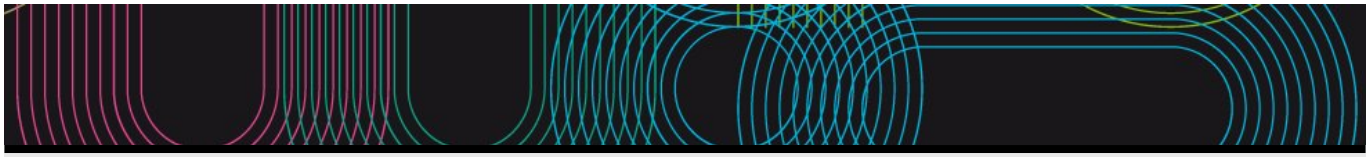

DATOS IDENTIFICATIVOS				
Conceptos y leyes en ciberseguridad				
Asignatura	Conceptos y leyes en ciberseguridad			
Código	V05M175V01201			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Carácter	Curso	Cuatrimestre
	3	OB	1	2c
Lengua Impartición	Castellano Gallego Inglés			
Departamento				
Coordinador/a	Rodríguez Vázquez, Virgilio			
Profesorado	Faraldo Cabana, Patricia Rodríguez Vázquez, Virgilio			
Correo-e	virxilio@uvigo.es			
Web	http://moovi.uvigo.gal/			
Descripción general	En esta materia se hará una aproximación a la normativa relativa a la ciberseguridad. A continuación se realizará un estudio criminológico de los principales delitos informáticos. El bloque central está formado por una revisión sistemática de la regulación de los delitos informáticos contenida en el Código Penal español. Además, se analizará la jurisprudencia existente en esta materia.			

Competencias	
Código	
CB3	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
CE3	Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
CE8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
CT1	Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria.
CT5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

Resultados de aprendizaje	
Resultados de aprendizaje	Competencias
Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.	CB3
Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información	CE3
Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad.	CE8
Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria.	CT1
Tener capacidad para comunicarse oralmente y por escrito en inglés.	CT5

Contenidos
Tema

1. Introducción al Derecho sobre ciberseguridad. Revisión de las normativas en materia de seguridad informática y gestión de riesgos.	1.1. La normativa de la UE. 1.2. La Ley de Seguridad Nacional: la estrategia de ciberseguridad nacional y el esquema de seguridad nacional. 1.3. El Reglamento (UE) 2016/679 de 27 de abril de 2016, Reglamento General de Protección de Datos (RGPD). La Ley Orgánica de Protección de Datos y el Reglamento de desarrollo. El Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). 1.4. El Código Penal en materia de delitos informáticos.
2. Aproximación criminológica a los delitos informáticos.	2.1. Fuentes estadísticas: principales organismos nacionales e internacionales. 2.2. Análisis de los principales informes sobre cibercriminalidad. 2.3. Identificación de los principales recursos tecnológicos utilizados.
3. La vulneración de la ciberseguridad a través de conductas delictivas.	3.1. Precisiones terminológicas: delitos informáticos y cibercrimen 3.2. La utilización de las TIC para cometer delitos y cuando las TIC son el objeto del delito. 3.3. El Código Penal español, LO 10/1995, de 23 de noviembre, la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, Convenio sobre cibercriminalidad o Convenio de Budapest, del Consejo de Europa, de 23 de noviembre de 2001.
4. Las principales conductas delictivas que afectan a la ciberseguridad.	4.1. Delitos de descubrimiento y revelación de secretos (I). Riesgos frecuentes: el ransomware y el robo de información. 4.2. Delitos de descubrimiento y revelación de secretos (II). Acceso e interceptación ilícita. El acceso a ficheros o soportes informáticos, electrónicos o telemáticos. Especial atención al responsable de los ficheros o soportes. La interceptación de transmisiones de datos informáticos. La utilización de malware (virus, troyanos y spyware). 4.3. Delitos de descubrimiento y revelación de secretos (III). Producir, adquirir, importar o facilitar programas informáticos para cometer los delitos anteriores o contraseñas de ordenador o códigos de acceso. 4.4. Delitos contra la intimidad y el derecho a la propia imagen: el uso indebido de cookies. 4.5. Delitos contra la propiedad (I). Estafas valiéndose de alguna manipulación informática. Producir, poseer o facilitar programas informáticos destinados a ese fin. 4.6. Delitos contra la propiedad (II). Defraudación utilizando señal de telecomunicaciones ajena. Uso de terminal de telecomunicaciones sin consentimiento del titular. 4.7. Delitos contra la propiedad (III). Daños en datos informáticos, programas informáticos o documentos electrónicos. Daños a sistemas informáticos. Daños a sistemas informáticos de una infraestructura crítica (breve referencia a los operadores de infraestructuras críticas, a los planes de seguridad del operador y a los planes de protección específicos). Obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno. Fabricar, poseer o facilitar a terceros programas informáticos con tal fin. Especial referencia a la responsabilidad penal de las personas jurídicas. 4.8. Delitos contra la propiedad intelectual e industrial. A través de la prestación de servicios de la sociedad de la información o a través de un portal de acceso a internet. 4.9. Delitos relativos al mercado y a los consumidores. Descubrimiento de secretos de empresa a través de las TIC. Acceso inteligible a un servicio de radiodifusión sonoro o televisivo, a servicios interactivos prestados a distancia por vía electrónica. 4.10. Delitos contra la fe pública: falsedades electrónicas.
5. Delitos cometidos contra las personas utilizando las TIC.	5.1. Delitos contra la libertad. Amenazas y coacciones utilizando redes sociales u otras TIC. Ciberstalking. 5.2. Delitos contra la libertad e indemnidad sexuales. Child grooming y pornografía infantil. 5.3. Delitos contra la intimidad y la privacidad. 5.4. Delitos contra el honor. Lesión de la reputación digital.
6. El ciberterrorismo.	6.1. Concepto. 6.2. Delitos informáticos realizados con una finalidad específica del art. 573 del Código Penal. 6.3. Delito de colaboración con organización o grupo terrorista a través de la prestación de servicios tecnológicos.
7. Delitos relativos a la Defensa nacional y otros.	Breve aproximación.

8. Análisis de la jurisprudencia española en relación con delitos informáticos.	8.1. Especial atención a la jurisprudencia del Tribunal Supremo. 8.2. Acuerdos del pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo relativos a delitos informáticos. 8.3. El Ministerio Fiscal y la Fiscalía especialista en materia de criminalidad informática.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	13	32	45
Prácticas de laboratorio	5	22	27
Examen de preguntas objetivas	2	0	2
Resolución de problemas y/o ejercicios	1	0	1

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Lección magistral	Exposición por parte del profesor de los contenidos sobre la materia objeto de estudio, bases teóricas y/o directrices de un trabajo, ejercicio que el/la estudiante tiene que desarrollar
Prácticas de laboratorio	Actividades de aplicación de los conocimientos a situaciones concretas y de adquisición de habilidades básicas y procedimentales relacionadas con la materia objeto de estudio.

Atención personalizada

Metodologías	Descripción
Lección magistral	El alumnado será atendido nos horarios de tutorías que serán publicados en la web del Máster. Podrá atenderse, previa cita -concertada mediante correo electrónico-, o bien a través de correo electrónico o bien a través de despacho virtual en el campus remoto.
Prácticas de laboratorio	El alumnado será atendido nos horarios de tutorías que serán publicados en la web del Máster. Podrá atenderse, previa cita -concertada mediante correo electrónico-, o bien a través de correo electrónico o bien a través de despacho virtual en el campus remoto.

Evaluación

	Descripción	Calificación	Competencias Evaluadas
Examen de preguntas objetivas	El sistema de evaluación continua consistirá en tres exámenes escritos: los dos primeros, de resolución de pruebas objetivas parciales ("exámenes de preguntas objetivas", tipo test, a los que se refiere este apartado de la Guía), y el tercero, de "resolución de problemas" (referido en el siguiente apartado de la guía). Los exámenes correspondientes a la "resolución de preguntas objetivas", pruebas tipo test: - se celebrarán a lo largo del curso, en horario de clase magistral. La planificación de las diferentes pruebas de evaluación intermedia se aprobará en una Comisión Académica de Máster Interuniversitaria (CAMI) y estará disponible al principio del cuatrimestre. - cada examen comprenderá la parte del temario que respectivamente se indique al inicio del cuatrimestre por parte del coordinador de la materia - consistirán en pruebas tipo test, para cuya calificación, de 0 a 2,5 puntos cada una de ellas, las respuestas correctas suman 0,1 y las incorrectas restan 0,05, no puntuando las dejadas en blanco - Ambos exámenes se ponderarán al 50% para la calificación final, correspondiendo el otro 50% a la "resolución de problemas" (que se describe en el apartado siguiente). Para superar la materia por el sistema de evaluación continua es necesario que la nota resultante de los tres exámenes, de acuerdo con la ponderación indicada, sea igual o superior a 5 puntos. Quien acuda a la primera prueba parcial (al primer examen de preguntas objetivas, tipo test), manifestando así su interés por acogerse a este sistema de evaluación continua, será evaluado en esta oportunidad de acuerdo con los criterios previamente establecidos y no tendrá derecho a ser evaluado mediante un examen final que constituya el 100% de la calificación de la materia. Por lo tanto, realizada la primera prueba parcial, no es posible renunciar al sistema de evaluación continua. Si realizada la primera prueba parcial, la alumna o alumno no se presentase a la siguiente o siguientes, la calificación de estas será de 0 puntos.	50	CB3 CE3 CE8 CT1

Resolución de problemas y/o ejercicios	El sistema de evaluación continua consistirá en tres exámenes escritos: los dos primeros, de resolución de pruebas objetivas parciales ("exámenes de preguntas objetivas", tipo test, a los que se refiere el apartado anterior de la Guía), y el tercero, de "resolución de problemas" (referido en este apartado de la guía). El citado examen correspondiente a la "resolución de problemas": - Se celebrará en la fecha oficial de examen final de la convocatoria ordinaria: primera oportunidad, según el calendario oficial aprobado por la Comisión Académica del Máster en el curso 2022-2023 - consistirá en la resolución de uno o varios casos prácticos y se calificará de 0 a 5 puntos - los problemas que planteen los casos prácticos pueden afectar a cuestiones comprendidas en la totalidad del temario - Se ponderará al 50% para la calificación final, correspondiendo el otro 50% a los dos exámenes citados de preguntas objetivas, de tipo test. Para superar la materia por el sistema de evaluación continua es necesario que la nota resultante de los tres exámenes, de acuerdo con la ponderación indicada, sea igual o superior a 5 puntos. Quien acuda a la primera prueba parcial, manifestando así su interés por acogerse a este sistema de evaluación continua, será evaluado en esta oportunidad de acuerdo con los criterios previamente establecidos y no tendrá derecho a ser evaluado mediante un examen final que constituya el 100% de la calificación de la materia. Por lo tanto, realizada la primera prueba parcial, non es posible renunciar al sistema de evaluación continua. Si realizada la primera pruba parcial, la alumna o alumno no se presenta a la siguiente o siguientes, la calificación de estas será de 0 puntos.	50	CB3	CE3 CE8	CT1 CT5

Otros comentarios sobre la Evaluación

1. PRIMERA OPORTUNIDADa) SISTEMA DE EVALUACIÓN CONTINUASe describe en los apartados anteriores.
b) SISTEMA DE EXAMEN FINAL

Para quien no opte por el sistema de evaluación continua, la evaluación de la materia consistirá en un único examen final, en la fecha fijada en el calendario oficial aprobado por la Comisión Académica del Máster para el curso 2022-2023.

El citado examen, que comprenderá la totalidad del temario y que constituye el 100% de la calificación de la materia, constará de
dos partes, una teórica y otra práctica, que se calificarán de 0 a 5 puntos cada una de ellas. La parte teórica consistirá en pruebas tipo test, para cuya calificación las respuestas correctas suman el doble que restan las incorrectas, no puntuando las dejadas en blanco. La parte práctica consistirá en la resolución de uno o varios casos prácticos. La calificación final del examen
será la suma de las calificaciones obtenidas en cada una de las partes. Para superar la materia es necesario obtener un mínimo de 5 puntos en la suma de la calificación de ambas partes.

2. SEGUNDA OPORTUNIDAD Y CONVOCATORIA EXTRAORDINARIA

La evaluación de la materia consistirá en un único exame final, en la fecha fijada en el calendario oficial aprobado por la Comisión Académica del Máster para el curso 2022-2023.

El citado examen, que comprenderá la totalidad del temario y que constituye el 100% de la calificación de la materia, constará de
dos partes, una teórica y otra práctica, que se calificarán de 0 a 5 puntos cada una de ellas. La parte teórica consistirá en pruebas tipo test, para cuya calificación las respuestas correctas suman el doble que restan las incorrectas, no puntuando las dejadas en blanco. La parte práctica consistirá en la resolución de uno o varios casos prácticos. La calificación final del examen
será la suma de las calificaciones obtenidas en cada una de las partes. Para superar la materia es necesario obtener un mínimo de 5 puntos en la suma de la calificación de ambas partes.

Fuentes 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 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

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Gestión de la seguridad de la información/V05M175V01101