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

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				
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				
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

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

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	Inglés			
Departamento				
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
Resolución de problemas y/o ejercicios	0	5	5
Examen de preguntas objetivas	2	0	2
Informe de prácticas, prácticum y prácticas externas	0	2	2
*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
Resolución de problemas y/o ejercicios	Resolución de cuestiones, problemas y ejercicios al largo del curso. Entrega individual por escrito.	30	
Examen de preguntas objetivas	Examen escrito. Resolución de cuestiones, problemas o ejercicios.	40	
Informe de prácticas, prácticum y prácticas externas	Informes sobre las prácticas realizadas individualmente o por parejas.	30	

Otros comentarios sobre la Evaluación

Se deja a la discreción de los alumnos dos métodos de evaluación alternativos en la materia: 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 al largo del curso y en los plazos establecidos de ejercicios resueltos (30%).
La evaluación única consistirá en la realización de un examen final escrito (70% de la calificación) y en el desarrollo de prácticas y proyectos (30%).
Las pruebas escritas de las modalidades de evaluación global y continua no serán necesariamente iguales.
Los alumnos podrán optar por una u otra modalidad de evaluación hasta la fecha del examen escrito del curso.
Aquellos alumnos que no superen la materia en la convocatoria común disponen de una segunda oportunidad extraordinaria al final del curso en la que se reevaluarán sus conocimientos con una prueba escrita.
La calificación de las pruebas sólo tiene efecto en el curso académico en que se obtengan, con independencia del itinerario de evaluación escogido.

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**, 9781617298042, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, 9781913805272, GCATI, 2020

Bibliografía Complementaria

Katharine Jarmul, **Practical Data Privacy**, 9781098129460, O'Reily Media, 2023

Nishant Bhajaria, **Data Privacy**, 9781617298998, Manning Publications, 2022

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

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				
Departamento				
Coordinador/a	López Nores, Martín			
Profesorado	Bellas Permuy, Fernando López Nores, Martín Losada Pérez, José			
Correo-e	mlnores@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530104&any_academic=2023_24&any_academic=2023_24			
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				
Coordinador/a	Rodríguez Rubio, Raúl Fernando			
Profesorado	Nóvoa de Manuel, Francisco Javier Rodríguez Rubio, Raúl Fernando			
Correo-e	rrubio@det.uvigo.es			
Web	http://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530105&any_academic=2023_24&any_academic=2023_24			
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				
Tecnologías de resgistro distribuído y Blockchain				
Asignatura	Tecnologías de resgistro distribuído y Blockchain			
Código	V05M175V11113			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición				
Departamento				
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://bit.ly/gd_trdb			
Descripción general	En la materia se adquieren los conocimientos básicos de las tecnologías basadas en registro distribuido (DLTs) y Blockchain.			

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 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				
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 (primera oportunidad), 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 evaluación 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				
Coordinador/a	Blanco Fernández, Yolanda			
Profesorado	Blanco Fernández, Yolanda Yáñez Izquierdo, Antonio Fermín			
Correo-e	yolanda@det.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530108&any_academic=2023_24			
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				
Departamento				
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				
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

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

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 inalá mbricas para dispositivos IoT/IioT.	Ciberseguridad en comunicaciones inalá mbricas 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	
Prácticas con apoyo de las TIC	Resolución de prácticas y realización de informes con los resultados obtenidos.	30	
Examen de preguntas objetivas	Examen escrito sobre los contenidos teóricos y prácticos impartidos durante el curso.	30	

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.

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**, Elsevier, 2014

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, GI Global, 2012

Tyson Macaulay,, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.,**, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems**, O'Reilly, 2015

Pascal Ackerman, **Industrial Cybersecurity,**, 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.**, 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				
Coordinador/a	Costa Montenegro, Enrique			
Profesorado	Carballal Mato, Adrián Costa Montenegro, Enrique			
Correo-e	kike@gti.uvigo.es			
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530110&any_academic=2023_24			
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				
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=2023_24&any_academic=2023_24			
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				
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=2023_24			
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				
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://https://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530113&any_academic=2023_24			
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				
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

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

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.

Sistema de evaluación continua

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

Sistema de evaluación global

La calificación global 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 global 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	Dpto. Externo Ingeniería 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				
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.
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.
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.
BaaS como modelo de externalización	Se presentan los elementos básicos de Blockchain como servicio (Blockchain as a Service, BaaS) para desarrollar, desplegar y gestionar aplicaciones blockchain sin necesidad de configurar y mantener infraestructura de cadena de bloques.
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	10.5	22.5	33
Prácticas con apoyo de las TIC	2.5	5.5	8

Prácticas con apoyo de las TIC	4	8.5	12.5
Prácticas con apoyo de las TIC	4	8.5	12.5
Examen de preguntas de desarrollo	1.5	3	4.5
Examen de preguntas de desarrollo	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.	20	
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.	20	
Examen de preguntas de desarrollo	Cada estudiante realizará, individualmente y sin ningún tipo de material de apoyo, un examen de teoría a mitad del cuartrimestre (la fecha exacta se publicará a principio de curso en la web de la materia) sobre los contenidos que se hayan explicado hasta la semana anterior a la prueba.	20	
Examen de preguntas de desarrollo	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.	30	

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 la teoría como a las prácticas.
- La EC incluye las pruebas descritas en el apartado anterior: dos puntuables 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 entrega (de EC o EG) al que se acoja. Dicha modalidad de evaluación será la que se aplicará también en la parte de teoría, de ahí que en el caso de que un estudiante opte finalmente por EG, la nota del primer puntuable de teoría, de ser el caso, quedaría anulada.
- Con independencia de la modalidad elegida, las prácticas se realizarán siempre individualmente.
- Se establece una nota mínima de 2 puntos (sobre 5) tanto en teoría como en prácticas para poder aprobar la asignatura.
- Si la nota resultante de sumar las calificaciones de teoría y prácticas es igual o mayor que 5 puntos pero el/la estudiante no alcanza la nota mínima exigida en alguna de ellas, su calificación final será suspenso (4.5).
- Si el alumnado se presenta a alguna de las pruebas de evaluación de la asignatura no podrá figurar en el acta como "no presentado".
- Las pruebas de EC sólo 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 la dirección del Centro a los efectos oportunos.

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

- **Parte teórica (50%):** La nota de esta parte resulta de sumar las calificaciones de los dos puntuables de teoría descritos anteriormente (a mitad y a final de cuatrimestre), cuyas calificaciones máximas son 2 y 3 puntos, respectivamente.
- **Parte práctica (50%):** La nota de esta parte depende de las calificaciones obtenidas en las prácticas (hasta 1, 2 y 2 puntos respectivamente, hasta 5 puntos en total).

El estudiantado que no apruebe la asignatura en la oportunidad ordinaria, podrá conservar la calificación obtenida tanto en teoría como en prácticas para la oportunidad extraordinaria, siempre que haya alcanzado la nota mínima exigida en la parte que deseen guardar (2 puntos sobre 5, en ambos casos).

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

- **Parte teórica (50%):** La nota de esta parte corresponde al examen final realizado en la fecha aprobada por la Junta de Escuela, sobre un máximo de 5 puntos.
- **Parte práctica (50%):** La nota de esta parte depende de las calificaciones obtenidas en las prácticas (hasta 1, 2 y 2 puntos respectivamente, hasta 5 puntos en total). Los entregables podrán ser idénticos a los exigidos en EC o incluir modificaciones en las funcionalidades a desarrollar. Se entregarán en formato digital y serán evaluados por el profesorado fuera de clase.

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

- **Parte teórica (50%)**. La nota de esta parte corresponde al examen final realizado en la fecha aprobada por la Junta de Escuela, sobre un máximo de 5 puntos.
- **Practical part (50%)**. Se entregarán los correspondientes prácticas digitalmente. Las funcionalidades exigidas podrán ser las mismas que en la oportunidad ordinaria 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 EG de la oportunidad ordinaria.

Fuentes de información

Bibliografía Básica

Lorne Lantz e Daniel Cawrey, **Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications**, 978-1492054702, O□Reilly Media., 2020

Daniel Drescher, **Blockchain Basics:A Non-Technical Introduction in 25 Steps**, 978-1484226032, Apress, 2017

Don Tapscott e Alex Tapscott, **Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World**, 978-1101980149, New enlarged edition, Penguin Publishing Group, 2018

Paul Vigna e Michae lJ. Case, **The Truth Machine: The Blockchain and the Future of Everything**, 978-0008301774, Harper Collins, 2019

Manuel J. Fernández Iglesias, **Introduction to Blockchain, Smart Contracts and Decentralized Applications**, bit.ly/intro_ciad, 2023

Bibliografía Complementaria

Andreas M. Antonopoulos, **The Internet of Money**, 978-1537000459, CreateSpace Independent Publishing Platform, 2016

Ethereum.org, **Ethereum Development Tutorials**, https://ethereum.org/en/developers/tutorials/, 2023

Bina Ramamurthy, **Blockchain Basics**, https://www.coursera.org/learn/blockchain-basics, Coursera, 2023

Mark Parzygnat, **IBM Blockchain 101: Quick-start guide for developers**, https://bit.ly/ibm_bc_basics, IBM Developer, 2023

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Tecnologías de resgistro distribuído y Blockchain/V05M175V11113