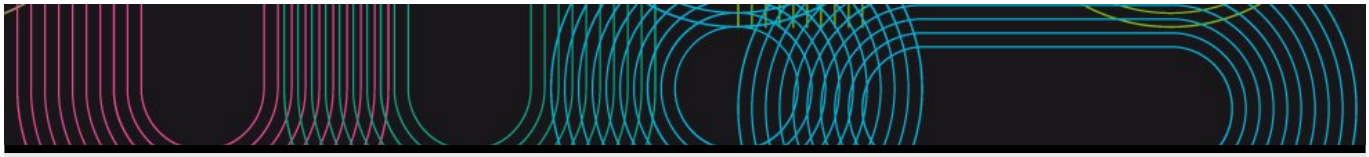

IDENTIFYING DATA				
Principles and Law in Cybersecurity				
Subject	Principles and Law in Cybersecurity			
Code	V05M175V01201			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Mandatory	1st	2nd
Teaching language	Spanish Galician English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

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 to the law on cybersecurity. Review of the rules on computer and risk management.	1.1. EU regulations. 1.2. The Law of National Security: the strategy of national security and the diagram of national security. 1.3. Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation. The Organic Law of Data Protection and the developmental Regulation. 1.4. Computing crimes in the Criminal Code.
2. Criminological approach to computing.	2.1. Statistical sources: main national and international organisms, crimes. 2.2. Analysis of the main reports on cybersecurity. 2.3. Identification of the main technological resources used.
3. Cybersecurity breaches through criminal conduct.	3.1. Definition: computing crimes and cybercrime. 3.2. The use of ICT to commit crimes and when ICT is the goal of the crime. 3.3. The Spanish Criminal Code, LO 10/1995, of 23 November, European Directive 2013/40/UE of the European Parliament and of the Council, of 12 August 2013, on attacks against information systems, Agreement on cybersecurity or Agreement of Budapest, of the Council of Europe, of 23 November 2001.
4. The main crimes that affect cybersecurity.	4.1. Crimes of discovering and disclosing secrets (I). Frequent risks: ransomware and the theft of information. 4.2. Crimes of discovering and disclosing secrets (II). Access and interception. The access to files or computer, electronic or telematic media. Special attention to the manager of the files or media. The interception of transmissions of computing data. The use of malware (virus, spyware...). 4.3. Crimes of discovering and disclosing of secrets (III). Producing, purchasing, importing or facilitating programs to commit the crimes listed above, or computer passwords or access codes. 4.4. Crimes against privacy and an individual□s right to their own image: the undue use of cookies. 4.5. Crimes against property (I). Scams committed via computer. Producing, possessing or facilitating computer programs used for this purpose. 4.6. Crimes against property (II). Fraud using a third-party telecommunication signal. Use of telecommunication terminal without the owner□s consent. 4.7. Crimes against property (III). Damages to computing data, computing programs or electronic documents. Damages to computing systems. Damages to computing systems of a critical infrastructure (brief reference to the operators of critical infrastructure, to the operator□s security plans and to the of specific protection plans). Hindering or interrupting the functioning of a third-party computing system. Manufacturing, possessing or facilitating to third parties computing programs to be used for this purpose. Special reference to the criminal liability of legal persons. 4.8. Crimes against intellectual and industrial property. Through the provision of information society services or through an Internet access portal. 4.9. Crimes relating to the market and to consumers. Discovering company secrets through the use of ICT. Intelligible access to a radio or television broadcast, to remote interactive services via electronic channels. 4.10. Crimes against public faith: electronic lies.
5. Crimes committed against persons using communication techniques.	5.1. Crimes against freedom. Threats using social networks or other ICT. Cyber stalking. 5.2. Crimes against the sexual freedom and indemnity. Child grooming and child pornography. 5.3. Crimes against intimacy and privacy. 5.4. Crimes against honour. Harming a person□s digital reputation.
6. Cyberterrorism.	6.1. Concept. 6.2. Computing crimes carried out with the specific purpose of art. 573 of the Criminal Code. 6.3. Crime of collaborating with a terrorist group or organisation through the provision of technological services.
7. Crimes relating to national Defence and others.	Brief approximation.

8. Analysis of Spanish caselaw in relation to computing crimes.	8.1. Special attention to the caselaw of the Supreme court. 8.2. Agreements of the non-jurisdictional plenary of the Second Chamber of the Supreme Court relating to computing crimes. 8.3. The Prosecution Service and the Prosecutor□s Office specialising in computer criminality.

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

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-integrates of the University of Vigo.
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-integrates of the University of Vigo.

Assessment			
	Description	Qualification	Training and Learning Results
Objective questions exam	The continuous assessment system will consist of three written examinations first two will focus on partial objective tests(objective questions exam, multiple choice, referred to in this part of the Guide), and the third, will focus on "problem solving" (referred to in the following part of the guide). The multiple choice □objective questions□ exam: - will be held throughout the course, during the lecture timetable.. The timetable for the different intermediate assessment tests will be approved by the Comisión Académica de Máster Interuniversitario (CAMI) and will be available at the beginning of each academic term. - each examination will comprise the part of the program that is indicated at the start of the term by the subject coordinator. - they will consist of a multiple choice test, with 0 to 2.5 points for each of them. Correct answers will be worth 0.1 and 0.05 will be deducted for each incorrect answer. Answers left blank will not score anything. - Both exams together will be worth 50% of the final mark, with the remaining 50% corresponding to the □problem solving□ (described in the following section). To pass the subject under the continuous assessment system the mark from the three exams, based on the weighting above, needs to be equal to or greater than 5. Those who attend the first partial test (the first multiple choice objective questions exam), thereby expressing their interest in being included in the continuous assessment system, will be assessed according to the criteria stated above and will not be entitled to be assessed by the final exam system that corresponds to 100% of the marks for the subject. Therefore, if a student takes the first partial exam, it is not possible to abandon the continuous assessment system. If a student takes the first partial exam and then does not take the next partial exam(s), they will score 0 points for this/these exam(s).	50	A3 C3 D1 C8

Problem and/or exercise solving	The continuous assessment system will consist of three written examinations: the first two will focus on partial objective tests (objective questions exam, multiple choice, referred to in the previous part of the guide exercise, and the third will focus on problem solving (referred to in this part of the guide). The examination corresponds to "problem solving": - it will be held on the official date of the ordinary announcement of the final exam: first opportunity, according to the official schedule approved by the Academic Commission of the Master's Degree for the 2019-2020 academic year - It will consist of solving one or several practical cases and will be marked with a score of 0 to 5 points - The problems posed by the practical cases may affect the issues covered in the course syllabus. - It will be worth 50% of the final mark, with the remaining 50% corresponding to the two multiple choice objective questions exams. To pass the subject under the continuous assessment system, the mark from the three exams, based on the weighting above, needs to be equal to or greater than 5. Those who attend the first partial test (the first multiple choice objective questions exam), thereby expressing their interest in being included in the continuous assessment system, will be assessed according to the criteria stated above and will not be entitled to be assessed by the final exam system that corresponds to 100% of the marks for the subject. Therefore, if a student takes the first partial exam, it is not possible to abandon the continuous assessment system. If a student takes the first partial exam and then does not take the next partial exam(s), they will score 0 points for this/these exam(s).	50	A3 C3 C8 D1 D5

Other comments on the Evaluation

1. FIRST OPPORTUNITY

a) CONTINUOUS ASSESSMENT SYSTEM described in the sections above.

b) FINAL EXAM SYSTEM

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

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

2. SECOND OPPORTUNITY AND EXTRAORDINARY EXAM

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

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

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

Contingency plan

Description

=== EXCEPTIONAL MEASURES SCHEDULED ===
In front of it uncertain and unpredictable evolution of the sanitary alert caused by the COVID- 19, the University establishes join extraordinary planning that will actuate in the moment in that the administrations and the institution determine it attending to criteria of security, health and responsibility, and guaranteeing the course in a scenario non presential or no totally presential. These already scheduled measures guarantee, in the moment that was prescriptive, the development of the course of a way but effective when being known beforehand (or with a wide advance) pole students and the teaching staff through the tool normalized and institutionalized of the teaching guides DOCNET.

=== ADAPTATION OF The METHODOLOGIES ===
There are not changes. Telematic platform of and virtual classroom and office.

=== ADAPTATION OF The EVALUATION ===
There are not changes. Telematic platform of and virtual classroom and office.