



## DATOS IDENTIFICATIVOS

### Conceptos e leis en ciberseguridade

Materia	Conceptos e leis en ciberseguridade			
Código	V05M175V01201			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OB	1	2c
Lingua de impartición	Castelán Galego Inglés			
Departamento				
Coordinador/a	Rodríguez Vázquez, Virgilio			
Profesorado	Faraldo Cabana, Patricia Rodríguez Vázquez, Virgilio			
Correo-e	virxilio@uvigo.es			
Web	<a href="http://moovi.uvigo.gal/">http://moovi.uvigo.gal/</a>			
Descrición xeral	Nesta materia farase unha aproximación á normativa relativa á ciberseguridade. A continuación realizarase un estudo criminolóxico dos principais delitos informáticos. O bloque central está formado por unha revisión sistemática da regulación dos delitos informáticos contida no Código Penal español. Ademais, analizarase a xurisprudenza existente nesta materia.			

## Competencias

Código	
A3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
C3	Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información
C8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
D1	Ter capacidade para comprender o significado e aplicación da perspectiva de xénero nos distintos ámbitos de coñecemento e na práctica profesional co obxectivo de acadar unha sociedade máis xusta e igualitaria.
D5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

## Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.	A3
Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información	C3
Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade.	C8
Ter capacidade para comprender o significado e aplicación da perspectiva de xénero nos distintos ámbitos de coñecemento e na práctica profesional co obxectivo de acadar unha sociedade máis xusta e igualitaria.	D1
Ter capacidade para comunicarse oralmente e por escrito en inglés.	D5

## Contidos

Tema
------

1. Introducción ao Dereito sobre ciberseguridade. Revisión das normativas en materia de seguridade informática e xestión de riscos.	<p>1.1. A normativa da UE.</p> <p>1.2. A Lei de Seguridade Nacional: a estratexia de ciberseguridade nacional e o esquema de seguridade nacional.</p> <p>1.3. O Regulamento (UE) 2016/679 de 27 de abril de 2016, [Regulamento Xeral de Protección de Datos] (RXPd). A Lei Orgánica de Protección de Datos e o Regulamento de desenvolvemento.</p> <p>1.4. O Código Penal en materia de delitos informáticos.</p>
2. Aproximación criminolóxica aos delitos informáticos.	<p>2.1. Fontes estatísticas: principais organismos nacionais e internacionais.</p> <p>2.2. Análise dos principais informes sobre cibercriminalidade.</p> <p>2.3. Identificación dos principais recursos tecnolóxicos utilizados.</p>
3. A vulneración da ciberseguridade a través de conductas delictivas.	<p>3.1. Precisións terminolóxicas: delitos informáticos e cibercrime.</p> <p>3.2. A utilización das TIC para cometer delitos e cando as TIC son o obxecto do delito.</p> <p>3.3. O Código Penal español, LO 10/1995, de 23 de novembro, a Directiva Europea 2013/40/UE do Parlamento Europeo e do Consello, de 12 de agosto de 2013, relativa aos ataques contra os sistemas de información, Convenio sobre cibercriminalidade ou Convenio de Budapest, do Consello de Europa, de 23 de novembro de 2001.</p>
4. As principais conductas delictivas que afectan á ciberseguridade.	<p>4.1. Delitos de descubrimento e revelación de segredos (I). Riscos frecuentes: ransomware e o roubo de información.</p> <p>4.2. Delitos de descubrimento e revelación de segretos (II). Acceso e interceptación ilícita. O acceso a ficheiros ou soportes informáticos, electrónicos ou telemáticos. Especial atención ao responsable dos ficheiros ou soportes. A interceptación de transmisións de datos informáticos. A utilización de malware (virus, troianos e spyware).</p> <p>4.3. Delitos de descubrimento e revelación de segretos (III). Producir, adquirir, importar ou facilitar programas informáticos para cometer os delitos anteriores, ou contrasinais de ordenador ou códigos de acceso.</p> <p>4.4. Delitos contra a intimidade e o dereito á propia imaxe: o uso indebido de cookies.</p> <p>4.5. Delitos contra a propiedade (I). Estafas valéndose dalgunha manipulación informática. Producir, posuír ou facilitar programas informáticos destinados a ese fin.</p> <p>4.6. Delitos contra a propiedade (II). Defraudación utilizando sinal de telecomunicacións allea. Uso de terminal de telecomunicacións sen consentimento do titular.</p> <p>4.7. Delitos contra a propiedade (III). Danos en datos informáticos, programas informáticos ou documentos electrónicos. Danos a sistemas informáticos. Danos a sistemas informáticos dunha infraestrutura crítica (breve referencia aos operadores de infraestruturas críticas, aos plans de seguridade do operador e aos plans de protección específicos). Obstaculizar ou interromper o funcionamento dun sistema informático alleo. Fabricar, posuír ou facilitar a terceiros programas informáticos con tal fin. Especial referencia á responsabilidade penal das persoas xurídicas.</p> <p>4.8. Delitos contra a propiedade intelectual e industrial. A través da prestación de servizos da sociedade da información ou a través dun portal de acceso a internet.</p> <p>4.9. Delitos relativos ao mercado e aos consumidores. Descubrimento de segredos de empresa a través das TIC. Acceso intelixible a un servizo de radiodifusión sonoro ou televisivo, a servizos interactivos prestados a distancia por vía electrónica.</p> <p>4.10. Delitos contra a fe pública: falsedades electrónicas.</p>
5. Delitos cometidos contra as persos utilizando as TIC.	<p>5.1. Delitos contra a liberdade. Ameazas e coaccións utilizando redes sociais ou outras TIC. Cyberstalking.</p> <p>5.2. Delitos contra a liberdade e a indemnidade sexuais. Child grooming e pornografía infantil.</p> <p>5.3. Delitos contra a intimidade e a privacidade.</p> <p>5.4. Delitos contra a honra. Lesión da reputación dixital.</p>
6. O ciberterrorismo.	<p>6.1. Concepto.</p> <p>6.2. Delitos informáticos realizados cunha finalidade específica do art. 573 do Código Penal.</p> <p>6.3. Delito de colaboración con organización ou grupo terrorista a través da prestación de servizos tecnolóxicos.</p>
7. Delitos relativos á Defensa nacional e outros.	Breve aproximación.

8. Análise da xurisprudenza española en relación con delitos informáticos.
- 8.1. Especial atención á xurisprudenza do Tribunal Supremo.  
 8.2. Acordos do pleno non xurisdiccional da Sala Segunda do Tribunal Supremo relativos a delitos informáticos.  
 8.3. O Ministerio Fiscal e a Fiscalía especialista en materia de criminalidade informática.

### Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	13	32	45
Prácticas de laboratorio	5	22	27
Exame de preguntas obxectivas	2	0	2
Resolución de problemas e/ou exercicios	1	0	1

\*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

### Metodoloxía docente

	Descrición
Lección maxistral	Exposición por parte do profesor/a dos contidos sobre a materia obxecto de estudo, bases teóricas e/ou directrices dun traballo, exercicio que o/a estudante ten que desenvolver.
Prácticas de laboratorio	Actividades de aplicación dos coñecementos a situacións concretas e de adquisición de habilidades básicas e procedementais relacionadas coa materia obxecto de estudo.

### Atención personalizada

Metodoloxías	Descrición
Lección maxistral	O alumnado será atendido nos horarios de titorías que serán publicados na web do Máster. Poderá atenderse, previa cita -concertada mediante correo electrónico-, ou ben a través de correo electrónico ou ben a través de despacho virtual no campus remoto-integra da Universidad de Vigo.
Prácticas de laboratorio	O alumnado será atendido nos horarios de titorías que serán publicados na web do Máster. Poderá atenderse, previa cita -concertada mediante correo electrónico-, ou ben a través de correo electrónico ou ben a través de despacho virtual no campus remoto-integra da Universidad de Vigo.

### Avaliación

Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Exame de preguntas obxectivas	<p>O sistema de avaliación continua consistirá en tres exames escritos: os dous primeiros, de resolución de probas obxectivas parciais (exames de preguntas obxectivas), tipo test, aos que se refire este apartado da Guía), e o terceiro, de "resolución de problemas" (referido no seguinte apartado da guía). Os exames correspondentes á "resolución de preguntas obxectivas", probas tipo test:</p> <ul style="list-style-type: none"> <li>- celebraranse ao longo do curso, en horario de clase maxistral. A planificación das diferentes probas de avaliación intermedia aprobarase nunha Comisión Académica de Máster Interuniversitaria (CAMI) e estará dispoñible ao principio do cuadrimestre.</li> <li>- cada exame comprenderá a parte do temario que respectivamente se indique ao inicio do cuadrimestre por parte do coordinador da materia</li> <li>- consistirán en probas tipo test, para cuxa cualificación, de 0 a 2,5 puntos cada unha delas, as respostas correctas suman 0,1 e as incorrectas restan 0,05, non puntuando as deixadas en branco</li> <li>-Ámbolos dous exames ponderaranse ao 50% para a cualificación final, correspondendo o outro 50% á "resolución de problemas" (que se describe no apartado seguinte).</li> </ul> <p>Para superar a materia polo sistema de avaliación continua é necesario que a nota resultante dos tres exames, de acordo coa ponderación indicada, sexa igual ou superior a 5 puntos. Quen acuda á primeira proba parcial (ao primeiro exame de preguntas obxectivas, tipo test), manifestando así o seu interese por acollerse a este sistema de avaliación continua, será avaliado nesta oportunidade de acordo cos criterios previamente establecidos e non terá dereito a ser avaliado mediante un exame final que constitúa o 100% da cualificación da materia. Polo tanto, realizada a primeira proba parcial, non é posible renunciar ao sistema de avaliación continua. Se realizada a primeira proba parcial, a alumna ou alumno non se presentase á seguinte ou seguintes, a cualificación destas será de 0 puntos.</p>	50	A3	C3 C8	D1
Resolución de problemas e/ou exercicios	<p>O sistema de avaliación continua consistirá en tres exames escritos: os dous primeiros, de resolución de probas obxectivas parciais (exames de preguntas obxectivas), tipo test, aos que se refire o apartado anterior da Guía), e o terceiro, de "resolución de problemas" (referido neste apartado da guía). O devandito exame correspondente á "resolución de problemas":</p> <ul style="list-style-type: none"> <li>- celebrárase na data oficial de exame final da convocatoria ordinaria: primeira oportunidade, segundo o calendario oficial aprobado pola Comisión Académica do Máster no curso 2021-2022.</li> <li>- consistirá na resolución dun ou varios casos prácticos e calificarase de 0 a 5 puntos</li> <li>- Os problemas que plantexen os casos prácticos poden afectar a cuestións comprendidas na totalidade do temario</li> <li>-Ponderarase ao 50% para a cualificación final, correspondendo o outro 50% aos dous exames anteditos de preguntas obxectivas, de tipo test.</li> </ul> <p>Para superar a materia polo sistema de avaliación continua é necesario que a nota resultante dos tres exames, de acordo coa ponderación indicada, sexa igual ou superior a 5 puntos. Quen acuda á primeira proba parcial, manifestando así o seu interese por acollerse a este sistema de avaliación continua, será avaliado nesta oportunidade de acordo cos criterios previamente establecidos e non terá dereito a ser avaliado mediante un exame final que constitúa o 100% da cualificación da materia. Polo tanto, realizada a primeira proba parcial, non é posible renunciar ao sistema de avaliación continua. Se realizada a primeira proba parcial, a alumna ou alumno non se presenta á seguinte ou seguintes, a cualificación destas será de 0 puntos.</p>	50	A3	C3 C8	D1 D5

### Outros comentarios sobre a Avaliación

#### 1. PRIMEIRA OPORTUNIDADEa) SISTEMA DE AVALIACIÓN CONTINUADescribítese nos apartados anteriores.

#### b) SISTEMA DE EXAME FINAL

Para quen non opte polo sistema de avaliación continua, a avaliación da materia consistirá nun único exame final, na data fixada no calendario oficial aprobado pola Comisión Académica do Máster para o curso 2021-2022.

O devandito exame, que comprenderá a totalidade do temario e constitúe o 100% da cualificación da materia, constará de dúas partes, unha teórica e outra práctica, que se cualificarán de 0 a 5 puntos cada unha delas. A parte teórica consistirá en

probas tipo test, para cuxa cualificación as respostas correctas suman o dobre que restan as incorrectas, non puntuando as deixadas en branco. A parte práctica consistirá na resolución dun ou varios casos prácticos. A cualificación final do exame será a suma das cualificacións obtidas en cada unha das partes. Para superar a materia é necesario obter un mínimo de 5 puntos na suma da cualificación de ámbalas dúas partes.

## 2. SEGUNDA OPORTUNIDADE E CONVOCATORIA EXTRAORDINARIA

A avaliación da materia consistirá nun único exame final, na data fixada no calendario oficial aprobado pola Comisión Académica do Máster para o curso 2021-2022.

O devandito exame, que comprenderá a totalidade do temario e constitúe o 100% da cualificación da materia, constará de dúas partes, unha teórica e outra práctica, que se cualificarán de 0 a 5 puntos cada unha delas. A parte teórica consistirá en probas tipo test, para cuxa cualificación as respostas correctas suman o dobre que restan as incorrectas, non puntuando as deixadas en branco. A parte práctica consistirá na resolución dun ou varios casos prácticos. A cualificación final do exame será a suma das cualificacións obtidas en cada unha das partes. Para superar a materia é necesario obter un mínimo de 5 puntos na suma da cualificación de ámbalas dúas partes.

---

### **Bibliografía. Fontes de información**

#### **Bibliografía Básica**

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

#### **Bibliografía Complementaria**

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 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

## Recomendacións

### Materias que se recomenda ter cursado previamente

Xestión da seguridade da información/V05M175V01101

## Plan de Continxencias

### Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===

Ante a incerta e imprevisible evolución da alerta sanitaria provocada pola COVID- 19, a Universidade establece una planificación extraordinaria que se activará no momento en que as administracións e a propia institución o determinen atendendo a criterios de seguridade, saúde e responsabilidade, e garantindo a docencia nun escenario non presencial ou non totalmente presencial. Estas medidas xa planificadas garanten, no momento que sexa preceptivo, o desenvolvemento da docencia dun xeito mais áxil e eficaz ao ser coñecido de antemán (ou cunha ampla antelación) polo alumnado e o profesorado a través da ferramenta normalizada e institucionalizada das guías docentes DOCNET.

=== ADAPTACIÓN DAS METODOLOXÍAS ===

Non hai cambios. Faranse a través de medios telemáticos (plataforma de teledocencia e aula e despacho virtual).

=== ADAPTACIÓN DA AVALIACIÓN ===

Non hai cambios. Faranse a través de medios telemáticos (plataforma de teledocencia e aula e despacho virtual).