Escuela de Ingeniería de Telecomunicación

(*)Páxina web

(*)

www.teleco.uvigo.es

(*)Presentación

La Escuela de Enxeñaría de Telecomunicación, con acreditación institucional desde el 28/01/2019 (RD 420/2015), oferta un grado y cuatro másteres totalmente adaptados al Espacio Europeo de Educación Superior, verificados por la ANECA y que se ajustan a las Órdenes Ministeriales CIN/352/2009 y CIN/355/2009.

Grado en Ingeniería de Tecnologías de Telecomunicación (GETT) - Bachelor□s Degree in Telecommunication Technologies Engineering

(Acreditado EUR-ACE®, 15/04/2019; Plan de Excelencia Ultreia 2020 de la Xunta de Galicia).

El Grado en Ingeniería de Tecnologías de Telecomunicación habilita para el ejercicio de las profesiones reguladas de ingeniería técnica. Las profesiones reguladas son aquellas para las que para su ejercicio se requiere cumplir una condición especial que, normalmente, es estar en posesión de un determinado título académico. En la actualidad, se rigen por el Real Decreto 1837/2008. El Espacio Europeo de Educación Superior (EEES) determinó que las atribuciones profesionales se pueden adquirir con la titulación de grado (Ingenieros e Ingenieras Técnicos) o con la titulación de máster universitario (Ingenieros e Ingenieras).

El GETT ha sido seleccionado para participar en el Plan de Excelencia del Sistema Universitario de Galicia Ultreia 2020, en el que se recogen un conjunto de acciones que tienen como objetivo que las universidades gallegas puedan dar un nuevo salto de calidad. Al amparo de este plan, a partir del curso 2018/19 **se oferta un itinerario en inglés para que, los alumnos y alumnas que así lo deseen, puedan cursar en esta lengua hasta el 80% de los créditos de la titulación**.

http://teleco.uvigo.es/images/stories/documentos/gett/diptico-uvigo-eet-grao-gal.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/gett

Máster en Ingeniería de Telecomunicación

Determinadas profesiones reguladas necesitan un nivel de estudios mayor y así, para poder ejercerlas, se requiere haber cursado un máster universitario habilitante. El Máster en Ingeniería de Telecomunicación es un máster con atribuciones profesionales plenas de Ingeniero e Ingeniera de Telecomunicación, regulado por la Orden Ministerial CIN/355/2009 de 9 de febrero de 2009 y publicado en el BOE nº 44 de 20/02/2009.

http://teleco.uvigo.es/images/stories/documentos/met/diptico-uvigo-eet-master-gal.pdf

www: http://teleco.uvigo.es/index.php/es/estudios/mit

Másteres Interuniversitarios

La oferta educativa actual del centro se completa con diferentes másteres interuniversitarios interrelacionados con el sector empresarial.

Master Interuniversitario en Ciberseguridad; www: https://www.munics.es/

Máster Interuniversitario en Matemática Industrial: www: http://m2i.es

Máster Interuniversitario en Visión por Computador: www: https://www.imcv.eu/

(*)Equipo directivo

EQUIPO DIRECTIVO DO CENTRO

Directora: Rebeca Pilar Díaz Redondo (teleco.direccion@uvigo.gal)

Secretaría e Subdirección de Novas Titulacións: Pedro Rodríguez Hernández

(teleco.subdir.secretaria@uvigo.gal;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)

COORDINACIÓN DO GRAO EN ENXEÑARÍA DE TECNOLOXÍAS DE TELECOMUNICACIÓN

Coordinadora Xeral: 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/

COORDINACIÓN DO MESTRADO EN ENXEÑARÍA DE TELECOMUNICACIÓN

Coordinador Xeral: 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/

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN CIBERSEGURIDADE

Coordinada Xeral: 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/

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN MATEMÁTICA INDUSTRIAL

Coordinadora Xeral: Elena Vázquez Cendón (USC)

Coordinador UVIGO: José Durany Castrillo (durany@dma.uvigo.es)

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

COORDINACIÓN DO MESTRADO INTERUNIVERSITARIO EN VISIÓN POR COMPUTADOR

Coordinador Xeral: Xose Manuel Pardo López (USC)

Coordinador UVIGO: José Luis Alba Castro (jalba@gts.uvigo.es)

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

COORDINADOR DO MESTRADO INTERUNIVERSITARIO EN CIENCIA E TECNOLOXÍAS DE INFORMACIÓN CUÁNTICA

Coordinador Xeral: Javier Mas (USC)

Coordinador UVIGO: Manuel Fernández Veiga(teleco.mqist@uvigo.es)

https://quantummastergalicia.es/info

Máster Universitario en Ciberseguridad

Asignaturas

Curso 1

Código	Nombre	Cuatrimestre	Cr.totales
V05M175V11108	Seguridad de la información	1c	5
V05M175V11109	Análisis de malware	1c	5
V05M175V11110	Privacidad y anonimidad	1c	5
V05M175V11111	Seguridad de aplicaciones	1c	5
V05M175V11112	Redes seguras	1c	5
V05M175V11113	Tecnologías de resgistro distribuído y Blockchain	1c	5
V05M175V11211	Seguridad en comunicaciones	2c	5
V05M175V11212	Fortificación de sistemas	2c	5
V05M175V11213	Ciberseguridade industrial e IoT	2c	5
V05M175V11214	Hacking ético y Test de intrusión	2c	5
V05M175V11215	Negocio en ciberseguridad y emprendimiento	2c	4
V05M175V11216	Análisis forense	2c	3
V05M175V11217	Seguridad en centros de datos	2c	3
V05M175V11218	Seguridad en dispositivos móviles	2c	3
V05M175V11219	Smart Contracts e dApps	2c	3

Curso 2

Código	Nombre	Cuatrimestre	Cr.totales
V05M175V11301	Gestión de seguridad de la información	1c	5
V05M175V11302	Conceptos y leyes	1c	4
V05M175V11303	Prácticas en empresa	1c	9
V05M175V11304	Trabajo Fin de Máster	1c	12

DATOS IDENTIFICATIVOS				
Seguridad de la información				
Asignatura	Seguridad de la información			
Código	V05M175V11108			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición	Inglés			
Departamento	Dpto. Externo Ingeniería telemática Teoría de la señal y comunicaciones			
Coordinador/a	Fernández Veiga, Manuel			
Profesorado	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
Correo-e	mveiga@det.uvigo.es			
Web	http://moovi.gal			
Descripción general	En esta asignatura se estudian las técnicas de criptografía y criptoanálisis, la generación de números y funciones aleatorias, los métodos de integridad de mensajes, el cifrado autenticado, el cifrado asimétrico, los métodos de privacidad y anonimato de la información, los esquemas de computación segura y la estenografía. Todas las anteriores son herramientas básicas para la protección de la información en redes y sistemas			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
1. Cifrado	Cifrado de Shannon Seguridad perfecta Seguridad semántica y computacional
2. Cifrado en flujo	Generadores pseudo aleatorios simples y compuestos Ataques Casos de estudio
3. Cifrado en bloques	Cifrado en bloques. Seguridad DES. AES Funciones pseudoaleatorias Construcción de PRF y cifrado en bloques
4. Integridad	Códigos de autenticación e integridad. Definición de seguridad. MAC con claves. Funciones pseudoaleatorias y MAC. Funciones hash. Hashing universal y hashing resistente a colisiones. Casos de estudio
5. Cifrado autenticado	Definición. Composición. Ataques. ejemplos y casos de estudio
6. Cifrado con clave pública	Definición. Seguridad semántica. Funciones de una dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas digitales. Casos de estudio
7. Cifrado avanzado	Cifrado sobre curvas elípticas. Retículos. Cifrado sobre retículos. RLWE. Ataques cuánticos. Computación homomórfica
8. Protocolos de identificación	Definición. Contraseñas (de un solo uso). Challenge-response. Sigmaprotocolos. Esquemas de Okamoto y Schnorr. Casos de estudio
9. Anonimización	Definición. t-integridad, divergencia. Análisis. Casos de estudio
10. Esteganografía y watermarking	Definiciones. Marcado de agua mediante espectro ensanchado. Codificación de papel sucio. Forensía digital.
(*)11. Computación segura	(*)Funcións computables. Computación segura a dúas vías e a varias vías. Computación interactiva. Computación homomórfica. Aplicacións.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Resolución de problemas	0	24	24
Prácticas de laboratorio	18	36	54
Lección magistral	17	51	68
Examen de preguntas de desarrollo	2	0	2
Resolución de problemas y/o ejercicios	2	0	2

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

Metodologías

	Descripción
Resolución de problemas	Los estudiantes resolverán problemas y ejercicios sobre los contenidos de las lecciones. Entrega por escrito y corrección
Prácticas de laboratorio	Los estudiantes desarrollarán en el laboratorio prácticas de seguridad de los datos y un proyecto de programación sobre cifrado, firma, anonimato o forenses digital. Las prácticas o proyectos serán supervisadas por los profesores.
Lección magistral	Exposición sistemática de los contenidos del curso: conceptos, resultados, algoritmos, ejemplos y casos de uso.

Atención personalizada

Metodologías	Descripción
Resolución de problemas	Se atenderán individualmente las consultas sobre la resolución de problemas y ejercicios planteados en las clases o trabajados de forma autónoma. El horario de tutorías puede consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Prácticas de laboratorio	Se responderán individualmente las cuestiones relativas a las prácticas de laboratorio y al desarrollo del proyecto. El horario de tutorías puede consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Lección magistral	Se dispensará atención individual a los estudiantes que precisen orientación para el estudio, explicación adicional sobre los contenidos de la disciplina, aclaración o guía sobre la resolución de problemas. El horario de tutorías puede consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Resolución de problemas	Resolución de cuestiones, problemas y ejercicios a lo largo del curso (4 cuestionarios). Entrega individual por escrito	30	
Prácticas de laboratorio	Desarrollo de proyectos de implementación de un sistema de protección de información. Pruebas funcionales y de rendimiento	30	
Examen de preguntas de desarrollo	Examen escrito. Resolución de cuestiones, problemas o ejercicios	40	

Otros comentarios sobre la Evaluación

Se dejan a discreción de los alumnos dos métodos de evaluación alternativos en la asignatura: evaluación continua y evaluación global.

La evaluación continua consistirá en la realización de un examen final (40% de la calificación), el desarrollo de prácticas y proyectos (30% de la calificación) y en la entrega a lo largo del curso de ejercicios resueltos (30%). La evaluación única consistirá en la realización de un examen final escrito (60% de la calificación) y en el desarrollo de proyectos de ingeniería a escala (dos, 30% de la calificación cada uno) que se presentará antes del último día hábil anterior al periodo oficial de exámenes. Las pruebas escritas de las modalidades de evaluación global y continua no serán necesariamente iguales.

Los alumnos podrán optarán por una u otra modalidad de evaluación hasta la fecha del examen escrito del curso.

Quienes no superen la asignatura en la convocatoria ordinaria disponen de una segunda oportunidad extraordinaria al final del curso en la que se reevaluarán sus conocimientos con una prueba escrita o se reevaluará su proyecto si se hubiera mejorado o modificado éste. Los pesos de cada una de las pruebas (examen y proyecto) serán los mismos que en el periodo ordinario de evaluación conforme a la modalidad que se hubiese elegido.

La calificación de las pruebas solo surte efecto en el curso académico en que se obtengan, con independencia del itinerario de evaluación escogido.

Fuentes de información

Bibliografía Básica

D. Boneh, V. Shoup, **A graduate course in applied cryptography**, http://toc.cryptobook.us, 2021

Bibliografía Complementaria

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

Recomendaciones

Otros comentarios

La asignatura se imparte en inglés. Es recomendable aptitud para el razonamiento matemático

DATOS IDENTIFICATIVOS				
Análisis de malware				
Asignatura	Análisis de malware			
Código	V05M175V11109			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición	Inglés			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Burguillo Rial, Juan Carlos			
Profesorado	Burguillo Rial, Juan Carlos Hernández Pereira, Elena María Rivas López, Jose Luis			
Correo-e	jrial@uvigo.es			
Web	http://https://moovi.uvigo.gal			
Descripción general	El malware utiliza los sistemas y las redes de comunicaciones para propagar virus, secuestrar dispositivos o robar datos confidenciales. El objetivo de esta asignatura es dotar al alumno de la capacidad para analizar, detectar y eliminar malware. Para ello se explorarán y ejemplificarán, de forma práctica y con casos reales, las técnicas actuales de ocultación y persistencia de malware, así como las tendencias más novedosas para su detección y eliminación. Esta asignatura se impartirá en inglés.			

Resultados de Formación y Aprendizaje	
Código	
B2	Conocer las técnicas de ocultación y persistencia de malware; así como las tendencias actuales en malware mediante el estudio de casos reales.
C2	Detectar y eliminar las vulnerabilidades susceptibles a malware, así como malware, en sistemas y redes de comunicaciones, así como evadir técnicas de ocultación y persistencia de malware.
D3	Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.
D6	Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas.

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Proporcionar al estudiante la capacidad para analizar, detectar y eliminar malware.	B2 C2
Explorar y evaluar, de forma práctica y con estudios de caso, las técnicas utilizadas hoy en día para esconder malware.	D3
Aprender a encontrar vulnerabilidades en sistemas reales, así como proteger y limitar la exposición a amenazas conocidas.	D6

Contenidos	
Tema	
Introducción al análisis e ingeniería de malware.	a) ¿Qué es el malware? b) ¿Cómo detectarlo y eliminarlo? c) ¿En qué consiste la ingeniería de malware?
Tipos de malware.	a) Estructura. b) Componentes. c) Vectores de infección.
Ingeniería de malware.	a) Técnicas de propagación. b) Procesos de infección. c) Persistencia del malware. d) Técnicas de ocultación.
Ingeniería inversa de malware.	a) ¿Cómo analizar e inferir el funcionamiento del malware? b) Comprensión del funcionamiento de nuevos tipos de malware.

Herramientas de análisis de malware.	a) Herramientas para la detección de malware. b) Herramientas para la eliminación de malware.

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Actividades introductorias	2	2	4
Lección magistral	10	30	40
Prácticas de laboratorio	15	40	55
Foros de discusión	0	2	2
Estudio de casos	5	4	9
Examen de preguntas objetivas	2	4	6
Resolución de problemas y/o ejercicios	3	6	9
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías	
	Descripción
Actividades introductorias	Hacer una introducción genérica a los objetivos, contenidos globales generales de la asignatura y resultados esperados. Esta actividad será realizada individualmente.
Lección magistral	Se introducen los distintos temas de la asignatura proporcionando el material docente necesario para su seguimiento. Con esta metodología se trabajan el conocimiento B2, la destreza C2 y la competencia D6. Esta actividad será realizada individualmente.
Prácticas de laboratorio	Se realizan prácticas de laboratorio para comprender mejor los contenidos vistos en las clases magistrales. Con esta metodología se trabaja el conocimiento B2, la destreza C2 y las competencias D3 y D6. Algunas prácticas se realizarán de forma individual y otras en grupos (dependiendo del número de estudiantes).
Foros de discusión	Los estudiantes deben participar en el foro dentro de la plataforma MOOVI. Con esta metodología se trabaja el conocimiento B2 y la competencia D6. Esta actividad será realizada individualmente.
Estudio de casos	Durante las clases magistrales se realizarán presentaciones de casos de estudio típicos de amenazas, problemas de seguridad conocidos o tecnologías actuales. Con esta metodología se trabaja el conocimiento B2, y las competencias D3 y D6. Esta actividad se realizará en grupo.

Atención personalizada	
Metodologías	**Descripción**
Actividades introductorias	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).
Lección magistral	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).
Prácticas de laboratorio	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).

Foros de discusión	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).
Estudio de casos	En las actividades formativas prácticas y tutorías, los profesores de la asignatura ofrecerán guías de atención personalizada a cada alumno sobre las tareas a realizar, con el fin de orientar el planteamiento y la metodología de elaboración. También se ofrecerá información de coordinación con otros contenidos y asignaturas del programa de estudios. Se recomienda consultar las dudas al profesorado a lo largo de todo el desarrollo de la materia, tanto para la comprensión de los fundamentos como para la realización de los proyectos y actividades de evaluación. El alumnado podrá consultar y solicitar tutorías a través de la plataforma Moovi (https://moovi.uvigo.gal).

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas de laboratorio	Los alumnos realizarán prácticas de laboratorio (3 x 15% = 45%), donde se trabajará con los conceptos estudiados en las clases teóricas.	45	
Foros de discusión	Los estudiantes deben participar en el foro de la plataforma MOOVI.	5	
Estudio de casos	El alumnado realizará presentaciones de casos de estudio, seleccionados por ellos, para analizar amenazas actuales.	15	
Examen de preguntas objetivas	Dos test de evaluación sucesivos para el contenido parcial de la materia impartida hasta ese momento. Los tests serán individuales y de tiempo limitado.	30	
Resolución de problemas y/o ejercicios	Durante las clases magistrales se realizarán preguntas a los estudiantes para conocer su comprensión del tema bajo estudio.	5	

Otros comentarios sobre la Evaluación

Los elementos que forman parte de la evaluación de la asignatura son los siguientes:
- **Cuestionarios**: a lo largo del curso se realizarán dos cuestionarios que aportarán un 15% de la nota final (cada uno).
- **Presentación de casos de estudio**: cada alumno (de forma individual o en grupo) deberá realizar una presentación original que aportará un 15% de la nota final.
- **Prácticas de laboratorio**: cada alumno deberá realizar individualmente y/o en grupo un conjunto de prácticas propuestas en el laboratorio (por defecto 3 prácticas con un peso de 15% cada una) que aportará un 45% de la nota final.
- **Participación en clase**: los estudiantes participarán y discutirán sobre las exposiciones realizadas por el profesor y esto contribuirá hasta un 5% a la nota final.
- **Participación en el foro**: los estudiantes deben participar en el foro de la asignatura, de forma individual, y esto contribuirá hasta un 5% a la nota final. Para conseguir dicho porcentaje se deben proporcionar, como mínimo, dos contribuciones relevantes.

Así tenemos:

Nota Final = Cuestionarios (2x15 = 30%) + Presentación de caso de estudio (15%) + Prácticas de lab. (45%) + Participación en clase (5%) + Foro (5%) = 100%.

Los estudiantes deben obtener al menos 4 puntos sobre 10 en la nota de los cuestionarios, los casos de estudio y las prácticas para poder calcular la nota media final. Si cualquiera de estas notas estuviese por debajo de 4, entonces la nota final obtenida nunca será superior a un 4.9 sobre 10.

La planificación de las diferentes pruebas de evaluación intermedia se aprobaraa en una Comisión Académica de Máster (CAM) y estará disponible al principio del cuatrimestre.

Siguiendo las directrices propias de la titulación se ofrecerá a los alumnos que cursen esta materia dos sistemas de evaluación: evaluación continua y evaluación única (fin del cuatrimestre).

Evaluación continua: el estudiante sigue la evaluación continua desde el momento en que se presenta a dos cuestionarios de la asignatura. Un alumno que opta por la evaluación continua se considera que se ha presentado a la asignatura, independientemente de que se presente o no a la evaluación única.

Evaluación global: el alumno deberá realizar un examen teórico que sustituye a los cuestionarios realizados a lo largo del

curso, además de entregar las prácticas y los trabajos equivalentes a los que se han realizado como parte de la evaluación continua.

Evaluación extraordinaria: el alumno deberá realizar la parte que no haya superado. En el caso de no haber superado los cuestionarios deberá realizar un examen equivalente.

Convocatoria de fin de carrera: el alumno deberá realizar la parte que no haya superado. En el caso de no haber superado los cuestionarios deberá realizar un examen equivalente.

En caso de detección de plagio en cualquiera de las pruebas (pruebas cortas, exámenes parciales o examen final), la calificación final será de SUSPENSO (0) y el hecho será comunicado a la dirección del Centro para los efectos oportunos.

Los trabajos y tareas prácticas propuestas y realizadas en este curso no son recuperables y sólo son válidas para el curso actual.

Fuentes de información

Bibliografía Básica

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

Bibliografía Complementaria

Recomendaciones

Asignaturas que se recomienda cursar simultáneamente

Análisis forense/V05M175V11216

DATOS IDENTIFICATIVOS				
Privacidad y anonimidad				
Asignatura	Privacidad y anonimidad			
Código	V05M175V11110			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición	#EnglishFriendly Castellano			
Departamento	Dpto. Externo Teoría de la señal y comunicaciones			
Coordinador/a	Pérez González, Fernando			
Profesorado	Hernández Pereira, Elena María Pérez González, Fernando			
Correo-e	fperez@gts.uvigo.es			
Web	http://http://moovi.gal			
Descripción general	Esta asignatura se presentan las principales técnicas para proporcionar privacidad y anonimidad en redes, sistemas y aplicaciones. Se estudian conceptos y métodos de privacidad diferencial, técnicas de mejora de la privacidad (PET), privacidad en la geolocalización, privacidad para aprendizaje máquina y técnicas de anonimidad. También se exploran las implicaciones de la privacidad desde el diseño y aspectos éticos y legales de la privacidad.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
Introducción. Ataques.	Introducción a la privacidad y la anonimidad. Ataques de inferencia. Ataques de análisis de tráfico. Rastreo online.
Privacidad diferencial.	Privacidad diferencial. Mecanismos para la privacidad diferencial. Teoremas de composición.
Técnicas de mantenimiento y mejora de la privacidad.	Primitivas con mantenimiento de la privacidad: recuperación de información, intersección de conjuntos. Técnicas de mejora de la privacidad con cifrado homomórfico y computación multipartita segura. Filtros de Bloom.
Anonimidad.	Conceptos básicos. K-anonimidad, l-diversidad y t-proximidad.
Aplicaciones en privacidad y anonimidad.	Privacidad de la geolocalización. Comunicaciones anónimas. Encaminamiento en cebolla. Mixes. Autenticación anónima. Privacidad en aprendizaje máquina.

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Prácticas de laboratorio	19	38	57
Lección magistral	19	38	57
Resolución de problemas	2	0	2
Examen de preguntas objetivas	2	0	2
Informe de prácticas, prácticum y prácticas externas	0	3	3
Informe de prácticas, prácticum y prácticas externas	0	4	4

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

Metodologías
Descripción

Prácticas de laboratorio	Los estudiantes desarrollarán en el laboratorio prácticas de privacidad y anonimidad como aplicaciones de las técnicas presentadas en las lecciones magistrales. Las prácticas o proyectos serán supervisadas por los profesores.
Lección magistral	Exposición sistemática de los contenidos del curso: conceptos, resultados, algoritmos, ejemplos y casos de uso.
Resolución de problemas	Resolución de problemas en el aula por parte de los docentes.

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	Se responderán individualmente las cuestiones relativas a las prácticas de laboratorio y al desarrollo del proyecto. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Lección magistral	Se dispensará atención individual a los estudiantes que precisen orientación para el estudio, explicación adicional sobre los contenidos de la disciplina, aclaración o guía sobre la resolución de problemas. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Resolución de problemas	Se atenderán individualmente las consultas sobre la resolución de problemas y ejercicios planteados en las clases o trabajados de forma autónoma. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Examen de preguntas objetivas	Examen escrito. Resolución de cuestiones, problemas o ejercicios.	40	
Informe de prácticas, prácticum y prácticas externas	Informes sobre las prácticas correspondientes a la primera parte del curso realizadas individualmente o por parejas.	30	
Informe de prácticas, prácticum y prácticas externas	Informes sobre las prácticas correspondientes a la segunda parte del curso realizadas individualmente o por parejas.	30	

Otros comentarios sobre la Evaluación

Es necesario alcanzar un mínimo de 4.00 en el examen escrito para poder aprobar la asignatura.

En los informes de prácticas, será necesario indicar si se emplearon herramientas de IA generativa y, de ser así, hacer constar explícitamente qué elementos del informe fueron producidos con ellas. En caso de detección de plagio o de uso no justificado de dichas herramientas, los profesores podrán calificar el entregable con 0 puntos.

La calificación de las pruebas solo tendrá efecto en el curso académico en que se obtengan.

Fuentes de información

Bibliografía Básica

C. Dwork, **The Algorithmic Foundations of Differential Privacy**, Now Publishers Inc., 2013

J. Morris Chang, Di Zhuang, and G. Dumindu Samaraweer, **Privacy-preserving Machine Learning**, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, GCATI, 2020

Bibliografía Complementaria

Katharine Jarmul, **Practical Data Privacy**, O'Reily Media, 2023

Nishant Bhajaria, **Data Privacy**, Manning Publications, 2022

PALISADE, **PALISADE HOMOMORPHIC ENCRYPTION SOFTWARE LIBRARY**,

Ilaria Chillotti, **TFHE Deep Dive**, https://www.zama.ai/post/tfhe-deep-dive-part-1,

Daniele Micciancio, and Oded Regev, **Lattice-based cryptography**, https://cseweb.ucsd.edu/%7Edaniele/papers/PostQuantum.pdf, Springer, 2009

Recomendaciones

DATOS IDENTIFICATIVOS				
Seguridad de aplicaciones				
Asignatura	Seguridad de aplicaciones			
Código	V05M175V11111			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición	Castellano			
Departamento	Ingeniería telemática			
Coordinador/a	Fernández Vilas, Ana			
Profesorado	Bellas Permuy, Fernando Losada Pérez, José			
Correo-e	avilas@uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530104&idioma=cast&any_academic=2024_25			
Descripción general	Desarrollar aplicaciones seguras no es una tarea trivial. Conocer las vulnerabilidades que habitualmente sufren las aplicaciones, los mecanismos de autenticación, autorización y control de acceso, así como la incorporación de la seguridad al ciclo de vida de desarrollo, es esencial para poder construir y mantener aplicaciones seguras con éxito. En esta materia se estudian de forma práctica todos estos aspectos, con especial énfasis en el desarrollo de aplicaciones y servicios web.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos
Tema

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías
Descripción

Atención personalizada

Evaluación		
Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS

Redes seguras

Asignatura	Redes seguras			
Código	V05M175V11112			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición				
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Rodríguez Rubio, Raúl Fernando			
Profesorado	Nóvoa de Manuel, Francisco Javier Rodríguez Rubio, Raúl Fernando			
Correo-e	rrubio@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530105&fitxa_apartat=3&any_academic=2024_25&idioma_assig=&any_academic=2024_25			
Descripción general	La materia Redes Seguras tiene como objetivo principal que los estudiantes aprendan a diseñar e implementar infraestructuras de red que sean capaces de proporcionar los servicios de seguridad necesarios en un entorno corporativo moderno. Deberán conocer las arquitecturas de seguridad de referencia y ser capaces de configurarlas y administrarlas, utilizando para ello tecnologías como IDS/IPS y Firewalls, entre otras. La materia esta concebida para que las prácticas de laboratorio, con equipos físicos y virtuales tengan una importancia capital en el proceso de aprendizaje.			

Resultados de Formación y Aprendizaje

Código

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos

Tema

Planificación

	Horas en clase	Horas fuera de clase	Horas totales

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

Metodologías

	Descripción

Atención personalizada

Evaluación

Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS				
Tecnoloxías de rexistro distribuído e Blockchain				
Asignatura	Tecnoloxías de rexistro distribuído e Blockchain			
Código	V05M175V11113			
Titulacion	Máster Universitario en Ciberseguridade			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición				
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Fernández Iglesias, Manuel José			
Profesorado	Álvarez Sabucedo, Luis Modesto Fernández Caramés, Tiago Manuel Fernández Iglesias, Manuel José			
Correo-e	manolo@uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530106&any_academic=2024_25			
Descripción general	Na materia adquírense os coñecementos básicos das tecnoloxías basadas en rexistro distribuído (DLTs) e Blockchain.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contidos
Tema

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodoloxía docente
Descripción

Atención personalizada

Avaliación		
Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Seguridad en comunicaciones				
Asignatura	Seguridad en comunicaciones			
Código	V05M175V11211			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Rodríguez Rubio, Raúl Fernando			
Profesorado	Fernández Iglesias, Diego Rodríguez Rubio, Raúl Fernando Suárez González, Andrés			
Correo-e	rrubio@det.uvigo.es			
Web	http://https://moovi.uvigo.gal			
Descripción general	Esta materia realiza un repaso por las capas de la arquitectura de comunicaciones de Internet, mostrando sus principales debilidades desde el punto de vista de la seguridad y proporcionando las técnicas y herramientas necesarias para mitigarlas. Los estudiantes conocerán en detalle los protocolos de red que aportan seguridad a la transmisión de la información, y las implicaciones derivadas del lugar que ocupan dentro de la arquitectura en que se organiza el software de comunicaciones.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
Arquitectura y protocolos de Internet	Conceptos fundamentales.
Seguridad en el nivel de enlace	Seguridad en redes cableadas/Ethernet: Control de acceso y autenticación basada en puertos Confidencialidad en redes Ethernet Seguridad en redes inalámbricas/WiFi: WPA/2/3 seguridad personal WPA/2/3 seguridad empresarial
Seguridad en el nivel de red	IPsec Protocolos de seguridad Gestión dinámica de claves Mecanismos de autenticación
Asegurando la infraestructura de Internet	Encaminamiento seguro Seguridad en DNS Seguridad en TCP
Seguridad en la transmisión de los datos	El protocolo TLS Suites criptográficas Infraestructura WebPKI Validación de certificados
Seguridad en redes móviles	Arquitectura del sistema Asociación y autenticación del terminal/usuario Privacidad

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	21	21	42
Prácticas de laboratorio	19	19	38
Prácticas con apoyo de las TIC	0	58	58
Examen de preguntas de desarrollo	2	0	2

Informe de prácticas, prácticum y prácticas externas	0	10	10

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

Metodologías	
	Descripción
Lección magistral	Las sesiones magistrales siguen el esquema habitual para este tipo de docencia. En estas sesiones se trabajan las competencias CG3, CE1, CE2, CE4, CE8
Prácticas de laboratorio	Se realizarán varias sesiones prácticas guiadas por los profesores donde se asentarán los conceptos aprendidos en las clases teóricas. En dichas prácticas se utilizarán dispositivos de red reales (routers y switches) y/o software de virtualización que permitirá al alumno su instrucción y entrenamiento en su propia casa. De forma natural, las actividades definidas podrán incluir apartados/retos adicionales que complementarán el trabajo autónomo del estudiante, que se describe en el siguiente item. Los alumnos deben adquirir en las prácticas las competencias CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
Prácticas con apoyo de las TIC	Más allá de las prácticas guiadas, el alumno tendrá que desplegar/configurar/implementar algunas soluciones particulares, para ciertos escenarios, de forma autónoma.En estas actividades se trabajan las competencias CB2, CB4, CB5, CG1, CG3, CG5, CE1, CE4, CE8

Atención personalizada	
Metodologías	**Descripción**
Lección magistral	Durante las horas de tutoría los docentes realizarán una atención personalizada para fortalecer u orientar al alumno en la comprensión de los conceptos teóricos explicados en las clases magistrales o en las sesiones demostrativas de carácter práctico; y para corregir o reorientar los pequeños trabajos prácticos optativos derivados de dichas clases de laboratorio. Tutorías: Raúl Rodríguez Rubio https://moovi.uvigo.gal/user/profile.php?id=11315 Andrés Suárez González https://moovi.uvigo.gal/user/profile.php?id=11340 Diego Fernández Iglesias https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614
Prácticas de laboratorio	Esta actividad es interactiva por definición, por lo que se espera que las cuestiones fluyan con naturalidad entre docentes y estudiantes, pudiendo involucrar a otros estudiantes en las respuestas buscadas.
Prácticas con apoyo de las TIC	Aunque el trabajo autónomo está orientado a que el estudiante resuelva por si mismo situaciones/retos que se encontrará en los sistemas reales, en las horas de tutoría los docentes podrán orientarlo cuestionando los soluciones elegidas o sugiriendo caminos alternativos.

Evaluación			
	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas de laboratorio	Serán calificadas como apto/no apto. El alumno será apto si asiste a todas las sesiones de este tipo. Si por algún motivo se perdiese alguna, deberá suplirla realizando alguna práctica complementaria que el profesor definirá en su momento. En algunas de las sesiones/actividades se podrá solicitar al alumno un trabajo autónomo adicional (y su informe asociado) que se evaluará cuantitativamente dentro del ítem más general que denominamos "Prácticas autónomas a través de TIC"	0	
Prácticas con apoyo de las TIC	Los estudiantes tendrán que realizar, ante los profesores, la demostración práctica que muestre la resolución de los distintos retos técnicos planteados, enfrentándose a preguntas sobre las soluciones adoptadas y su grado de completitud. Esta defensa/entrevista tendrá lugar, por término general, tras la entrega de la última tarea encargada y antes del periodo oficial de exámenes de cada convocatoria; consensuándose la fecha concreta entre alumnos y profesores con antelación suficiente. Todo reto o actividad autónoma exigirá un informe escrito, cuya estructura, composición y legibilidad tendrán su peso en la valoración final.	60	
Examen de preguntas de desarrollo	Se realizará un exámen escrito al final del cuatrimestre, donde se evalúan tanto los conceptos teóricos impartidos en las sesiones magistrales, como los fundamentos prácticos derivados de las clases/trabajos prácticos acometidos.	40	
Informe de prácticas, prácticum y prácticas externas	El trabajo autónomo del alumno deberá ser recogido en el/los informes de prácticas pertinentes, y su valoración formará parte de la valoración integral de aquél.	0	

Otros comentarios sobre la Evaluación

La evaluación de la materia podrá seguir el canal de evaluación continua o bien evaluación global. Un alumno elegirá evaluación continua al entregar la solución e informe del primer reto o trabajo autónomo que se le plantee durante el devenir normal del curso. Los porcentajes expresados en el epígrafe anterior sólo reflejan el máximo obtenible en cada tipo de prueba en la modalidad de evaluación continua; y son sólo orientativos. La forma de evaluación detallada se expresa a continuación:

Para la evaluación continua (oportunidad ordinaria), la nota final será la media geométrica ponderada entre la nota del trabajo autónomo (TA, 60%) y la calificación correspondiente al examen de preguntas de desarrollo (E, 40%). La nota TA será la media aritmética de las calificaciones asociadas a cada uno de los retos/prácticas autónomas que el alumno tendrá que resolver a lo largo del cuatrimestre, que nunca serán menos de dos.

NOTA FINAL(EC)=(TA^0.6)×(E^0.4)

Si las prácticas de laboratorio fueron calificadas como no aptas, la nota será la mínima entre la nota del examen escrito (E) y 3.

Los alumnos que opten por la evaluación global deberán presentarse a un examen final que consistirá de tres partes: una prueba escrita análoga a la prueba de evaluación continua (E), una prueba de aptitud en el laboratorio y uno o varios trabajos prácticos (T). La nota final, en este caso, es la media geométrica ponderada entre la nota de teoría (E, 80%) y el trabajo práctico (T, 20%), con la condición de que se supere la prueba de aptitud. Si el alumno no supera la prueba de aptitud, la nota final será el mínimo entre E y 3.

NOTA FINAL(EU)=(T^0.2)×(E^0.8)

Finalmente, para la oportunidad extraordinaria (junio/julio), el alumno podrá proseguir con el modo de evaluación que ya había elegido (conservándosele la nota de la parte -E o TA/T- que hubiera superado, y afrontando únicamente la parte suspensa - con posibles modificaciones en las especificaciones de los trabajos prácticos), o afrontar desde cero una evaluación que tendrá las mismas características que el examen final que acabamos de describir. La prueba de aptitud sólo será necesaria si no asistió a todas las sesiones del laboratorio.

Fuentes de información

Bibliografía Básica

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 Inamdar, **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

Bibliografía Complementaria

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,

Recomendaciones

DATOS IDENTIFICATIVOS				
Fortificación de sistemas				
Asignatura	Fortificación de sistemas			
Código	V05M175V11212			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Blanco Fernández, Yolanda			
Profesorado	Blanco Fernández, Yolanda Yáñez Izquierdo, Antonio Fermín			
Correo-e	yolanda@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530108&any_academic=2024_25			
Descripción general	Un sistema operativo recién instalado es intrínsecamente inseguro. Presenta ciertas vulnerabilidades en función de factores como la antigüedad del S.O., la existencia de puertas traseras, los servicios que proporciona y el uso de políticas por defecto que no tienen la seguridad como objetivo principal. Por fortificación de un S.O. nos referimos al acto de configurar este S.O. con la intención de hacerlo lo más seguro posible, tratando de minimizar el riesgo de que se vea comprometido para ser explotado por alguna de las vulnerabilidades. Esto suele implicar la aplicación de parches de seguridad, el cambio de ciertas políticas por defecto del S.O. y la eliminación (o desactivación) de aplicaciones y servicios no esenciales. La guía de la asignatura está disponible en el enlace especificado de la UDC.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos
Tema

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías
Descripción

Atención personalizada

Evaluación		
Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS				
Ciberseguridade industrial e IoT				
Asignatura	Ciberseguridade industrial e IoT			
Código	V05M175V11213			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Castellano Gallego			
Departamento	Dpto. Externo Ingeniería de sistemas y automática Ingeniería telemática			
Coordinador/a	Diaz-Cacho Medina, Miguel Ramón			
Profesorado	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel Gil Castiñeira, Felipe José			
Correo-e	mcacho@uvigo.es			
Web	http://www.moovi.gal			
Descripción general	Los dispositivos inteligentes nos están prestando cada vez más servicios casi sin que nos demos cuenta de su presencia: el coche ha dejado de ser una simple máquina mecánica para convertirse en un sistema conectado con un enorme control electrónico; en los hoteles ya no usamos llave, sino que podemos abrir nuestra habitación con una tarjeta o nuestro teléfono móvil; Nuestros termostatos domésticos se pueden conectar a un servicio de pronóstico del tiempo y ajustarse al clima en las próximas horas. Los entornos industriales son casos de uso particularmente importantes, ya que la conexión en red de dispositivos que miden y controlan procesos permite la Industria 4.0. Todos son ejemplos de las aplicaciones habilitadas por tecnologías "integradas", redes de comunicaciones inalámbricas y, en última instancia, "Internet de las cosas" (IoT). Esta asignatura analiza los problemas y las mejores prácticas para hacer que este tipo de sistemas sean seguros, con especial énfasis en la seguridad de las tecnologías de la Industria 4.0, como los sistemas IoT/IioT, los sistemas robóticos, la computación en la nube/borde, la realidad aumentada, la cadena de bloques o los AGV.			

Resultados de Formación y Aprendizaje	
Código	
B9	Identificar la arquitectura de los sistemas IoT, su complejidad y sus vulnerabilidades, así como comprender la seguridad en el ámbito los sistemas empotrados y los sistemas de comunicación IoT.
C9	Analizar las implicaciones del nivel de seguridad de tecnologías relacionadas con la digitalización de los sectores de producción, así como valorar y modelar amenazas y ejecutar ataques con el objetivo de diseñar sistemas IoT seguros.
D2	Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
D5	Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones.
D7	Aplicar políticas de seguridad e implementar las diferentes técnicas de protección en base a la comprensión de los ataques en sistemas industriales para minimizar las problemáticas de seguridad y los ataques a redes de control industrial.

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
RA01. Comprender la ejecución de políticas de seguridad y sus implicaciones en entornos industriales.	B9 C9 D7
RA02. Comprender las diferentes técnicas de protección y ataque en sistemas industriales y saber cómo se pueden implementar.	B9 C9 D2 D5 D7

RA03. Entender las problemáticas de seguridad y los ataques a redes de control industrial y conocer los mecanismos que permiten minimizarlos.	B9 C9 D5 D7
RA04. Conocer e identificar la arquitectura de los sistemas IoT, su complejidad y sus vulnerabilidades	B9
RA05. Comprender la seguridad en el ámbito de los sistemas empotrados	B9 C9 D2 D5 D7
RA06. Comprender la seguridad en el ámbito de los sistemas de comunicación IoT.	B9 C9 D5
RA07. Conocer casos reales de ataques a sistemas IoT.	B9 D7
RA08. Ser capaz de comprender las implicaciones a nivel de seguridad de tecnologías relacionadas con conceptos como la Industria 4.0/5.0.	B9 C9 D5 D7
RA09. Ser capaz de valorar y modelar amenazas y ejecutar ataques sobre un sistema IoT	B9 C9 D2
RA10. Ser capaz de diseñar sistemas IoT seguros	B9 C9 D2 D5 D7

Contenidos

Tema	
Introducción a la ciberseguridad industrial.	Introducción a la ciberseguridad industrial.
Introducción a los sistemas ciberfísicos e IoT: hardware, firmware, comunicaciones y cloud	Introducción a los sistemas ciberfísicos e IoT: hardware, firmware, comunicaciones y cloud
Ciberseguridad de sistemas de control y comunicaciones industriales.	Ciberseguridad de sistemas de control y comunicaciones industriales.
Ciberseguridad de tecnologías de la Industria 4.0/5.0.	Ciberseguridad de tecnologías de la Industria 4.0/5.0.
Ciberseguridad de dispositivos IoT/IIoT: hardware, firmware y middleware.	Ciberseguridad de dispositivos IoT/IIoT: hardware, firmware y middleware.
Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica.	Ciberseguridad en entornos IIoT: sistemas de posicionamiento y sensórica.
Ciberseguridad en comunicaciones inalámbricas para dispositivos IoT/IioT.	Ciberseguridad en comunicaciones inalámbricas para dispositivos IoT/IioT.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Aprendizaje basado en proyectos	5	45	50
Lección magistral	14	20	34
Prácticas con apoyo de las TIC	15	25	40
Examen de preguntas objetivas	1	0	1

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

Metodologías

	Descripción
Aprendizaje basado en proyectos	Implementación grupal del diseño, implementación y pruebas de un sistema IoT, con especial énfasis en la seguridad. Realizar ataques grupales a la seguridad de los sistemas implementados por otros compañeros o terceros.
Lección magistral	Presentación, por parte del profesorado, de los principales contenidos teóricos relacionados con la seguridad industrial e IoT (seguridad embebida, en comunicaciones y backends, con especial foco en entornos industriales)
Prácticas con apoyo de las TIC	Realización por parte de los alumnos de prácticas guiadas y supervisadas.

Atención personalizada

Metodologías	Descripción
Aprendizaje basado en proyectos	El profesorado de la asignatura prestará una atención individual y personalizada al alumnado durante el curso, resolviendo sus dudas y preguntas. Asimismo, el profesorado orientará al alumnado durante la realización del proyecto. Las dudas se resolverán durante las tutorías en grupo, o en el horario establecido para las tutorías. El horario de tutorías se establecerá al inicio del curso y se publicará en la web de la asignatura.
Lección magistral	El profesorado de la asignatura prestará una atención individual y personalizada al alumnado durante el curso, resolviendo sus dudas y preguntas. Las dudas se resolverán durante la propia sesión magistral, o en el horario establecido para las tutorías. El horario de tutorías se establecerá al inicio del curso y se publicará en la web de la asignatura.
Prácticas con apoyo de las TIC	El profesorado de la asignatura prestará una atención individual y personalizada al alumnado durante el curso, resolviendo sus dudas y preguntas. Asimismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que les hayan sido asignadas, tanto en las prácticas. Las dudas se resolverán bien durante las propias clases o bien en el horario establecido para las tutorías.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje		
Aprendizaje basado en proyectos	El alumnado se dividirá en grupos para la realización del diseño, implementación y prueba de un sistema IoT, poniendo un énfasis especial en la seguridad y/o realizará ataques a la seguridad de los sistemas implementados por otros compañeros/as o por terceros. El proyecto realizado, y el informe que contiene el resultado de los ataques completados (en cuanto a su calidad y a su éxito) serán evaluados después de su entrega valorando aspectos como la corrección, la calidad, las prestaciones y las funcionalidades. Se deberá entregar el código, prototipos y documentación realizados. Asimismo, será necesario realizar una presentación de los resultados. Durante la realización del proyecto se realizará un seguimiento continuo del diseño y de la evolución de la implementación. Si los resultados intermedios no son satisfactorios, se podrá aplicar una penalización de hasta el 20% de la nota. El seguimiento será grupal e individual: cada uno de lo miembros del grupo debe documentar las tareas desarrolladas dentro de su equipo y responder sobre ellas.	40	B9	C9	D2 D5 D7
Prácticas con apoyo de las TIC	Resolución de prácticas y realización de informes con los resultados obtenidos.	30	B9	C9	D2 D5 D7
Examen de preguntas objetivas	Examen escrito sobre los contenidos teóricos y prácticos impartidos durante el curso.	30	B9	C9	D2 D5 D7

Otros comentarios sobre la Evaluación

Para superar la asignatura es necesario completar las distintas partes en las que se divide (examen o exámenes acerca de los contenidos expuestos en la sesión magistral y el proyecto). La nota final será el resultado de aplicar la **media geométrica ponderada** de la nota de cada una de las partes.

Así, si la nota de las sesiones magistrales es NT, la nota del proyecto es NP y la nota de las prácticas es NL, la nota final será:

Nota = NT^0.3 × NP^0.4 × NL^0.3

Durante el primer mes, el estudiantado deberá indicar explícitamente y por escrito su deseo de cursar la materia siguiendo la evaluación global. En otro caso se considerará que siguen la evaluación continua. Quienes sigan la evaluación continua no se podrán considerar "no presentados" así que hayan realizado la entrega del primer cuestionario o tarea.

El alumnado que opte por la evaluación global deberá presentar adicionalmente un *dossier* que deberá defender presencialmente ante el profesorado, en el que se incluyan todos los detalles sobre la realización de las distintas tareas, y muy especialmente el proyecto. En el caso de seguir la evaluación global, los alumnos/as deberán realizar el trabajo de forma individual, salvo que el profesorado les comunique explícitamente la autorización para realizarlo en grupo.

Evaluación extraordinaria

Solo podrán optar a la evaluación extraordinaria quien no supere la primera oportunidad (al finalizar el cuatrimestre). La evaluación será la descrita en los apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante el profesorado, en el que se incluyan todos los detalles sobre la realización de las

distintas tareas, muy especialmente el proyecto.

Quien hubiese seguido la evaluación continua puede optar por mantener las notas obtenidas en la primera oportunidad para las distintas partes de la asignatura o descartarlas.

Otros comentarios

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor. Aunque el proyecto se desarrollará (en la medida de lo posible) en grupos, el alumnado debe guardar evidencias de su trabajo individual dentro del grupo. En el caso en el que el rendimiento de un alumno o alumna no sea acorde al de sus compañeros de grupo, se considerará su expulsión del mismo y/o podrá ser evaluado/a de forma completamente individual en esta parte.

El uso de cualquiera material durante la realización de los exámenes tendrá que ser autorizado explícitamente por el profesorado.

En caso de detección de plagio o de comportamiento no ético en alguno de los trabajos/pruebas realizadas, la calificación de la materia será de "suspenso (0)" y los profesores comunicarán el asunto a las autoridades académicas para que tomen las medidas oportunas.

En la realización de las actividades académicas de esta materia se permite el uso de inteligencia artificial generativa (IAG). Su uso debe realizarse de forma ética, crítica y responsable. En el caso de utilizar IAG, debe evaluarse de forma crítica cualquier resultado que proporcione, y verificar de forma cuidadosa cualquier cita o referencia generada. Asimismo, se recomienda declarar el uso de las herramientas utilizadas.

Fuentes de información

Bibliografía Básica

Brian Russell, Drew Van Duren,, **Practical Internet of Things Security**, 978-1788625821, 2, Packt Publishing, 2018

Eric Knapp, Joel Thomas Langill, **Industrial Network Security**, 978-0-12-420114-9, 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,**, 978-1788395151, Packt, 2017

Bibliografía Complementaria

Houbing Song, Glenn A. Fink, Sabina Jeschke, **Security and Privacy in Cyber-Physical Systems. Foundations, Principles, and Applications.**, 978-1-119-22604-8, 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

Recomendaciones

DATOS IDENTIFICATIVOS				
Hacking ético y Test de intrusión				
Asignatura	Hacking ético y Test de intrusión			
Código	V05M175V11214			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Costa Montenegro, Enrique			
Profesorado	Carballal Mato, Adrián Costa Montenegro, Enrique			
Correo-e	kike@gti.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530110&any_academic=2024_25&idioma=cast			
Descripción general	No hay mejor forma de probar la fuerza de un sistema que atacarlo. Las pruebas de *intrusión sirven para reproducir los intentos de acceso de un atacante usando las vulnerabilidades que pueden existir en una infraestructura dada. En este curso se abordarán los temas fundamentales orientados a las pruebas de *intrusión (*pentesting), que abarcan las diferentes fases de un ataque y explotación (desde el reconocimiento y control del acceso a la eliminación de pistas).No hay una mejor forma de probar la fortaleza de un sistema que atacarlo. Los Test de Intrusión sirven para reproducir intentos de acceso de un atacante valiéndose de las vulnerabilidades que puedan existir en una determinada infraestructura. En este curso se cubrirán los temas fundamentales orientados a los test de intrusión (pentesting) cubriendo las distintas fases de un ataque y explotación (desde el reconocimiento y el control de acceso hasta el borrado de huellas).			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos
Tema

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías
Descripción

Atención personalizada

Evaluación		
Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS

Negocio en ciberseguridad y emprendimiento

Asignatura	Negocio en ciberseguridad y emprendimiento			
Código	V05M175V11215			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	4	OB	1	2c
Lengua Impartición				
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Fernández Vilas, Ana			
Profesorado	Carneiro Díaz, Victor Manuel Fernández Vilas, Ana			
Correo-e	avilas@uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530111&any_academic=2024_25&idioma=cast&any_academic=2024_25			
Descripción general	En la asignatura Negocios en ciberseguridad y emprendimiento se aborda la seguridad como un elemento transversal en la organización, desde el punto de vista estratégico y de generación de negocio. Se presentan diferentes enfoques de la monetización de los datos y su seguridad, así como los diferentes perfiles profesionales presentes en la organización, centrándose en el funcionamiento de un Centro de Operaciones de Seguridad (SOC) y sus herramientas asociadas. Finalmente, se abordan diferentes casos de éxito y oportunidades de negocio orientadas a diferentes sectores productivos, con especial atención al emprendimiento.			

Resultados de Formación y Aprendizaje

Código

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos

Tema

Planificación

	Horas en clase	Horas fuera de clase	Horas totales

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

Metodologías

	Descripción

Atención personalizada

Evaluación

Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS				
Análisis forense				
Asignatura	Análisis forense			
Código	V05M175V11216			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Suárez González, Andrés			
Profesorado	Suárez González, Andrés Vázquez Naya, José Manuel			
Correo-e	asuarez@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530112&any_academic=2024_25			
Descripción general	El análisis forense de equipos consiste en la aplicación de técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Esta materia tiene una fuerte componente práctica. Se comenzará con una introducción a la informática forense, explicando conceptos clave. A continuación, se estudiarán fundamentos y metodologías de análisis forense desde un punto de vista genérico y aplicable a nuevos casos, pero también se estudiarán ejemplos concretos basados en casos reales. En las prácticas de laboratorio el/la alumno/a aprenderá a manejar diferentes herramientas de análisis forense y realizará prácticas simulando problemas reales.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos
Tema

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías
Descripción

Atención personalizada

Evaluación		
Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS				
Seguridad en centros de datos				
Asignatura	Seguridad en centros de datos			
Código	V05M175V11217			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Suárez González, Andrés			
Profesorado	Dafonte Vázquez, José Carlos López Rivas, Antonio Daniel Suárez González, Andrés			
Correo-e	asuarez@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530113&any_academic=2024_25			
Descripción general	La seguridad en un centro de procesamiento de datos implica la implementación de una variedad de medidas físicas y lógicas para proteger la infraestructura y los datos almacenados en el CPD, con el objetivo de garantizar la disponibilidad, confidencialidad e integridad de la información y los sistemas críticos para una organización. En esta asignatura se realizará una introducción a las distintas arquitecturas de centros de datos así como a las instalaciones física auxiliares que son necesarias para su funcionamiento.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos
Tema

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías
Descripción

Atención personalizada

Evaluación		
Descripción	Calificación	Resultados de Formación y Aprendizaje

Otros comentarios sobre la Evaluación

Fuentes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS				
Seguridad en dispositivos móviles				
Asignatura	Seguridad en dispositivos móviles			
Código	V05M175V11218			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano Gallego Inglés			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	López Bravo, Cristina			
Profesorado	Fernández Caramés, Tiago Manuel López Bravo, Cristina Rivas López, Jose Luis			
Correo-e	clbravo@det.uvigo.es			
Web	http://http://moovi.uvigo.gal			
Descripción general	En esta materia se muestra una visión general de la seguridad en dispositivos móviles con diferentes características. Partiendo del estudio de la arquitectura de estos dispositivos, descubriremos su funcionamiento interno y cuáles son las principales herramientas de seguridad que incluyen, junto con los riesgos y amenazas que sufren. Estudiaremos cómo encontrar, analizar y mitigar las vulnerabilidades que afectan a los dispositivos móviles, usando herramientas de análisis forense, de desarrollo de aplicaciones seguras y de gestión de dispositivos en entornos empresariales. La documentación de esta materia estará en inglés.			

Resultados de Formación y Aprendizaje	
Código	
B14	Distinguir los conceptos fundamentales asociados con la seguridad en los sistemas operativos para móviles y el desarrollo de apps seguras, así como los sistemas gestión de dispositivos móviles.
C14	Identificar vulnerabilidades en sistemas operativos y aplicaciones propios de los dispositivos móviles, así como realizar un análisis forense y definir la política de seguridad que afecta a las comunicaciones y sistemas móviles de una organización.
D3	Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.
D8	Realizar test de intrusión en entornos prácticos complejos para la identificación de vulnerabilidades, así como para realizar ataques en entornos controlados con juicio crítico y ético.
D9	Aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad mediante técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Conocer los conceptos fundamentales asociados con la seguridad en los sistemas operativos móviles y desarrollo de apps seguras.	B14 C14
Identificar una app con comportamiento malicioso y vulnerabilidades en sistemas operativos y apps	C14 D3
Ser capaz de realizar un análisis forense de un dispositivo móvil	C14 D8 D9
Conocer los sistemas de gestión de los dispositivos móviles	B14 C14

Contenidos
Tema
Introducción: Amenazas y vulnerabilidades que afectan a los dispositivos móviles
Arquitecturas de dispositivos móviles

Modelos de seguridad de dispositivos móviles	
Desarrollo de aplicaciones seguras	Permisos Gestión de paquetes Gestión de usuarios APIs
Seguridad de los datos	
Seguridad de los dispositivos	
Seguridad de la red	
Vulnerabilidades, exploits y aplicaciones maliciosas	
Análisis forense de sistemas operativos móviles	
Sistemas de Gestión de Movilidad Empresarial (EMM)	

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	9	9	18
Prácticas con apoyo de las TIC	12	12	24
Examen de preguntas objetivas	2	14	16
Resolución de problemas y/o ejercicios	0	5	5
Informe de prácticas, prácticum y prácticas externas	0	12	12
*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 profesorado, de los principales contenidos teóricos relacionados con la seguridad en dispositivos móviles. Con esta metodología se contribuirá a la adquisición de las competencias B14 y C14.
Prácticas con apoyo de las TIC	Realización por parte del alumnado de prácticas guiadas y supervisadas. Con esta metodología se trabajarán las competencias C14, D3, D8 y D9.

Atención personalizada

Metodologías	Descripción
Prácticas con apoyo de las TIC	El conjunto de profesores de la materia proporcionará atención individual y personalizada a los alumnos y alumnas durante el curso, solucionando sus dudas y preguntas. Asimismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas con apoyo de TIC. Las dudas se atenderán de forma presencial o telemática (durante las propias prácticas, o durante el horario de tutorías). El horario de tutorías se establecerá al inicio del curso y se publicará en la página web de la materia. Fuera de ese horario, será preciso reservar las tutorías mediante cita previa.
Lección magistral	El conjunto de profesores de la materia proporcionará atención individual y personalizada a los alumnos y alumnas durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial y telemática (durante la propia sesión magistral, o durante el horario de tutorías). El horario de tutorías se establecerá al inicio del curso y se publicará en la página web de la materia. Fuera de ese horario, será preciso reservar las tutorías mediante cita previa.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Examen de preguntas objetivas	Examen de preguntas cortas sobre los contenidos teóricos y prácticos revisados al largo del curso, tanto en las sesiones magistrales, como en las prácticas de laboratorio. Este examen se realizará al finalizar el cuatrimestre.	40	
Resolución de problemas y/o ejercicios	Resolución de problemas en los que se haga uso de los conocimientos adquiridos tanto en las sesiones de teoría como de prácticas. Esta prueba se realizará al largo del cuatrimestre, con entregas parciales en las fechas indicadas por el profesorado.	25	
Informe de prácticas, prácticum y prácticas externas	El alumnado completará de forma individual cuestionarios y/o informes de prácticas donde mostrarán la correcta realización y comprensión de las prácticas.	35	

Otros comentarios sobre la Evaluación

OPORTUNIDAD ORDINARIA

Siguiendo las directrices propias de la titulación se ofertarán a quien curse esta materia dos sistemas de evaluación: evaluación continua y evaluación global.

Antes de que finalice la cuarta semana del curso, los y las estudiantes deberán indicar al profesorado de la materia el sistema de evaluación elegido. Quien opte por el sistema de evaluación continua no podrá ser calificado como "no presentado" si realiza una entrega o prueba de evaluación con posterioridad a la comunicación de su decisión.

Evaluación continua

La calificación final de la materia será igual a la media aritmética ponderada de las pruebas indicadas previamente. Para superar la materia la calificación final debe ser mayor o igual que cinco.

Evaluación global

La calificación final de la materia será igual a la media aritmética ponderada de las pruebas indicadas previamente. En este caso, la prueba de resolución de problemas se hará en una única prueba al finalizar el cuatrimestre. Para superar la materia, la calificación final debe ser mayor o igual que cinco.

OPORTUNIDAD EXTRAORDINARIA

La evaluación consistirá en realizar un examen de preguntas objetivas, un examen de resolución de problemas y entregar los informes de prácticas de todas las prácticas realizadas al largo del curso.

OTROS COMENTARIOS

Las puntuaciones obtenidas solo son válidas para el curso académico en vigor.

El uso de cualquiera material durante la realización de los exámenes y pruebas de evaluación deberá ser autorizado explícitamente por el profesorado de la materia.

En el caso de detección de plagio en alguno de los trabajos/pruebas realizadas, la calificación final de la materia será de suspenso (0) y los profesores comunicarán el asunto a la dirección de la escuela para que tome las medidas que considere oportunas.

Fuentes de información

Bibliografía Básica

Dominic Chell, **The mobile application hacker´s handbook**, 1, Jonh Wiley & Sons, 2015

Bibliografía Complementaria

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

Recomendaciones

Otros comentarios

Se recomienda tener conocimientos básicos sobre el SO Linux y conocimientos de programación en Java. Asimismo, si bien no es imprescindible, se recomienda tener conocimientos de programación de dispositivos móviles Android.

DATOS IDENTIFICATIVOS				
Smart Contracts e dApps				
Asignatura	Smart Contracts e dApps			
Código	V05M175V11219			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	1	2c
Lengua Impartición	Castellano			
Departamento	Ingeniería telemática			
Coordinador/a	Fernández Iglesias, Manuel José			
Profesorado	Álvarez Sabucedo, Luis Modesto Fernández Iglesias, Manuel José			
Correo-e	manolo@uvigo.es			
Web				
Descripción general	Esta asignatura ofrece una visión introductoria de los conceptos y prácticas relacionados con el desarrollo y despliegue de contratos inteligentes y aplicaciones descentralizadas seguras. Los y las estudiantes explorarán las especificidades de la programación de contratos inteligentes y examinarán diversas vulnerabilidades y amenazas de seguridad específicas de los contratos inteligentes y las aplicaciones descentralizadas. A través de ejercicios prácticos, ejemplos de casos reales y explicaciones en el aula, el alumnado aprenderá a emplear las mejores prácticas para mitigar los riesgos y protegerse contra los ataques en el ecosistema blockchain. Al final del curso, se dispondrá de conocimientos y habilidades para desarrollar contratos inteligentes seguros y diseñar aplicaciones descentralizadas robustas que puedan soportar los desafíos que presentan estas tecnologías.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
Conceptos básicos	Presentación de los conceptos básicos relacionados con el desarrollo de contratos inteligentes y aplicaciones descentralizadas.
Diseño y desarrollo de contratos inteligentes	Se abordar el desarrollo de contratos inteligentes, teniendo en cuenta los aspectos relacionados con la seguridad más relevantes en su desarrollo.
Sistemas de archivos peer-to-peer	Se presentan las características básicas de las redes peer-to-peer, para a continuación describir los elementos esenciales de los sistemas de archivos descentralizados y su relación con las tecnologías blockchain. Se presenta IPFS como caso de estudio.
Tokens no fungibles	Se presenta un caso de uso concreto muy popular en el mundo de los contratos inteligentes y las aplicaciones decentralizadas: los tokens no fungibles o NFT.
Oráculos. Buenas prácticas	Se presentan los oráculos como servicios de terceros que proporcionan datos o eventos externos a un contrato inteligente en una blockchain. Se identifican buenas prácticas para su desarrollo y utilización.
Aspectos relacionados con la ciberseguridad	Se realiza una recapitulación de los elementos clave para el diseño de contratos inteligentes, oráculos y aplicaciones descentralizadas seguras.

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	11.5	24.5	36
Prácticas con apoyo de las TIC	2.5	6	8.5
Prácticas con apoyo de las TIC	4	9	13
Prácticas con apoyo de las TIC	4	9	13
Examen de preguntas objetivas	1.5	3	4.5

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

Metodologías

	Descripción
Lección magistral	Se expondrán en clase los conceptos teóricos y su aplicación práctica. Se intentará que el alumnado participe intercalando la resolución de supuestos prácticos (estudio de casos), de tal forma que en cada sesión de clase se combine la presentación del profesorado con la participación del alumnado.
Prácticas con apoyo de las TIC	Se plantearán pequeños proyectos o ejercicios de programación de contratos inteligentes o aplicaciones descentralizadas, a realizar en el laboratorio y/o mediante trabajo autónomo, bajo la supervisión del profesorado. Se utilizarán plataformas y lenguajes de referencia en el ámbito de las cadenas de bloques.
Prácticas con apoyo de las TIC	Se plantearán pequeños proyectos o ejercicios de programación de contratos inteligentes o aplicaciones descentralizadas, a realizar en el laboratorio y/o mediante trabajo autónomo, bajo la supervisión del profesorado. Se utilizarán plataformas y lenguajes de referencia en el ámbito de las cadenas de bloques.
Prácticas con apoyo de las TIC	Se plantearán pequeños proyectos o ejercicios de programación de contratos inteligentes o aplicaciones descentralizadas, a realizar en el laboratorio y/o mediante trabajo autónomo, bajo la supervisión del profesorado. Se utilizarán plataformas y lenguajes de referencia en el ámbito de las cadenas de bloques.

Atención personalizada

Metodologías	Descripción
Lección magistral	El alumnado tendrá ocasión de acudir a tutorías personalizadas de acuerdo con el procedimiento que se establecerá a tal efecto al principio del curso. Este procedimiento se publicará en la web de la asignatura.
Prácticas con apoyo de las TIC	El alumnado tendrá ocasión de acudir a tutorías personalizadas de acuerdo con el procedimiento que se establecerá a tal efecto al principio del curso. Este procedimiento se publicará en la web de la asignatura.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas con apoyo de las TIC	Se evaluará la solución ofrecida a la primera práctica de la materia, teniendo en cuenta la corrección de la solución propuesta, la calidad del código, la eficiencia del mismo, las habilidades de resolución de problemas y la documentación del código.	10	
Prácticas con apoyo de las TIC	Se evaluará la solución ofrecida a la segunda práctica de la materia, teniendo en cuenta la corrección de la solución propuesta, la calidad del código, la eficiencia del mismo, las habilidades de resolución de problemas y la documentación del código.	25	
Prácticas con apoyo de las TIC	Se evaluará la solución ofrecida a la tercera práctica de la materia, teniendo en cuenta la corrección de la solución propuesta, la calidad del código, la eficiencia del mismo, las habilidades de resolución de problemas y la documentación del código.	25	
Examen de preguntas objetivas	Cada estudiante realizará, individualmente y sin ningún tipo de material de apoyo, un examen de teoría a final del cuatrimestre (la fecha exacta se publicará a principio de curso en la web de la materia) sobre la totalidad de los contenidos de la materia.	40	

Otros comentarios sobre la Evaluación

Existen dos mecanismos de evaluación, evaluación continua (EC) y evaluación global (EG), regidos por las siguientes condiciones:

- La modalidad de evaluación elegida (EC o EG) será única y, por tanto, aplicable tanto a teoría cómo a prácticas.
- La EC incluirá las pruebas descritas en el apartado anterior: un puntuable de teoría, y tres prácticas.
- El alumnado confirmará la modalidad de evaluación definitiva a través de la entrega de las prácticas, en función del plazo (de EC o EG) al que se acoja.
- Con independencia de la modalidad elegida, las prácticas se realizarán siempre individualmente.
- Se establece e una nota mínima de 2 puntos tanto en teoría (de un total de 4 puntos) como en prácticas (de un total de 6 puntos) para poder aprobar la asignatura.
- Si la nota resultante de sumar las calificaciones de teoría y prácticas a igual o mayor que 5 puntos pero el/la estudiante no alcanza la nota mínima exigida en alguna de ellas, la calificación final será suspenso (4.5).

- Si el alumnado se presenta a alguna de las pruebas de evaluación de la materia no podrá figurar en el acta como "no presentado".
- Las pruebas de EC se llevarán a cabo en las fechas estipuladas por el equipo docente, no pudiendo repetirse más tarde.
- En caso de plagio, se asignará la nota suspenso (0) y este hecho será notificado a dirección del Centro para los efectos oportunos.

Procedimiento de evaluación en la oportunidad común para el alumnado que opte por EC:

- **Parte teórica** (40%): La nota de esta parte resulta de la calificación del examen de teoría final de cuatrimestre) cuya calificación máxima es de 4 puntos.
- **Parte práctica** (60%): La nota de esta parte depende de las calificaciones obtenidas en las practicas (hasta 1, 2,5 y 2,5 puntos respectivamente, hasta 6 puntos en total).

El estudiantado que no apruebe la materia en la oportunidad común, podrá conservar la calificación obtenida tanto en teoría como en prácticas para la oportunidad extraordinaria, siempre que alcanzara la nota mínima exigida en la parte que deseen guardar (2 puntos en ambos casos).

Procedimiento de evaluación en la oportunidad común para el alumnado que opte por EG:

- **Parte teórica** (40%): La nota de esta parte corresponde al examen final realizado en la fecha aprobada por la Xunta de Escuela, sobre un máximo de 4 puntos.
- **Parte práctica** (60%): La nota de esta parte depende de las calificaciones obtenidas en las prácticas (hasta 1, 2,5 y 2,5 puntos respectivamente, hasta 6 puntos en total). Los entregables podrán ser idénticos a los exigidos en EC o incluir modificaciones en las funcionalidades para desarrollar. Se entregarán en formato electrónico y serán evaluados por el profesorado fuera de clase.

Procedimiento de evaluación en la oportunidad extraordinaria y en la convocatoria fin de carrera:

- **Parte teórica** (40%). La nota de esta parte corresponde al examen final en la fecha que aprobará la Xunta de Escuela, sobre un máximo de 4 puntos.
- **Parte práctica** (60%). Se entregarán las 3 prácticas en formato digital. Las funcionalidades exigidas podrán ser las mismas que en la oportunidad común o incluir modificaciones que serán publicadas con la debida antelación. Dado que no existe la modalidad de EC, las condiciones de evaluación son idénticas a las descritas en el apartado de AG de la oportunidad común.

Fuentes de información

Bibliografía Básica

Lorne Lantz e Daniel Cawrey, **Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications**, O□Reilly Media., 2020

Daniel Drescher, **Blockchain Basics:A Non-Technical Introduction in 25 Steps**, Apress, 2017

Don Tapscott e Alex Tapscott, **Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World**, New enlarged edition, Penguin Publishing Group, 2018

Paul Vigna e Michae lJ. 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

Bibliografía Complementaria

Andreas M. Antonopoulos, **The Internet of Money**, CreateSpace Independent Publishing Platform, 2016

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

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Tecnologías de resgistro distribuído y Blockchain/V05M175V11113

DATOS IDENTIFICATIVOS				
Gestión de seguridad de la información				
Asignatura	Gestión de seguridad de la información			
Código	V05M175V11301			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	2	1c
Lengua Impartición	#EnglishFriendly Castellano Gallego			
Departamento	Ingeniería telemática			
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel Fernández Vilas, Ana			
Correo-e	mcaeiro@det.uvigo.es			
Web	http://http://moovi.uvigo.es			
Descripción general	En esta asignatura se introducen los conceptos fundamentales relacionados con la gestión de la seguridad de la información (e.g. vulnerabilidad, amenaza, riesgo) y se estudian las metodologías, herramientas y especificaciones que se ocupan del análisis de riesgos y del desarrollo de sistemas de gestión de seguridad de la información. Se tratan también los sistemas de respuesta a incidentes, recuperación de desastres y continuidad de negocio.			

Resultados de Formación y Aprendizaje	
Código	
B16	Describir los conceptos fundamentales y la normativa técnica relacionada con la Gestión de la Seguridad de la Información, las metodologías de Análisis de Riesgos, así como las herramientas para llevar a cabo tareas de análisis de riesgos, auditoría de seguridad, gestión de incidentes, gestión de continuidad de negocio y recuperaciones.
C16	Gestionar la seguridad de la información, utilizar herramientas de análisis de riesgos y la auditoria de seguridad, identificar y clasificar posibles incidentes de forma proactiva y definir los cauces para su gestión y resolución.
D11	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia, analizar los riesgos, planificar periodos de detección de incidentes o desastres, y su recuperación, desarrollar un plan de continuidad de negocio, certificar sistemas seguros y realizar la auditoría de seguridad de sistemas e instalaciones.
D14	Proyectar, modelar, calcular y diseñar soluciones técnicas y de gestión de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación, con criterios éticos de responsabilidad y deontología profesional.

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Conocer los conceptos fundamentales relacionados con la Gestión de la Seguridad de la Información: vulnerabilidad, amenaza, riesgo, contramedida, política de seguridad, plan de seguridad, auditoría	B16
Conocer las diferentes metodologías de Gestión de Seguridad de la Información, comúnmente aceptadas	C16 D11
Conocer las herramientas propias para llevar a cabo tareas relacionadas con el análisis de riesgos y la auditoría de seguridad, así como saber cuáles son las más adecuadas a cada entorno	C16 D11
Desarrollar y evaluar sistemas de respuesta a incidentes, respuesta a desastres y continuidad del negocio.	D14

Contenidos	
Tema	
Fundamentos	Conceptos básicos Marco legal Normalización Entidades relevantes
Análisis de riesgos, gestión y certificación:	Metodologías Herramientas de análisis de riesgos
Sistemas de Gestión de Seguridad de la Información	Familia ISO 27000 Esquema Nacional de Seguridad Auditoría

Continuidad de negocio	Roles Secuencia típica de un ataque Resiliencia Planes de contingencia
Detección de incidentes y gestión de respuesta	Sistemas de detección y prevención de intrusiones Respuesta a incidentes Notificación de incidentes
Recuperación de desastres	Plan de recuperación de desastres Arquitecturas tecnológicas de recuperación de desastres

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	19.5	28	47.5
Trabajo tutelado	0.5	5	5.5
Prácticas de laboratorio	15	20	35
Examen de preguntas objetivas	2	20	22
Estudio de casos	5	10	15

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

Metodologías

	Descripción
Lección magistral	Presentación por parte del profesorado del temario de la materia. Con esta metodología se trabajan las competencias: B16, C16, D11 y D14
Trabajo tutelado	Cada alumno de forma individual realizará un trabajo sobre uno de los temas de la asignatura a presentar en el grupo A. Con esta metodología se trabajarán las competencias B16 y C16
Prácticas de laboratorio	En el laboratorio se desarrollarán prácticas guiadas. Con esta metodología se trabajarán las competencias D11 y D14

Atención personalizada

Metodologías	**Descripción**
Trabajo tutelado	El profesorado de la asignatura proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial o en línea (durante la propia sesión magistral, o durante lo horario establecido para las tutorías). El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Prácticas de laboratorio	El profesorado de la materia proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas de laboratorio. Las dudas se atenderán de forma presencial (durante las prácticas, o durante el horario establecido para tutorias). El horario de tutorias se establecerá al principio del curso y se publicará en la página web de la asignatura.
Pruebas	**Descripción**
Estudio de casos	El profesorado de la materia proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas de laboratorio. Las dudas se atenderán de forma presencial (durante las prácticas, o durante el horario establecido para tutorias). El horario de tutorias se establecerá al principio del curso y se publicará en la página web de la asignatura.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Trabajo tutelado	Cada alumno de forma individual realizará un trabajo sobre uno de los temas de la asignatura a presentar en el grupo A.	10	B16 C16
Prácticas de laboratorio	Se desarrollarán al menos dos prácticas, una sobre el desarrollo de un SGSI incluyendo una análisis de riesgos y otra sobre gestión de incidentes.	40	D11 D14
Examen de preguntas objetivas	Examen de conocimientos teóricos y de desarrollo práctico	40	B16 C16 D11 D14
Estudio de casos	Se desarrollarán un caso práctico en la parte de laboratorio en relación con la gestión de incidentes y continuidad de negocio.	10	D11 D14

Otros comentarios sobre la Evaluación

Students can decide to be evaluated according to a continuous assessment model or a global assessment. All students who submit the first case study 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 (40%); (iii) case studies (10%) and (iv) supervised 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 20%. 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.

Fuentes de información

Bibliografía Básica

Cess van der Wens, **ISO 27001 ISMS Handbook: Implementing and auditing an Information Security Management System in small and medium-sized businesses**, 979-8852486288, 2023

Ester Chicano Tejada, **Gestión de incidentes de seguridad informática**, 9788411036191, IC Editorial, 2023

Bibliografía Complementaria

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

Recomendaciones

Asignaturas que se recomienda cursar simultáneamente

Conceptos y leyes/V05M175V11302

DATOS IDENTIFICATIVOS				
Conceptos y leyes				
Asignatura	Conceptos y leyes			
Código	V05M175V11302			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	4	OB	2	1c
Lengua Impartición	Castellano Gallego Inglés			
Departamento	Derecho público			
Coordinador/a	Rodríguez Vázquez, Virgilio			
Profesorado	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.			

Resultados de Formación y Aprendizaje	
Código	
B17	Analizar 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.
C17	Analizar y comunicar la normativa legal relacionada con la ciberseguridad, sus cuestiones ético-legales y los delitos la criminalidad informática en el contexto nacional, europeo e internacional.
C18	Saber aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
C19	Saber comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades.
D15	Comunicar conocimientos y conclusiones, así como las razones últimas que las sustentan, a públicos especializados y no especializados de un modo claro y sin ambigüedades.
D19	Aplicar 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.

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Analizar la normativa técnica y legal aplicable a la ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información.	B17
Analizar y comunicar la normativa legal relacionada con la ciberseguridad, sus cuestiones ético-jurídicas y los delitos de ciberdelincuencia en el contexto nacional, europeo e internacional.	C17
Saber aplicar los conocimientos adquiridos y su capacidad para resolver problemas en contornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.	C18
Saber comunicar sus conclusiones ---y los últimos conocimientos y razones que las sustentan--- a públicos especializados y no especializados de forma clara y sin ambigüedades.	C19
Comunicar los conocimientos y las conclusiones, así como las razones últimas que hay detrás de ellas, a públicos especializados y no especializados de forma clara y sin ambigüedades.	D15
Aplicar la perspectiva de género en los diferentes ámbitos del conocimiento y en la práctica profesional con el objetivo de conseguir una sociedad más justa e igualitaria.	D19

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.

2. Cuestiones ético-legales relacionadas con la ciberseguridad.	2.1. Límites jurídicos al uso de las tecnologías de la información en materia de ciberseguridad. Derechos que pueden verse afectados: libertad, intimidad, dignidad. 2.2. Límites éticos en materia de ciberseguridad. 2.3. Problemas relativos el empleo de nuevas tecnologías: reconocimiento facial, blockchain, web crawling.
3. Problemáticas especiales de los delitos informáticos en el contexto de la parte general del Derecho penal.	3.1. El lugar de comisión del delito. 3.2. El momento de comisión del delito. 3.3. La pluralidad de sujetos. 3.4. Problemas de prueba. 3.5. Las dificultades en su investigación y persecución. Breve referencia a la extradición.
4. La vulneración de la ciberseguridad a través de conductas delictivas.	4.1. Precisiones terminológicas: delitos informáticos y cibercrimen. 4.2. La utilización de las TIC para cometer delitos y cuando las TIC son el objeto del delito. 4.3. El Código Penitenciario 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.
5. Ciberdelitos de descubrimiento y revelación de secretos	5.1. Delitos de descubrimiento y revelación de secretos (I). Riesgos frecuentes: ransomware y el robo de información. 5.2. Delitos de descubrimiento y revelación de secretos (II). Acceso y 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, troianos y spyware). 5.3. Delitos de descubrimiento y revelación de segretos (III). Producir, adquirir, importar o facilitar programas informáticos para cometer los delitos anteriores, o contraseñas de ordenador o códigos de acceso. 5.4. Delitos contra la intimidad y el derecho a la propia imagen: el uso indebido de cookies.
6. Ciberdelitos contra la propiedad	6.1. Delitos contra la propiedad (I). Estafas valiéndose de alguna manipulación informática. Producir, poseer o facilitar programas informáticos destinados la ese fin. 6.2. Delitos contra la propiedad (II). Defraudación utilizando señal de telecomunicaciones ajena. Uso de terminal de telecomunicaciones sin consentimiento del titular. 6.3. 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 penitenciaria de las personas jurídicas.
7. Delitos cometidos contra las personas utilizando las TIC.	7.1. Delitos contra la libertad. Amenazas y coacciones utilizando redes sociales u otras TIC. Ciberstalking. 7.2. Delitos contra la libertad y la indemnidad sexuales. Child grooming y pornografía infantil. 7.3. Delitos contra la intimidad y la privacidad. 7.4. Delitos contra la honra. Lesión de la reputación digital.
8. Ciberdelitos contra intereses colectivos	8.1. 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. 8.2. Delitos relativos al mercado y a los consumidores. Descubrimiento de secretos de empresa a través de las TIC. Acceso intelixible a un servicio de radiodifusión sonoro o televisivo, a servicios interactivos prestados la distancia por vía electrónica. 8.3. Delitos contra la fe pública: falsedades electrónicas.
9. El ciberterrorismo.	9.1. Concepto. 9.2. Delitos informáticos realizados con una finalidad específica del art. 573 del Código Penitenciario. 9.3. Delito de colaboración con organización o grupo terrorista a través de la prestación de servicios tecnológicos.
10. Delitos relativos a la Defensa nacional y otros.	Breve aproximación.

11. Aproximación criminológica a los delitos informáticos.	11.1. Fuentes estadísticas: principales organismos nacionales e internacionales. 11.2. Análisis de los principales informes sobre cibercriminalidad. 11.3. Identificación de los principales recursos tecnológicos utilizados.
12. Análisis de la jurisprudenza española en relación con delitos informáticos.	12.1. Especial atención a la jurisprudenza del Tribunal Supremo. 12.2. Acuerdos del pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo relativos a delitos informáticos. 12.3. El Ministerio Fiscal y la Fiscalía especialista en materia de criminalidad informática.
13. Protección de datos personales	13.1. Normativa de la UE. El Reglamento (UE) 2016/679 de 27 de abril de 2016, Reglamento General de Protección de Datos (RGPD). 13.2. 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 lo que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). 13.3. La Ley Orgánica de Protección de Datos y el Reglamento de desarrollo. 13.4. La agencia de protección de datos personales. 13.5. Programas de compliance en materia de protección de datos personales.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	12	32	44
Prácticas de laboratorio	13	22	35
Examen de preguntas objetivas	3	0	3
Resolución de problemas y/o ejercicios	2	0	2

*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	Resultados de Formación y Aprendizaje

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 al largo del curso, en horario de clase magistral. - 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, en el que las respuestas incorrectas restarán el 50%. -Cada examen tipo test se corresponde al 25% de 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 primero examen de preguntas objetivas, tipo test), manifestando así su interés por acogerse la 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. Se realizada la primera prueba parcial, la alumna o alumno no se presentara a la siguiente o siguientes, la calificación de estas será de 0 puntos.	50	B17 C17 D15 C18 D19 C19
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 dicho examen correspondiente a la "resolución de problemas": - se celebrará en la fecha oficial de examen final de la convocatoria común: primera oportunidad, según el calendario oficial aprobado por la Comisión Académica del Máster. - consistirá en la resolución de uno o varios casos prácticos. - 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 referidos 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 la 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. Se realizada la primera prueba parcial, la alumna o alumno no se presenta a la siguiente o siguientes, la calificación de estas será de 0 puntos.	50	B17 C17 D15 C18 D19 C19

Otros comentarios sobre la Evaluación

1. PRIMERA OPORTUNIDADa) SISTEMA DE EVALUACIÓN CONTINUASe describe en las secciones anteriores.b) SISTEMA DE EXAMEN FINALPara aquellos que no opten por el sistema de evaluación continua, la evaluación de la asignatura consistirá en un único examen final, en la fecha fijado en el calendario oficial aprobado por la Comisión Académica del Máster.Este examen, que comprenderá todo el temario y constituye el 100% de la nota de la asignatura, constará de dos partes, una teórica y otra práctica, que se calificarán de 0 a 5 puntos cada una. La parte teórica constará de pruebas tipo test, para cuya calificación las respuestas correctas suman el doble de las incorrectas, sin puntuación las que quedaron en blanco. La parte práctica consistirá en la resolución de uno o más casos prácticos. La nota final del examen será la suma de las calificaciones obtenidas en cada una de las partes. Para aprobar la asignatura es necesario obtener un mínimo de 5 puntos en la suma de la calificación de ambas partes.2. SEGUNDA OPORTUNIDAD Y CONVOCATORIA EXTRAORDINARIALa evaluación de la asignatura consistirá en un único examen final, en la fecha fijado en el calendario oficial aprobado por la Comisión Académica del Máster.Este examen, que comprenderá todo el temario y constituye el 100% de la nota de la asignatura, constará de dos partes, una teórica y otra práctica, que se calificarán de 0 a 5 puntos cada una. La parte teórica constará de pruebas tipo test, para cuya calificación las respuestas correctas suman el doble de las incorrectas, sin puntuación las que quedaron en blanco. La parte práctica consistirá en la resolución de uno o más casos prácticos. La nota final del examen será la suma de las calificaciones obtenidas en cada una de las partes. Para aprobar la asignatura 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 cursar simultáneamente

Gestión de seguridad de la información/V05M175V11301

DATOS IDENTIFICATIVOS				
Prácticas en empresa				
Asignatura	Prácticas en empresa			
Código	V05M175V11303			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	9	OB	2	1c
Lengua Impartición	Castellano			
Departamento				
Coordinador/a	Marcos Acevedo, Jorge			
Profesorado	Marcos Acevedo, Jorge			
Correo-e	acevedo@uvigo.es			
Web	http://www.munics.es/			
Descripción general	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.			

Resultados de Formación y Aprendizaje	
Código	
B1	Conocer los métodos y técnicas básicas de la criptografía clásica, estándares y protocolos de seguridad criptográfica, esteganografía y cifrado post-cuántico.
B2	Conocer las técnicas de ocultación y persistencia de malware; así como las tendencias actuales en malware mediante el estudio de casos reales.
B3	Identificar los métodos de ataque a la privacidad y de los conceptos de preservación de la privacidad y anonimato: privacidad diferencial, cifrado homomórfico y computación segura multi-partita
B4	Distinguir las principales vulnerabilidades que sufren las aplicaciones, así como los principales mecanismos de autenticación, autorización y control de acceso, con énfasis especial en aplicaciones web y servicios web.
B5	Conocer de las vulnerabilidades en los dispositivos y tecnologías de acceso de red, las herramientas para explorarlas y las medidas de protección para obtener redes de comunicaciones seguras, así como comprender el concepto de política de seguridad aplicado a redes, la seguridad perimetral y los cortafuegos.
B6	Comprender los conceptos básicos y el funcionamiento general de las tecnologías basadas en registro distribuido; así como su evaluación en términos de confidencialidad, integridad y disponibilidad; y sus principales aplicaciones y casos de uso.
C1	Determinar el grado de seguridad de una solución criptográfica, elegir la más adecuada a un sistema de información o de comunicaciones, así como aplicar y adaptar sus elementos.
C2	Detectar y eliminar las vulnerabilidades susceptibles a malware, así como malware, en sistemas y redes de comunicaciones, así como evadir técnicas de ocultación y persistencia de malware.
C3	Elegir la solución de privacidad y anonimato más adecuada para un sistema de información o de comunicaciones, así como saber aplicar y adaptar los elementos de privacidad y de comunicación anónima a un producto, servicio o sistema de información y comunicaciones en función de las necesidades y teniendo en cuenta el compromiso entre utilidad de la información y privacidad de los datos.
C4	Prevenir, identificar y corregir las principales vulnerabilidades que sufren las aplicaciones, así como incorporar mecanismos de autenticación, autorización y control de acceso a las aplicaciones.
C5	Diseñar e implementar redes seguras, seleccionando y configurando los dispositivos adecuados para cada sección de la red y utilizando proactivamente la monitorización de red como de modo que se implemente correctamente la política de seguridad de la organización.
C6	Aplicar tecnologías de registro distribuido a casos de uso específico, así como diseñar, desarrollar y desplegar una solución basada en dichas tecnologías, optimizando sus parámetros esenciales y aplicando mecanismos de protección para evitar y mitigar ataques.
C7	Decidir la solución/protocolo adecuado para asegurar la seguridad de comunicaciones extremo a extremo, así como configurar las diferentes herramientas que los distintos sistemas operativos/plataformas nos aportan para activar la seguridad en las comunicaciones.
C8	Identificar las vulnerabilidades de un SO en un entorno de uso concreto, modificar la configuración para minimizar su exposición y comprobar su niel de seguridad.
C9	Analizar las implicaciones del nivel de seguridad de tecnologías relacionadas con la digitalización de los sectores de producción, así como valorar y modelar amenazas y ejecutar ataques con el objetivo de diseñar sistemas IoT seguros.
C10	Identificar y aprovechar, de manera analítica y práctica, vulnerabilidades de los sistemas de información, así como identificar posibles vectores de ataque e innovar en técnicas y procesos referidos al hacking ético.

C11	Valorar una empresa en el ámbito de la seguridad e incluso a sectores más específicos dentro de este ámbito, así como definir los perfiles necesarios, propios de la empresa o externos, asociados a la ciberseguridad.
C12	Identificar, preservar y analizar evidencias, realizar análisis forense de un sistema de información, y generar informes que sean claros, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática.
C13	Aplicar herramientas de virtualización de infraestructuras en Centros de Procesado de Datos, así como utilizar herramientas para la monitorización de sus infraestructuras y servicios.
C14	Identificar vulnerabilidades en sistemas operativos y aplicaciones propios de los dispositivos móviles, así como realizar un análisis forense y definir la política de seguridad que afecta a las comunicaciones y sistemas móviles de una organización.
C15	Aplicar los contratos inteligentes al desarrollo de sistemas descentralizados, evaluar si un desarrollo es adecuado a la problemática y utilizar las herramientas de desarrollo apropiadas para programar, desplegar e interaccionar con contratos inteligentes, así como usar oráculos bajo condiciones de robustez y seguridad.
C16	Gestionar la seguridad de la información, utilizar herramientas de análisis de riesgos y la auditoria de seguridad, identificar y clasificar posibles incidentes de forma proactiva y definir los cauces para su gestión y resolución.
C17	Analizar y comunicar la normativa legal relacionada con la ciberseguridad, sus cuestiones ético-legales y los delitos la criminalidad informática en el contexto nacional, europeo e internacional.
C18	Saber aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
C19	Saber comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades.
D1	Resolver problemas relacionados con el uso de información cifrada y tener autonomía e iniciativa para desarrollar soluciones innovadoras en los campos de la criptografía, el criptoanálisis, la anonimia y la privacidad.
D2	Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
D3	Trabajar como analista de malware, para proteger aplicaciones, así como analizar su seguridad en cualquier área de aplicación.
D4	Aplicar la tecnología de cadenas de bloques a la protección descentralizada verificable de la información, ya sea referida ésta a activos digitales de información o referida a activos digitales que representan bienes de uso.
D5	Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones.

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Experiencia en el desempeño de la profesión y de sus funciones más habituales en un entorno real de empresa.	B1 B2 B3 B4 B5 B6 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 D1 D2 D3 D4 D5

Contenidos

Tema	
Contenido general	A definir por el tutor en la empresa y el tutor académico.
ntegración en la empresa y en su entorno de trabajo	Durante su estancia el alumno se integrará en la organización de la empresa y se deberá coordinar con el resto de integrantes del equipo de trabajo al que sea asignado.
Desarrollo de su actividad profesional	El alumno realizará las tareas encomendadas, de acuerdo con sus conocimientos y competencias.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Prácticum, Practicas externas y clínicas	220	5	225

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

Metodologías

	Descripción
Prácticum, Practicas externas y clínicas	Estancia en una empresa desarrollando funciones propias de un titulado de Master de Ciberseguridad para que pueda poner en práctica los conocimientos y competencias adquiridas, para completar su formación académica.

Atención personalizada

Metodologías	Descripción
Prácticum, Practicas externas y clínicas	El alumno tendrá un tutor dentro de la empresa que le guiará y supervisará en las tareas específicas que tendrá que desarrollar dentro de la misma; y un tutor académico -profesor de la E.E.T. de la Universidad de Vigo- que definirá junto con el tutor de la empresa, el marco general de la actividad del alumno, comprobando que se ajusta al perfil/mención estudiado por el estudiante.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje

Prácticum, Practicas externas y clínicas	Prácticum, Practicas externas y clínicasPrácticas externas La evaluación se realizará en función de: 1) La memoria de actividades 2) La evaluación del tutor en la empresa	100	B1 B2 B3 B4 B5 B6	C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19	D1 D2 D3 D4 D5

Otros comentarios sobre la Evaluación

MEMORIA DE ACTIVIDADES: El alumno/a deberá entregar una memoria explicativa de las actividades realizadas durante las prácticas, especificando su duración, las unidades o departamentos de la empresa en que se realizaron, la formación recibida (cursos, programas informáticos, etc.), el nivel de integración dentro de la empresa y las relaciones con el personal.

La memoria debe incluir también un apartado de conclusiones, que contendrá una reflexión sobre la adecuación de las enseñanzas recibidas durante la carrera para el desempeño de la práctica (aspectos positivos y negativos más significativos relacionados con el desarrollo de las prácticas). Se valorará, además, la inclusión de información sobre la experiencia profesional y personal obtenida con las prácticas (valoración personal del aprendizaje conseguido a lo largo de las prácticas y sugerencias o aportaciones propias sobre la estructura y funcionamiento de la empresa visitada).

La valoración de la memoria será el 60% de la nota final.

EVALUACIÓN DEL TUTOR EN LA EMPRESA: El tutor de la empresa entregará un informe valorando aspectos relacionados con las prácticas realizadas por el alumno: puntualidad, asistencia, responsabilidad, capacidad de trabajo en equipo e integración en la empresa, calidad del trabajo realizado, etc.

La valoración del tutor en la empresa será el 40% de la nota final.

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendaciones

DATOS IDENTIFICATIVOS				
Trabajo Fin de Máster				
Asignatura	Trabajo Fin de Máster			
Código	V05M175V11304			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	12	OB	2	1c
Lengua Impartición	Castellano Gallego			
Departamento	Ingeniería telemática			
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel			
Correo-e	mcaeiro@det.uvigo.es			
Web	http://moovi.uvigo.es			
Descripción general	(*)O Traballo Fin de Máster (TFM) é un traballo académico, persoal e orixinal que se debe presentar en público e que é avaliado por un tribunal. Trátase dun proxecto no que o estudante ten que mostrar os coñecementos adquiridos durante o mestrado. Debe concluir coa redacción por escrito dun conxunto de explicacións, teorías, ideas, razoamentos, descrición de desenvolvementos ou deseños, etc. sobre unha temática elixida polo alumno, e supervisada por un titor ou titores, que velarán pola súa progresión e polo nivel de calidade. Non obstante, o Traballo Fin de Máster é responsabilidade única do aspirante ao título de máster.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
El Trabajo Fin de Máster es un trabajo académico, personal y original en el que el estudiante tiene que mostrar los conocimientos adquiridos durante el máster. Por lo tanto, el contenido de cada trabajo debe ser único, aunque deberá mostrar la capacidad del alumno para analizar un problema de una forma sistemática, proponer soluciones, analizar los resultados obtenidos y exponerlos de forma clara.	1. Objectivos 2. Metodología y planificación 3. Trabajo previo (situación actual, estándares, etc.) 4. Resultados y contribuciones técnico-científicas 5. Conclusiones 6. Bibliografía 7. Redacción de la memoria 8. Presentación oral

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Trabajo tutelado	0	275	275
Presentación	1	24	25
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

Metodologías	
	Descripción
Trabajo tutelado	(*)O estudante realizará un traballo académico, persoal e orixinal no que deberá mostrar os coñecementos adquiridos durante o mestrado. Debe concluír coa redacción por escrito dun conxunto de explicacións, teorías, ideas, razoamentos, descrición de desenvolvementos ou deseños, etc. sobre unha temática elixida polo alumno, e supervisada por un titor ou titores, que velarán pola súa progresión e polo nivel de calidade.

Atención personalizada

Metodologías	Descripción
Trabajo tutelado	

Pruebas	Descripción
Presentación	

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Trabajo tutelado	(*) traballo será avaliado por un tribunal. O alumno poñerá á súa disposición a memoria do traballo, e realizará unha presentación pública. O tribunal utilizará unha rúbrica que estará dispoñible publicamente para facer a avaliación	100	

Otros comentarios sobre la Evaluación

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Manuel Ruiz-de-Luzuriaga-Peña, **Guía para citar y referenciar. Estilo IEEE**, Universidad Pública de Navarra, 2016

Recomendaciones