expected results from this subject                                                                                                                                                                                                                                                                                              | Training and Learning Results |
| Understand and assess the security of network protocols and communications: Analyze communication protocols across the different network layers, identify associated vulnerabilities and threats, and evaluate the most appropriate protection and mitigation measures.                                                         | B7<br>D5                      |
| Design, implement, and manage secure communications: Select, configure, and administer security protocols, tools, and mechanisms that ensure the confidentiality, integrity, authenticity, and availability of end-to-end communications across different technological environments.                                           | C7<br>D2                      |
| Audit and solve complex security challenges in communication infrastructures: Apply security analysis, auditing, and management methodologies to protect corporate infrastructures, ensure business continuity, and develop innovative solutions for complex scenarios involving multiple technologies and distributed systems. | D2<br>D10                     |

| <b>Contents</b>                     |                                                                                                                                                                                                                 |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Topic                               |                                                                                                                                                                                                                 |
| Internet architecture and protocols | Fundamental concepts                                                                                                                                                                                            |
| Link level security                 | Wired security/Ethernet networks:<br>Access control and port-based authentication<br>Confidentiality in Ethernet networks<br><br>Wireless Security/WiFi networks:<br>WPA/2/3: Personal &&&& Enterprise security |

|                                  |                                                                                             |
|----------------------------------|---------------------------------------------------------------------------------------------|
| Network level security           | IPsec security protocols<br>IPsec dynamic key management<br>IPsec authentication mechanisms |
| Securing Internet infrastructure | Routing protocols security<br>DNS security<br>TCP security                                  |
| Data transmission security       | The TLS protocol<br>Cryptographic suites<br>WebPKI infrastructure<br>Certificate validation |
| Mobile networks security         | System architecture<br>Association and authentication of the user/terminal<br>Privacy       |

## Planning

|                                                       | Class hours | Hours outside the classroom | Total hours |
|-------------------------------------------------------|-------------|-----------------------------|-------------|
| Lecturing                                             | 21          | 21                          | 42          |
| Laboratory practical                                  | 19          | 15                          | 34          |
| Practices through ICT                                 | 0           | 42                          | 42          |
| Essay questions exam                                  | 2           | 0                           | 2           |
| Report of practices, practicum and external practices | 0           | 5                           | 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             | 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 <a href="https://moovi.uvigo.gal/user/profile.php?id=11315">https://moovi.uvigo.gal/user/profile.php?id=11315</a> Andrés Suárez González <a href="https://moovi.uvigo.gal/user/profile.php?id=11340">https://moovi.uvigo.gal/user/profile.php?id=11340</a> Diego Fernández Iglesias <a href="https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614">https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614</a> |
| 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.<br>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             | D5                            |

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |    |    |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| 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. | 60 |    |
|                                                       | Every challenge or autonomous activity will require a written report, whose structure, composition and readability will affect final mark.                                                                                                                                                                                                                                                                                                                                                                      |    |    |
| 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  | D5 |

### 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.

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

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.

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

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 Inamdard, **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                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------|-------------------------------|
| <b>Systems Fortification</b>                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                               |             |                               |
| E-mail                                                                                                                        | yolanda@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                               |             |                               |
| Web                                                                                                                           | <a href="http://academica.udc.gal/doa/consultaPublica/look%5Bconpub%5DMostrarPubGuiaDocAs?entradaPublica=true&amp;codAsignatura=202746">http://academica.udc.gal/doa/consultaPublica/look%5Bconpub%5DMostrarPubGuiaDocAs?entradaPublica=true&amp;codAsignatura=202746</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                               |             |                               |
| 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. |                               |             |                               |
| <b>Training and Learning Results</b>                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Code                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Expected results from this subject</b>                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Expected results from this subject                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             | Training and Learning Results |
| <b>Contents</b>                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Topic                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Planning</b>                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
|                                                                                                                               | Class hours                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Hours outside the classroom   | Total hours |                               |
| *The information in the planning table is for guidance only and does not take into account the heterogeneity of the students. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Methodologies</b>                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
|                                                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |             |                               |
| <b>Personalized assistance</b>                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Assessment</b>                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Description                                                                                                                   | Qualification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Training and Learning Results |             |                               |
| <b>Other comments on the Evaluation</b>                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Sources of information</b>                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Basic Bibliography</b>                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Complementary Bibliography</b>                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Recommendations</b>                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |

| IDENTIFYING DATA                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| Industrial cybersecurity and IoT |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| Subject                          | Industrial cybersecurity and IoT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |      |            |
| Code                             | V05M175V11213                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |           |      |            |
| Study programme                  | Máster Universitario en Ciberseguridad                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |      |            |
| Descriptors                      | ECTS Credits                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Choose    | Year | Quadmester |
|                                  | 5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Mandatory | 1st  | 2nd        |
| Teaching language                | Spanish<br>Galician                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |      |            |
| Department                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| Coordinator                      | Díaz-Cacho Medina, Miguel Ramón                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| Lecturers                        | Díaz-Cacho Medina, Miguel Ramón<br>Gil Castiñeira, Felipe José                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
| E-mail                           | mcacho@uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| Web                              | http://www.moovi.gal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |           |      |            |
| General description              | <p>Smart devices are increasingly providing us with services almost without us even noticing their presence: the car has ceased to be a simple mechanical machine and has become a connected system with enormous electronic control; in hotels we no longer use a key, but can open our room with a card or our mobile phone; our domestic thermostats can connect to a weather forecast service and adjust to the weather in the next few hours.</p> <p>Industrial environments are particularly important use cases, as the networking of devices that measure and control processes enables Industry 4.0.</p> <p>These are all examples of the applications enabled by "embedded" technologies, wireless communication networks and ultimately the "Internet of Things" (IoT). This course looks at the issues and best practices for making these types of systems secure, with a particular emphasis on the security of Industry 4.0 technologies such as IoT/IoT systems, robotic systems, cloud/edge computing, augmented reality, blockchain or AGVs.</p> |           |      |            |

| Training and Learning Results |                                                                                                                                                                                                                                                      |  |  |  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|
| Code                          |                                                                                                                                                                                                                                                      |  |  |  |
| B9                            | Identify the architecture of IoT systems, their complexity and vulnerabilities, and understand security in the field of embedded systems and IoT communication systems.                                                                              |  |  |  |
| 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.                                                  |  |  |  |
| 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. |  |  |  |
| 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. |  |  |  |
| D7                            | Apply security policies and implement different protection techniques based on an understanding of attacks on industrial systems to minimise security issues and attacks on industrial control networks.                                             |  |  |  |

| Expected results from this subject                                                                                                             |                               |    |                |  |
|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----|----------------|--|
| Expected results from this subject                                                                                                             | Training and Learning Results |    |                |  |
| RA01. Comprise the security policies and his implications in industrial environments.                                                          | B9                            | C9 | D7             |  |
| RA02. Comprise the different techniques of protection and attack in industrial systems and knowing how they can be implemented.                | B9                            | C9 | D2<br>D5<br>D7 |  |
| RA03. Understand the security issues and the attacks to networks of industrial control and knowing the mechanisms that allow to minimise them. | B9                            | C9 | D5<br>D7       |  |
| RA04. Know and identify the architecture of the IoT systems, his complexity and his vulnerabilities                                            | B9                            |    |                |  |
| RA05. Comprise the security in the frame of embeded systems.                                                                                   | B9                            | C9 | D2<br>D5<br>D7 |  |
| RA06. Comprise the security in frame of IoT communications.                                                                                    | B9                            | C9 | D5             |  |
| RA07. Knowing real cases of attacks to IoT systems.                                                                                            | B9                            |    | D7             |  |
| RA08. Be able to comprise the implications to level of security of technologies related with concepts like the Industry 4.0/5.0.               | B9                            | C9 | D5<br>D7       |  |
| RA09. Be able to value and model threats and execute attacks on an IoT system.                                                                 | B9                            | C9 | D2             |  |

## Contents

| Topic                                                                                            |                                                                                                  |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Introduction to the Industrial Cibersecurity.                                                    | Introduction to the Industrial Cibersecurity.                                                    |
| Introduction to the ciberphysical systems and IoT: hardware, firmware, communications and cloud. | Introduction to the ciberphysical systems and IoT: hardware, firmware, communications and cloud. |
| Cybersecurity in Control Systems and Industrial Communications.                                  | Cybersecurity in Control Systems and Industrial Communications.                                  |
| Cybersecurity in Industry 4.0/5.0.                                                               | Cybersecurity in Industry 4.0/5.0.                                                               |
| Cybersecurity of IoT/IIoT devices: hardware, firmware and middleware.                            | Cybersecurity of IoT/IIoT devices: hardware, firmware and middleware.                            |
| Cybersecurity in IIoT environments: positioning systems and sensors.                             | Cybersecurity in IIoT environments: positioning systems and sensors.                             |
| Cybersecurity In wireless communications for IoT/IIoT devices.                                   | Cybersecurity In wireless communications for IoT/IIoT devices.                                   |

## Planning

|                          | Class hours | Hours outside the classroom | Total hours |
|--------------------------|-------------|-----------------------------|-------------|
| Project based learning   | 5           | 40                          | 45          |
| Lecturing                | 21          | 20                          | 41          |
| Practices through ICT    | 16          | 22                          | 38          |
| Objective questions exam | 1           | 0                           | 1           |

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

## Methodologies

|                        | Description                                                                                                                                                                                                     |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Project based learning | Group implementation of the design, implementation and proofs of a system IoT, with special emphasis in the security. Make grouping attacks to the security of the systems implemented by other mates or third. |
| Lecturing              | Presentation, by the teachers, of the main theoretical contents related with the industrial security and IoT (embedded security, in communications and backends, with special focus in industrial environments) |
| Practices through ICT  | Realisation by part of the students of practices guided and supervised.                                                                                                                                         |

## Personalized assistance

| Methodologies          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Project based learning | The teachers of the subject will loan an individual and personalised attention to the students during the course, resolving his doubts and questions. Likewise, the teachers will orient to the students during the realisation of the project. The doubts will resolve during the personal meetings in group, or in the schedule established for the personal assesment. The schedule of personal assesment will establish to the start of the course and will publish in the web of the subject. |
| Lecturing              | The teachers of the subject will loan an individual and personalised attention to the students during the course, resolving his doubts and questions. The doubts will resolve during the lectures, or in the schedule established for the personal assesment. The schedule of personal assesment will establish to the start of the course and will publish in the web of the subject.                                                                                                             |
| Practices through ICT  | The teachers of the subject will loan an individual and personalised attention to the students during the course, resolving his doubts and questions. Likewise, the teachers will orient and will guide to the students during the realisation of the tasks that have been them assigned, so much in the practices. The doubts will resolve well during the own classes or in the schedule established for the personal assesment.                                                                 |

## Assessment

| Description | Qualification | Training and Learning Results |
|-------------|---------------|-------------------------------|
|-------------|---------------|-------------------------------|

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |    |    |    |                |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|----|----------------|
| Project based learning   | Students will be divided into groups to carry out the design, implementation and testing of an IoT system, placing special emphasis on security and/or will carry out attacks on the security of systems implemented by other classmates or third parties.<br><br>The project carried out, and the report containing the results of the completed attacks (in terms of quality and success) will be evaluated after delivery, assessing aspects such as correctness, quality, performance and functionality. The code, prototypes and documentation produced must be delivered. Likewise, a presentation of the results will be necessary.<br><br>During the project, continuous monitoring of the design and the evolution of the implementation will be carried out. If the intermediate results are not satisfactory, a penalty of up to 20% of the grade may be applied.<br><br>Monitoring will be group and individual: each member of the group must document the tasks developed within their team and respond to them. | 40 | B9 | C9 | D2<br>D5<br>D7 |
| Practices through ICT    | Resolution of practical exercises and preparation of reports with the results obtained.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 30 | B9 | C9 | D2<br>D5<br>D7 |
| Objective questions exam | Written exam on the theoretical and practical content taught during the course.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 30 | B9 | C9 | D2<br>D5<br>D7 |

### Other comments on the Evaluation

To surpass the subject is necessary to complete the distinct parts in which it divides (examination about the exposed contents in the lessons and the project). The final note will be the result to apply the **weighted geometric mean** of the note of each one of the parts.

If the note of the lessons is NT, the note of the project is NP and the note of the practices is NL, the final note will be:

$$\text{Note} = \text{NT} \times 0.3 + \text{NP} \times 0.4 + \text{NL} \times 0.3$$

During the first month, the student has to indicate by writing his wish of attend the matter following the global evaluation. In another case the student has to follow the continuous evaluation. Those who follow the continuous evaluation will not be considered "Not Presented" once they delivered the first questionnaire or task.

The students that opt by the global evaluation have to present incidentally a dossier that have to defend live in front of the teachers, in which they include all the details of the distinct tasks they present, and very especially the project. In the case to follow the global evaluation, the students/ace have to make the work in individual form, except that the teachers communicate them an authorithation to make it in group.

### Extraordinary evaluation

Only the one who do not surpass the first opportunity (when finalising the semester) can do the Extraordinary Evaluation. The evaluation will be described in the previous sections, but incidentally it will be necessary to present a *dossier*, that have to be defended live in front of the teachers, in which they include all the details of the distinct tasks, very especially the project.

The one who had followed the continuous evaluation can opt for keeping the notes obtained at the earliest opportunity for the distinct parts of the subject or leave them.

### Other comments

The scores obtained are only valid for the current academic year. Although the project will be developed (as far as possible) in groups, students must keep evidence of their individual work within the group. In the event that a student's performance is not in line with that of his or her group mates, he or she will be considered expelled from the group and/or may be evaluated completely individually in this part.

The use of any material during the completion of the exams must be explicitly authorized by the teaching staff.

In the event of detection of plagiarism or unethical behavior in any of the work/tests carried out, the grade for the subject will be "fail (0)" and the teachers will report the matter to the academic authorities so that they can take appropriate measures.

### Sources of information

## 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**, 978-0124201149, 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**, 978-1800202092, 2, Packt, 2017

## Complementary Bibliography

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 978-1119226048, 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

## Recommendations

| 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                          | Costa Montenegro, Enrique                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| E-mail                             | kike@gti.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                            |           |      |            |
| Web                                | <a href="http://academica.udc.gal/doa/consultaPublica/look[conpub]MostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202748">http://academica.udc.gal/doa/consultaPublica/look[conpub]MostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202748</a>                                                                                                                                                                                          |           |      |            |
| 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                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------|------------|
| <b>Business in cybersecurity and entrepreneurship</b>                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| 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                                                                                                                     | Fernández Vilas, Ana                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                               |                               |            |
| E-mail                                                                                                                        | avilas@uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| Web                                                                                                                           | <a href="http://academica.udc.gal/doi/consultaPublica/look%5Bconpub%5DMostrarPubGuiaDocAs?entradaPublica=true&amp;codAsignatura=202749">http://academica.udc.gal/doi/consultaPublica/look%5Bconpub%5DMostrarPubGuiaDocAs?entradaPublica=true&amp;codAsignatura=202749</a>                                                                                                                                                                                                                                                                                                                                                |                               |                               |            |
| 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. |                               |                               |            |
| <b>Training and Learning Results</b>                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| Code                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Expected results from this subject</b>                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| Expected results from this subject                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               | Training and Learning Results |            |
| <b>Contents</b>                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| Topic                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Planning</b>                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
|                                                                                                                               | Class hours                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Hours outside the classroom   | Total hours                   |            |
| *The information in the planning table is for guidance only and does not take into account the heterogeneity of the students. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Methodologies</b>                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
|                                                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                               |                               |            |
| <b>Personalized assistance</b>                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Assessment</b>                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| Description                                                                                                                   | Qualification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Training and Learning Results |                               |            |
| <b>Other comments on the Evaluation</b>                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Sources of information</b>                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Basic Bibliography</b>                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Complementary Bibliography</b>                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |
| <b>Recommendations</b>                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                               |                               |            |

| IDENTIFYING DATA                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------|-------------------------------|
| <b>Forensic analysis</b>                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                               |             |                               |
| E-mail                                                                                                                        | asuarez@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                               |             |                               |
| Web                                                                                                                           | <a href="http://academica.udc.gal/doa/consultaPublica/look%5Bconpub%5DMostrarPubGuiaDocAs?entradaPublica=true&amp;codAsignatura=202750">http://academica.udc.gal/doa/consultaPublica/look%5Bconpub%5DMostrarPubGuiaDocAs?entradaPublica=true&amp;codAsignatura=202750</a>                                                                                                                                                                                                                                                                                                                                                                                                 |                               |             |                               |
| 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. |                               |             |                               |
| <b>Training and Learning Results</b>                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Code                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Expected results from this subject</b>                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Expected results from this subject                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             | Training and Learning Results |
| <b>Contents</b>                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Topic                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Planning</b>                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
|                                                                                                                               | Class hours                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Hours outside the classroom   | Total hours |                               |
| *The information in the planning table is for guidance only and does not take into account the heterogeneity of the students. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Methodologies</b>                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
|                                                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |             |                               |
| <b>Personalized assistance</b>                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Assessment</b>                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| Description                                                                                                                   | Qualification                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Training and Learning Results |             |                               |
| <b>Other comments on the Evaluation</b>                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Sources of information</b>                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Basic Bibliography</b>                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Complementary Bibliography</b>                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |
| <b>Recommendations</b>                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |             |                               |

| IDENTIFYING DATA            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |      |            |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|------------|
| <b>Data center security</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |          |      |            |
| 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                   | Suárez González, Andrés                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |      |            |
| E-mail                      | asuarez@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                              |          |      |            |
| Web                         | <a href="http://academica.udc.gal/doa/consultaPublica/look[conpub]MostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202751">http://academica.udc.gal/doa/consultaPublica/look[conpub]MostrarPubGuiaDocAs?entradaPublica=true&amp;_codAsignatura=202751</a>                                                                                                                                                                                                               |          |      |            |
| 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                                      |                               |
| <b>Expected results from this subject</b> |                               |
| 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 m3viles                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |      |            |
| Subject                                                                                                                                                                                                     | (*)Seguridade en dispositivos m3viles                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |          |      |            |
| Code                                                                                                                                                                                                        | V05M175V11218                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |          |      |            |
| Study programme                                                                                                                                                                                             | M3ster Universitario en Ciberseguridad                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |      |            |
| Descriptors                                                                                                                                                                                                 | ECTS Credits                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Choose   | Year | Quadmester |
|                                                                                                                                                                                                             | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Optional | 1st  | 2nd        |
| Teaching language                                                                                                                                                                                           | #EnglishFriendly<br>Spanish<br>Galician<br>English                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |          |      |            |
| Department                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |      |            |
| Coordinator                                                                                                                                                                                                 | L3pez Bravo, Cristina                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |          |      |            |
| Lecturers                                                                                                                                                                                                   | L3pez Bravo, Cristina<br>Rivas L3pez, Jose Luis<br>R3a Est3vez, Jos3 Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |      |            |
| E-mail                                                                                                                                                                                                      | clbravo@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |          |      |            |
| Web                                                                                                                                                                                                         | 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.                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |      |            |
| English Friendly Subject: International students may request from the teachers: a) resources and bibliographic references in English, b) tutoring sessions in English, c) exams and assessments in English. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |      |            |

| <b>Training and Learning Results</b> |                                                                                                                                                                                                                                               |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 aplicaci3ns dos dispositivos m3viles, as3 como realizar unha an3lise forense e definir a pol3tica de seguridade que afecta 3s comunicaci3ns e aos sistemas m3viles dunha organizaci3n. |
| 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.                   |

| <b>Expected results from this subject</b>                                                                                 |                               |
|---------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| 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<br>C14                    |
| Identify an app with malicious behavior and vulnerabilities in operative systems and apps                                 | C14<br>D3                     |
| Be able to realize a forensic analysis of a mobile device                                                                 | C14<br>D8<br>D9               |
| Know the systems of management of the mobile devices                                                                      | B14<br>C14                    |

| <b>Contents</b>                                                      |  |
|----------------------------------------------------------------------|--|
| Topic                                                                |  |
| Introduction: Threats and vulnerabilities that affect mobile devices |  |
| Mobile devices architectures                                         |  |
| Security models in mobile devices                                    |  |

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.

After any assessment, teaching staff may call students for oral verification interviews, either at random or where there are indications of cheating, unauthorized use of artificial intelligence, or other fraudulent means in completing the exam. Grades for the assessments shall remain provisional until any such interviews have been completed. During these interviews, students must demonstrate that they possess the knowledge and skills needed to adequately justify the solutions they submitted.

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.

| <b>IDENTIFYING DATA</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |      |            |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------|------------|
| <b>Smart Contracts and dApps</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |      |            |
| 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<br>Fernández Iglesias, Manuel José                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |          |      |            |
| E-mail                           | manolo@uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |      |            |
| Web                              | http://moovi.uvigo.gal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |      |            |
| 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 |                                                                                                                                                                                                                                                                                        |
| B15  | To understand the basic concepts of smart contracts and decentralised applications, as well as the technologies for their technical design and development and security considerations (testing and code analysis).                                                                    |
| 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. |
| 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.                                                                                                                |

### Expected results from this subject

| Expected results from this subject                                                                                        | Training and Learning Results |
|---------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Understand the usefulness of smart contracts and their application to the development of decentralised systems.           | B15<br>C15                    |
| Assess whether a solution based on decentralised ledger technologies and smart contracts is suitable for a given problem. | B15<br>C15                    |
| Use the appropriate development tools to deploy and interact with smart contracts.                                        | B15<br>C15                    |
| Program smart contracts and connect them to external applications.                                                        | B15<br>C15<br>D4              |
| Analyse smart contract code to assess its robustness and security.                                                        | B15<br>C15<br>D3<br>D4        |

### Contents

|                                                  |                                                                                                                                                    |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Topic                                            |                                                                                                                                                    |
| Basic concepts                                   | An introduction to the basic concepts related to the development of smart contracts and decentralized applications.                                |
| Design and development of intelligent agreements | This topic covers the development of smart contracts, focusing on the most critical security aspects involved.                                     |
| Non-fungible Tokens                              | A specific use case that is very popular in the world of smart contracts and decentralized applications is introduced: non-fungible tokens (NFTs). |

|                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Complementary infrastructure of the blockchain ecosystem | The main mechanisms that enable the capabilities of blockchain networks to be expanded beyond their native limitations are presented. In particular, the role of oracles as a bridge between smart contracts and external data sources, decentralized storage systems as an alternative to on-chain storage of large volumes of information, and cross-chain bridges as tools for interoperability and asset transfer between different networks will be examined. Likewise, the architectural fundamentals, the most relevant use cases, and the main risks associated with each of these technologies will be analyzed. |
| Decentralized Finances (DeFi)                            | This topic introduces the fundamental principles of decentralized finance (DeFi), an ecosystem of financial applications built on blockchain networks and smart contracts. It will cover basic concepts such as financial disintermediation, decentralized exchanges, lending and borrowing protocols, stablecoins, and liquidity provision. It will also analyze the main advantages, risks, and challenges of DeFi, as well as its role in the evolution of digital financial services.                                                                                                                                 |
| Additional cybersecurity issues                          | A summary is provided of the key elements for designing secure smart contracts, oracles, and decentralized applications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Planning

|                          | Class hours | Hours outside the classroom | Total hours |
|--------------------------|-------------|-----------------------------|-------------|
| Lecturing                | 10.5        | 25.5                        | 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

---

Manuel J. Fernández Iglesias, Christian von Eitzen Delgado, Luis E. anido Rifón, **Blockchain, criptomonedas, NFT e aplicacións descentralizadas: fundamentos tecnolóxicos**, 1, Universidade de Vigo, 2024

---

Paul Vigna e Michael J. 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

---

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

---

Manuel J. Fernández Iglesias, **Finanzas descentralizadas para estudiantes de ingeniería software**, 2026

---

---

## Recommendations

---

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

---

Distributed ledger and Blockchain technologies/V05M175V11113

---

| <b>IDENTIFYING DATA</b>                |                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Information security management</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
| 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<br>Spanish<br>Galician                                                                                                                                                                                                                                                                                                                                                                                             |           |      |            |
| Department                             |                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
| Coordinator                            | Caeiro Rodríguez, Manuel                                                                                                                                                                                                                                                                                                                                                                                                            |           |      |            |
| Lecturers                              | Caeiro Rodríguez, Manuel<br>Fernández Vilas, Ana                                                                                                                                                                                                                                                                                                                                                                                    |           |      |            |
| E-mail                                 | mcaeiro@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                |           |      |            |
| Web                                    | 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

| 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<br>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<br>D11                    |
| Develop and evaluate incident response, disaster response and business continuity.                                                                              | D14                           |

### Contents

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

|                                            |                                                                                         |
|--------------------------------------------|-----------------------------------------------------------------------------------------|
| Incident detection and response management | Intrusion detection and prevention system<br>Incident response<br>Incident notification |
| Disaster recovery                          | Disaster recovery plan<br>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     | 20          | 30                          | 50          |
| Objective questions exam | 2           | 20                          | 22          |

\*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.     |

## 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. | 50            |                               |     | D11<br>D14 |
| Objective questions exam | Examination of theoretical knowledge and of practical development                                                                                     | 40            | B16                           | C16 | D11<br>D14 |

## Other comments on the Evaluation

Students can decide to be evaluated according to a continuous assessment model or a global assessment. All students who submit the first lab practice report are opting for continuous assessment. Once students opt for the continuous assessment model, their grade can never be "Not presented".

In the continuous assessment model, the grade will be the result of applying the weighted average between the results: (i) exam of objective questions (40%), (ii) laboratory practice (50%); and (iii) mentored work(10%).

In the global assessment model, the grade will be the result of applying the weighted average between the results: (i) exam of objective questions (50%), (ii) laboratory practice (50%).

To achieve the passing grade, it is necessary to achieve at least 40% of the grade in each of the tests.

**Exam of objective questions:** it will take place on the dates published in the official calendar.

**Practical part:**

1- Continuous evaluation model. Two reports of 2 laboratory practices. One report will be on the development of an ISMS including a risk analysis and the other on incident management and business continuity. Each report will have a weight in the final grade of 25%. The reports will be developed in groups and all students in the same group will receive the same grade. As a group and as part of the laboratory, a case study will also be carried out.

2- Global evaluation model. Individual delivery of the 2 reports of the two practical cases on the same date of the objective questions exam published in the official calendar. In this case, neither case studies nor supervised work will be carried out, so each report will have a weight in the final grade of 25%.

In the extraordinary evaluation, students will be evaluated using the global evaluation modality.

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

*English Friendly subject: International students may request from the teachers: a) materials and bibliographic references in English, b) tutoring sessions in English, c) exams and assessments in English.*

---

### **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**, ISO, 2023

Ester Chicano Tejada, **Gestión de incidentes de seguridad informática**, 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

---

| <b>IDENTIFYING DATA</b>  |                                                                                                                                                                                                                                                                                                                                                  |           |      |            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Concepts and laws</b> |                                                                                                                                                                                                                                                                                                                                                  |           |      |            |
| 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<br>Galician<br>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. |           |      |            |

| <b>Training and Learning Results</b> |                                                                                                                                                                                          |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                          |

| <b>Expected results from this subject</b>                                                                                                                                                |                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| 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                           |

| <b>Contents</b>                                                                                              |                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Topic                                                                                                        |                                                                                                                                                                                                                                                                                           |
| 1. Introduction to Cybersecurity Law. Review of regulations regarding computer security and risk management. | 1.1. EU regulations.<br>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.<br>2.2. Ethical limits in cybersecurity.<br>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. | <p>3.1. The place of commission of the crime.</p> <p>3.2. The moment of commission of the crime.</p> <p>3.3. The plurality of subjects.</p> <p>3.4. Testing problems.</p> <p>3.5. The difficulties in their investigation and prosecution. Brief reference to extradition.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 4. The violation of cybersecurity through criminal conduct.                                | <p>4.1. Terminological precisions: computer crimes and cybercrime.</p> <p>4.2. The use of ICT to commit crimes and when ICT is the object of the crime.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 5. Cybercrimes of discovery and disclosure of secrets                                      | <p>5.1. Crimes of discovering and disclosing secrets (I). Frequent risks: ransomware and the theft of information.</p> <p>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...).</p> <p>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.</p> <p>5.4. Crimes against privacy and an individuals right to their own image: the undue use of cookies</p>                                                                                                                                                                       |
| 6. Cybercrimes against property.                                                           | <p>6.1. Crimes against property (I). Scams committed via computer. Producing, possessing or facilitating computer programs used for this purpose.</p> <p>6.2. Crimes against property (II). Fraud using a third-party telecommunication signal. Use of telecommunication terminal without the owners consent.</p> <p>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.</p> |
| 7. Cybercrimes against collective rights.                                                  | <p>7.1. Crimes against intellectual and industrial property. Through the provision of information society services or through an Internet access portal.</p> <p>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.</p> <p>7.3. Crimes against public faith: electronic lies.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 8. Crimes committed against persons using communication techniques.                        | <p>8.1. Crimes against freedom. Threats using social networks or other ICT. Cyber stalking.</p> <p>8.2. Crimes against the sexual freedom and indemnity. Child grooming and child pornography.</p> <p>8.3. Crimes against intimacy and privacy.</p> <p>8.4. Crimes against honour. Harming a persons digital reputation.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 9. Cyberterrorism.                                                                         | <p>9.1. Concept.</p> <p>9.2. Computing crimes carried out with the specific purpose of art. 573 of the Criminal Code.</p> <p>9.3. Crime of collaborating with a terrorist group or organisation through the provision of technological services.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 10. Crimes relating to national Defence and others.                                        | Brief approximation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 11. Criminological approach to computing.                                                  | <p>11.1. Statistical sources: main national and international organisms, crimes.</p> <p>11.2. Analysis of the main reports on cybersecurity.</p> <p>11.3. Identification of the main technological resources used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12. Analysis of Spanish caselaw in relation to computing crimes. | 12.1. Special attention to the caselaw of the Supreme court.<br>12.2. Agreements of the non-jurisdictional plenary of the Second Chamber of the Supreme Court relating to computing crimes.<br>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).<br>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).<br>13.3. The Organic Law of Data Protection and the Development Regulation.<br>13.4. The personal data protection agency.<br>13.5. Compliance programs in the field of personal data protection. |

## Planning

|                                 | Class hours | Hours outside the classroom | Total hours |
|---------------------------------|-------------|-----------------------------|-------------|
| Lecturing                       | 12          | 40                          | 52          |
| Laboratory practical            | 13          | 30                          | 43          |
| 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        | <p>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).</p> <p>The multiple choice objective questions exam:</p> <ul style="list-style-type: none"> <li>- will be held throughout the course, during the lecture timetable.. The timetable for the different intermediate assessment tests will be approved by the Comisión Académica de Máster Interuniversitario (CAMI) and will be available at the beginning of each academic term.</li> <li>- each examination will comprise the part of the program that is indicated at the start of the term by the subject coordinator.</li> <li>- they will consist of a multiple choice test, with 0 to 2.5 points for each of them. Correct answers will be worth 0.1 and 0.05 will be deducted for each incorrect answer. Answers left blank will not score anything.</li> <li>- Both exams together will be worth 50% of the final mark, with the remaining 50% corresponding to the problem solving (described in the following section).</li> </ul> <p>To pass the subject under the continuous assessment system the mark from the three exams, based on the weighting above, needs to be equal to or greater than 5. Those who attend the first partial test (the first multiple choice objective questions exam), thereby expressing their interest in being included in the continuous assessment system, will be assessed according to the criteria stated above and will not be entitled to be assessed by the final exam system that corresponds to 100% of the marks for the subject. Therefore, if a student takes the first partial exam, it is not possible to abandon the continuous assessment system. If a student takes the first partial exam and then does not take the next partial exam(s), he/she will score 0 points for this/these exam(s).</p> | 50 | B17 C17 D15<br>C18 D19<br>C19 |
| Problem and/or exercise solving | <p>The continuous assessment system will consist of three written examinations: the first two will focus on partial objective tests (objective questions exam, multiple choice, referred to in the previous part of the guide exercise, and the third will focus on problem solving (referred to in this part of the guide).</p> <p>The examination corresponds to problem solving:</p> <ul style="list-style-type: none"> <li>- it will be held on the official date of the ordinary announcement of the final exam: first opportunity, according to the official schedule approved by the Academic Commission of the Master's Degree for the 2022-2023 academic year</li> <li>- It will consist of solving one or several practical cases and will be marked with a score of 0 to 5 points</li> <li>- The problems posed by the practical cases may affect the issues covered in the course syllabus.</li> <li>- It will be worth 50% of the final mark, with the remaining 50% corresponding to the two multiple choice objective questions exams.</li> </ul> <p>To pass the subject under the continuous assessment system, the mark from the three exams, based on the weighting above, needs to be equal to or greater than 5. Those who attend the first partial test (the first multiple choice objective questions exam), thereby expressing their interest in being included in the continuous assessment system, will be assessed according to the criteria stated above and will not be entitled to be assessed by the final exam system that corresponds to 100% of the marks for the subject. Therefore, if a student takes the first partial exam, it is not possible to abandon the continuous assessment system. If a student takes the first partial exam and then does not take the next partial exam(s), he/she will score 0 points for this/these exam(s).</p>                                                                                                                                                                                      | 50 | B17 C17 D15<br>C18 D19<br>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 deducted for incorrect answers. Any answers left blank will not score anything. The practical part will consist of solving one or several practical cases. The final mark for the exam will be obtained by adding together the marks obtained in each of the parts. To pass the subject students must obtain a minimum of 5 points after adding the marks from both parts together.

## 2. SECOND OPPORTUNITY AND EXTRAORDINARY EXAM

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

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

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

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, **Ciberdelitos, los delitos cometidos a través de Internet : estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros**, 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 Relacións, 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

TOURINO, 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

| <b>IDENTIFYING DATA</b>  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |      |            |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Business practice</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |      |            |
| 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://moovi.uvigo.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. |           |      |            |

| <b>Training and Learning Results</b> |                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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<br>B2<br>B3<br>B4<br>B5<br>B6<br>C1<br>C2<br>C3<br>C4<br>C5<br>C6<br>C7<br>C8<br>C9<br>C10<br>C11<br>C12<br>C13<br>C14<br>C15<br>C16<br>C17<br>C18<br>C19<br>D1<br>D2<br>D3<br>D4<br>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 | The assessment will take into account: (1) The report of activities and (2) The assessment of the company tutor. | 100           | B1                            | C1  | D1 |
|                                                      |                                                                                                                  |               | B2                            | C2  | D2 |
|                                                      |                                                                                                                  |               | B3                            | C3  | D3 |
|                                                      |                                                                                                                  |               | B4                            | C4  | D4 |
|                                                      |                                                                                                                  |               | B5                            | C5  | D5 |
|                                                      |                                                                                                                  |               | B6                            | C6  |    |
|                                                      |                                                                                                                  |               |                               | C7  |    |
|                                                      |                                                                                                                  |               |                               | C8  |    |
|                                                      |                                                                                                                  |               |                               | C9  |    |
|                                                      |                                                                                                                  |               |                               | C10 |    |
|                                                      |                                                                                                                  |               |                               | C11 |    |
|                                                      |                                                                                                                  |               |                               | C12 |    |
|                                                      |                                                                                                                  |               |                               | C13 |    |
|                                                      |                                                                                                                  |               |                               | C14 |    |
|                                                      |                                                                                                                  |               |                               | C15 |    |
|                                                      |                                                                                                                  |               |                               | C16 |    |
|                                                      |                                                                                                                  |               |                               | C17 |    |
|                                                      |                                                                                                                  |               |                               | C18 |    |
|                                                      |                                                                                                                  |               |                               | C19 |    |

### 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            |

| <b>IDENTIFYING DATA</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |      |            |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------|------------|
| <b>Final Master's Project</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |      |            |
| 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<br>Galician                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |      |            |
| Department                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |      |            |
| Coordinator                   | Herrería Alonso, Sergio                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |      |            |
| Lecturers                     | Herrería Alonso, Sergio                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |      |            |
| E-mail                        | sha@det.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |      |            |
| Web                           | http://moovi.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |      |            |
| General description           | The Master's Thesis (TFM) is an academic, personal, and original work that must be presented in public and evaluated by a committee.                                                                                                                                                                                                                                                                                                                                                      |           |      |            |
|                               | It is a project in which the student must demonstrate the knowledge acquired during the master's program. It must conclude with the submission of a written report describing a set of explanations, theories, ideas, reasoning, developments, or designs on a topic chosen by the student and supervised by an advisor, who will ensure the student's progress and the quality of the work. In any case, the TFM is the sole responsibility of the student pursuing the master's degree. |           |      |            |

| <b>Training and Learning Results</b> |                                                                                                                                                                                                                                                                |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Code                                 |                                                                                                                                                                                                                                                                |
| 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.                                                                                |
| D13                                  | Apply acquired knowledge and problem-solving skills in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their area of study.                                                                                           |
| 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.                        |
| D15                                  | Communicate knowledge and findings, and the ultimate reasons behind them, to specialist and non-specialist audiences in a clear and unambiguous way.                                                                                                           |
| D16                                  | Innovate and contribute to the advancement of the principles, techniques and processes related to their professional field, designing new algorithms, devices, techniques or models useful for the protection of public, private or commercial digital assets. |

| <b>Expected results from this subject</b>                                                                                                                                |                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Expected results from this subject                                                                                                                                       | Training and Learning Results |
| Capacity for planning and executing an original work in the cybersecurity field.                                                                                         | D13<br>D14<br>D16             |
| Capacity for finding relevant information in the cybersecurity field, for its study and analysis, and the retrieval of relevant results.                                 | D13<br>D14                    |
| Resolution of original problems with real implications in the cybersecurity field.                                                                                       | D13<br>D16                    |
| Elaboration of a project report that summarizes the state of the art, the analyzed problematic, the objectives, the work realized, the conclusions and the future lines. | C19<br>D15                    |
| Presentation of a summary of the main results in front of a public jury and non-specialized audience.                                                                    | C19<br>D15                    |

| <b>Contents</b> |  |
|-----------------|--|
| 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/she will have to show the knowledge obtained during the master. It must conclude with a written report describing explanations, theories, ideas, reasoning, developments or designs, on the subject chosen by the student, and supervised by an advisor, who will ensure the student's progress and the quality of the work. |

## Personalized assistance

### Methodologies Description

|               |                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mentored work | During the Master's Thesis there will be periodic meetings between the student and the advisors to define, orient, supervise and delimit the work, as well as to orient the writing of the report. The TFM coordinator will establish tutoring hours at the beginning of the term. These hours could be checked at the subject web page <a href="https://moovi.uvigo.gal/">https://moovi.uvigo.gal/</a> . |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Tests Description

|              |                                                                                                                                                                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Presentation | The advisors 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 <a href="https://moovi.uvigo.gal/">https://moovi.uvigo.gal/</a> . |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Assessment

|               | Description                                                                                                                                                                                                                                         | Qualification | Training and Learning Results |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------------------------|
| Mentored work | The TFM will be evaluated by an assessment committee. The student will provide a written report, and will make a public presentation describing the work done. The committee will use a rubric that will be publicly available to evaluate the TFM. | 100           |                               |

## Other comments on the Evaluation

### Generative AI

In the performance of the academic activities of this subject, the use of generative artificial intelligence (GAI) is allowed. Its use must be done ethically, critically and responsibly. In the case of using GAI, any results provided by GAI should be critically evaluated, and any citations or references generated should be carefully checked. It is also mandatory to declare the use of these tools.

## 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