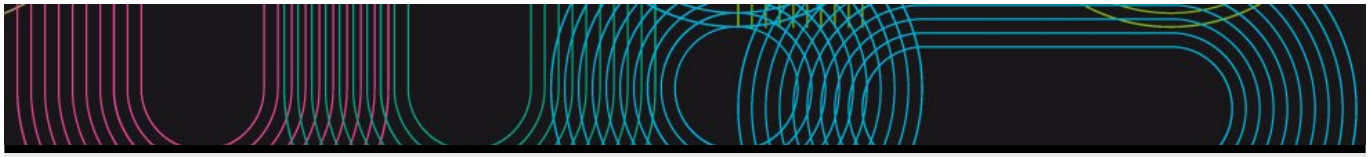

| IDENTIFYING DATA | | | | |
|---|---|---|---|---|
| **Principles and Law in Cybersecurity** | | | | |
| Subject | Principles and Law in Cybersecurity | | | |
| Code | V05M175V01201 | | | |
| Study programme | (*)Máster Universitario en Ciberseguridade | | | |
| Descriptors | ECTS Credits | Choose | Year | Quadmester |
| | 3 | Mandatory | 1st | 2nd |
| Teaching language | Spanish<br>Galician<br>English | | | |
| Department | Public Law<br>External | | | |
| Coordinator | Rodríguez Vázquez, Virgilio | | | |
| Lecturers | Faraldo Cabana, Patricia<br>Rodríguez Vázquez, Virgilio | | | |
| E-mail | virxilio@uvigo.es | | | |
| Web | | | | |
| General description | In this subject will do an approximation to the relative rule to the cybersecurity. A criminological study of the main computing crimes will be made. The central block is formed by a systematic review of the regulation of the computing crimes contained in the Spanish Criminal Code. Besides, it will analyze the judicial law existing in this subject. | | | |

| Competencies | |
|---|---|
| Code | |
| A3 | Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements. |
| C3 | Knowledge of the legal and technical standards used in cybersecurity, their implications in systems design, in the use of security tools and in the protection of information. |
| C8 | Skills for conceive, design, deploy and operate cybersecurity systems. |
| D1 | Ability to apprehend the meaning and implications of the gender perspective in the different areas of knowledge and in the professional exercise, with the aim of attaining a fairer and more egalitarian society. |
| D5 | Ability for oral and written communication in English. |

| Learning outcomes | |
|---|---|
| Expected results from this subject | Training and Learning Results |
| Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the application of their professional capabilities and judgements. | A3 |
| Knowledge of the legal and technical standards used in cybersecurity, their implications in systems design, in the use of security tools and in the protection of information. | C3 |
| Skills for conceive, design, deploy and operate cybersecurity systems. | C8 |
| Ability to apprehend the meaning and implications of the gender perspective in the different areas of knowledge and in the professional exercise, with the aim of attaining a fairer and more egalitarian society. | D1 |
| Ability for oral and written communication in English. | D5 |

| Contents |
|---|
| Topic |

| | |
|---|---|
| 1. Introduction. The Right on cybersecurity. Review of the rules in subject of security computing and management of risks. | 1.1. The rule of the EU.<br>1.2. The Law of National Security: the strategy of national security and the diagram of national security.<br>1.3. The Regulation (UE) 2016/679 of 27 of April of 2016, General Regulation of Protection of Data. The Organic Law of Data Protection and the developmental Regulation.<br>1.4. Computing crimes in the Criminal Code. |
| 2. Criminological approach to the computiing crimes. | 2.1. Statistical sources: main national and international organisms.<br>2.2. Analysis of the main reports on cybersecurity.<br>2.3. Identification of the main technological resources used. |
| 3. The vulnerability of the cybersecurity through crimes. | 3.1. Definition: computing crimes and cybercrime.<br>3.2. The utilization of the TIC to commit crimes and when the TIC are the goal of the crime.<br>3.3. The Spanish Criminal Code, LO 10/1995, of 23 of November, the European Directive 2013/40/UE of the European Parliament and of the Council, of 12 of August of 2013, relative to the attacks against the systems of information, Agreement on cybersecutiry or Agreement of Budapest, of the Council of Europe, of 23 of November of 2001. |
| 4. The main crimes that affect to the cybersecurity. | 4.1. Crimes of finding and disclosure of secrets (I). Frequent risks: ransomware and the burglary of information.<br>4.2. Crimes of finding and disclosure of secrets (II). Access and interception. The access to files or computing bear, electronic or telematic. Special attention to the manager of the files or bear. The interception of transmissions of computing data. The utilization of malware (virus, spyware...).<br>4.3. Crimes of finding and disclosure of secrets (III). Produce, purchase, master or facilitate programs to commit the previous crimes, or passwords of computer or codes of access.<br>4.4. Crimes against the privacy and the right to the own image: the undue use of cookies.<br>4.5. Crimes against the property (I). Swindles costing of any manipulation computing. Produce, possess or facilitate programs computing destined it this end.<br>4.6. Crimes against the property (II). Fraud using signal of extraneous telecommunications. Use of terminal of telecommunications without consent of the headline.<br>4.7. Crimes against the property (III). Damages in computing data, computing programs or electronic documents. Damages to computing systems. Damages to computing systems of an critical infrastructure (brief reference to the operators of critical infrastructure, to the plans of security of the operator and to the plans of specific protection). Hinder or interrupt the operation of a computing system extraneous. Manufacture, possess or facilitate to third computing programs with such end. Special reference to the criminal responsibility of the juridical people.<br>4.8. Crimes against the intellectual and industrial property. Through the provision of services of the society of the information or through a portal of access to internet.<br>4.9. Relative crimes to the bought and to the consumers. Finding of secrets of company through the TIC. Intelligible access it a service of audible or television broadcast, to interactive services rendered the distance by electronic road.<br>4.10. Crimes against the public faith: electronic false. |
| 5. Crimes committed against the persons using the communication technique. | 5.1. Crimes against the freedom. Threats using social nets or other TIC. Cyber stalking.<br>5.2. Crimes against the freedom and indemnity sexual. Child grooming And childish pornography.<br>5.3. Crimes against the privacy and the privacy.<br>5.4. Crimes against honors. Injury of the digital reputation. |
| 6. The cyberterrorist attacks. | 6.1. Concept.<br>6.2. Computing crimes realized with a specific aim of the art. 573 of the Criminal Code.<br>6.3. Crime of collaboration with organisation or terrorist group through the provision of technological services. |
| 7. Relative crimes to the national Defence and others. | Brief approximation. |

| | |
|---|---|
| 8. Analysis of the Spanish judicial law in relation with computing crimes. | 8.1. Special attention to the decisions of the High court.<br>8.2. Agreements of the full no-judicial of the Second Room of the relative High court to computing crimes.<br>8.3. The General Attorney and the specialist attorney on criminality computing. |

| Planning | | | |
|---|---|---|---|
| | Class hours | Hours outside the classroom | Total hours |
| Lecturing | 13 | 32 | 45 |
| Laboratory practices | 5 | 22 | 27 |
| Objective questions exam | 2 | 0 | 2 |
| Problem solving | 1 | 0 | 1 |
| *The information in the planning table is for guidance only and does not take into account the heterogeneity of the students. | | | |

| Methodologies | |
|---|---|
| | Description |
| Lecturing | Presentation by the teacher of the contents on the subject under study, theoretical and / or guidelines for a job, exercise or project to be developed by the student. |
| Laboratory practices | Activities application of knowledge to specific situations and basic skills acquisition and related procedural matter under study. Special spaces are developed with specialized equipment (scientific and technical laboratories, languages, etc.). |

| Personalized attention | |
|---|---|
| **Methodologies** | **Description** |
| Lecturing | The students will be attended in the timetable that will be published in the web of the Máster. |
| Laboratory practices | The students will be attended in the timetable that will be published in the web of the Máster. |

| Assessment | | | | |
|---|---|---|---|---|
| | Description | Qualification | Training and Learning Results | |
| Objective questions exam | The system of continuous evaluation will consist in three examinations writings: the two first, of resolution of objective proofs (examinations of objective questions, type test, that refers this part of the Guide), and the third, of "resolution of problems" (referred in the following part of the guide).<br>The corresponding examinations to the "resolution of objective questions", proofs type test:<br>- they will celebrate along the course, in schedule of kind theoretical class<br>- each examination will comprise the part of the program that respectively indicate to the start of the course by part of the coordinator of the subject<br>- will consist in proofs type test, stop whose qualification, of 0 to 2,5 points each of them, the correct answers sum 0,1 and the incorrect -0,05, not marking the left in white<br>-Two examinations will ponder to 50% stop the final qualification, corresponding the another 50% to the "resolution of problems" (that describes in the following part of the Guide).<br>To pass the subject put system of continuous evaluation is necessary that the resultant note of the three examinations, in accordance with the weighting indicated, was equal or upper to 5 points. The one who goes to the first partial proof (to the first examination of objective questions, type test), manifesting like this his interest for receiving it this system of continuous evaluation, will be evaluated in this opportunity in accordance with the previously established criteria and will not have right to be evaluated by means of a final examination that constitute 100% of the qualification of the subject. Therefore, realized the first partial proof, is not possible to renounce to the system of continuous evaluation. Realized the first partial proof, the student or student no presented to the following or following, the qualification of these will be of 0 points. | 50 | A3 C3 D1 C8 | |

| | | | | |
|---|---|---|---|---|
| Problem solving | The system of continuous evaluation will consist in three examinations writings: the two first, of resolution of objective proofs partial (examinations of objective questions, type test, to the that refers the previous part of the Guide), and the third, of "resolution of problems" (referred in this part of the guide).<br>The corresponding examination to the "resolution of problems":<br>- it will celebrate in the official date of final examination of the common announcement: first<br>opportunity, second the official calendar approved by the Academic Commission of the Master in the course 2018-2019<br>- will consist in the resolution of one or several practical cases, from 0 to 5 points<br>- The problems that pose the practical cases can affect the questions comprised in the totality of the program<br>-Will ponder to 50% stop the final qualification, corresponding the another 50% to the two examinations of objective questions, of type test.<br>To surpass the subject put system of continuous evaluation is necessary that the resultant note of the three examinations, in accordance with the weighting indicated, was equal or upper to 5 points. The one who goes to the first partial proof, manifesting like this his interest for receiving it this system of continuous evaluation, will be evaluated in this opportunity in accordance with the previously established criteria and will not have right to be evaluated by means of a final examination that constitute 100% of the<br>qualification of the subject. Therefore, realized the first partial proof, is not possible to renounce to the system of continuous evaluation. Realized the first partial proof, the student or student no presents to the following or following, the qualification of these will be of 0 points. | 50 | A3 C3 C8 | D1 D5 |

**Other comments on the Evaluation**

**1. FIRST OPPORTUNITY (May 2019)It) SYSTEM OF CONTINUOUS EVALUATIONIt describes in the previous parts of the guide.**
**b) SYSTEM OF FINAL EXAMINATION**

The one who does not opt pole system of continuous evaluation, the evaluation of the subject will consist in one only final examination, in the date
Fixed in the official calendar approved by the Academic Commission of the Master for the course 2018-2019.
The examination, that will comprise the totality of the program and constitutes 100% of the qualification of the subject, will feature of
Two parts, a theorist and another practical, that will qualify of 0 to 5 points each of them. The theoretical part will consist in Proofs type test, stop whose qualification the correct answers sum the double that subtract the incorrect, not marking
The left in white. The practical part will consist in the resolution of one or several practical cases. The final qualification of the examination
It will be the sum of the qualifications obtained in each of the parts. To surpass the subject is necessary to obtain a minimum of 5

Points in the sum of the qualification of two parts.

**2. SECOND OPPORTUNITY (July 2019)**

The evaluation of the subject will consist in one only final examination, in the date fixed in the official calendar approved by the Academic Commission of the Master for the course 2018-2019.
The examination, that will comprise the totality of the program and constitutes 100% of the qualification of the subject, will feature of
Two parts, a theorist and another practical, that will qualify of 0 to 5 points each of them. The theoretical part will consist in Proofs type test, stop whose qualification the correct answers sum the double that subtract the incorrect, not marking
The left in white. The practical part will consist in the resolution of one or several practical cases. The final qualification of the examination
It will be the sum of the qualifications obtained in each of the parts. To surpass the subject is necessary to obtain a minimum of 5

Points in the sum of the qualification of two parts.

**Sources of information**

**Basic Bibliography**

DE LA CUESTA ARZAMANDI, José Luis (dir.), **Derecho penal informático**, 1.ª, Civitas, 2010
LUZÓN PEÑA, Diego-Manuel (dir.), **Código Penal**, 5.ª, Reus, 2017

**Complementary Bibliography**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Recommendations

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

Management of Information Security/V05M175V01101