Escola de Enxeñaría de Telecomunicación

Páxina web

www.teleco.uvigo.es

Presentación

A Escola Enxeñaría de Telecomunicación, con acreditación institucional dende o 28/01/2019 (RD 420/2015), oferta un grao e catro másteres totalmente adaptados ao Espazo Europeo de Educación Superior, verificados pola ANECA axustándose ás Ordes Ministeriais CIN/352/2009 e CIN/355/2009.

Grao en Enxeñaría de Tecnoloxías de Telecomunicación (GETT) - Bachelor□s Degree in Telecommunication Technologies Engineering

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

O Grao en Enxeñaría de Tecnoloxías de Telecomunicación habilita para o exercicio das profesións reguladas de enxeñería técnica. As profesións reguladas son aquelas para que o exercicio require cumprir unha condición especial que, xeralmente, é estar en posesión dun determinado título académico. Na actualidade, réxense polo Real Decreto 1837/2008. O Espazo Europeo de Educación Superior (EEES) determinou que as atribucións profesionais pódense adquirir coa titulación de grao (Enxeñeiros e Enxeñeiras Técnicos) ou coa titulación de mestrado universitario (Enxeñeiros e Enxeñeiras).

O GETT foi seleccionado para participar no Plan de Excelencia do Sistema Universitario de Galicia Ultreia 2020, no que se recolle un conxunto de accións que teñen como obxectivo que as universidades galegas poidan dar un novo salto de calidade. Ao abeiro deste plan, a partir do curso 2018/19 **ofértase un itinerario en inglés para que, os alumnos e alumnas que o desexen, podan cursar nesta lingua ata o 80% dos créditos da 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 Enxeñaría de Telecomunicación

Determinadas profesións reguladas necesitan un nivel de estudos maior e así, para poder exercelas, requírese ter cursado un mestrado universitario habilitante. O Mestrado en Enxeñaría de Telecomunicación é un mestrado con atribucións profesionais plenas de Enxeñeiro e Enxeñeira de Telecomunicación, regulado pola Orde Ministerial CIN/355/2009 de 9 de febreiro de 2009 e publicado no 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

Mestrados Interuniversitarios

A oferta educativa actual do centro complétase con diferentes mestrados interuniversitarios interrelacionados co sector empresarial.

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

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

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 Ciberseguridade

Materias

Curso 1

Código	Nome	Cuadrimestre	Cr.totais
V05M175V11108	Seguridade da información	1c	5
V05M175V11109	Análise de malware	1c	5
V05M175V11110	Privacidade e anonimidade	1c	5
V05M175V11111	Seguridade de aplicacións	1c	5
V05M175V11112	Redes seguras	1c	5
V05M175V11113	Tecnoloxías de rexistro distribuído e Blockchain	1c	5
V05M175V11211	Seguridade en comunicacións	2c	5
V05M175V11212	Fortificación de sistemas	2c	5
V05M175V11213	Ciberseguridade industrial e IoT	2c	5
V05M175V11214	Hacking ético e Test de intrusión	2c	5
V05M175V11215	Negocio en ciberseguridade e emprendemento	2c	4
V05M175V11216	Análise forense	2c	3
V05M175V11217	Seguridade en centros de datos	2c	3
V05M175V11218	Seguridade en dispositivos móviles	2c	3
V05M175V11219	Smart Contracts e dApps	2c	3

DATOS IDENTIFICATIVOS				
Seguridade da información				
Materia	Seguridade da información			
Código	V05M175V11108			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de 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			
Descrición xeral	Nesta materia se estúdanse as técnicas de criptografía e criptoanálise, a xeración de números e funcións aleatorias, os métodos de integridade de mensaxes, o cifrado autenticado, o cifrado asimétrico, os métodos de privacidade e anonimato da información, os esquemas de computación segura e a esteganografía. Todas as anteriores son ferramentas básicas para a protección da información en redes e sistemas.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
1. Cifrado	Cifrado Shannon. Seguridade perfecta. Seguridade semántica. Seguridade baseada na teoría da información. A canle wiretap
2. Cifrado en fluxo	Xeneradores seudoaleatorios simples e compostos. Ataques. Casos de estudo
3. Cifrado en bloques	Cifrado en bloques. Seguridade. DES. AES. Funcións seudoaleatorias. Contrución de PRF e cifrado en bloques.
4. Integridade	Códigos de autenticación e integridade de mensaxes. Definición de seguridade. MAC con chaves. Funcións seudoaleatorias e MAC. Funcións hash. Hashing universal e resistente a colisión. Casos de estudo
5. Cifrado autenticado	Definición. Composición. Ataques. Exemplos e casos de estudo
6. Cifrado con chave pública	Definición. Seguridade semántica. Funcións ducha dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas dixitais. Casos de estudo
7. Cifrado avanzado	Cifrado sobre curvas elípticas. Retículos e cifrado sobre retículas. RLWE. Ataques cuánticos. Cifrado homomórfico
8. Protocolos de identificación	Definición. Contraseñas (dun so uso). Challenge.response. Sigmaprotocolos. Esquemas de Okamoto e Schnorr. Casos de estudo
9. Anonimización	Definición. t-integridade, diverxencia, análise
10. Ocultación de datos e forensic dixital	Definicións. Marcado de auga mediante espectro ensanchado. Codificación de papel sucio. Forensia dixital.
11. Computación segura	Funcións computables. Computación segura a dúas vías e a varias vías. Computación interactiva. Computación homomórfica. Aplicacións.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Resolución de problemas	0	24	24
Prácticas de laboratorio	18	36	54
Lección maxistral	17	51	68
Exame de preguntas de desenvolvemento	2	0	2
Resolución de problemas e/ou exercicios	2	0	2

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

Metodoloxía docente	
	Descrición
Resolución de problemas	Os estudantes resolverán problemas e exercicios sobre o material do curso.
Prácticas de laboratorio	Os estudantes desenvolverán no laboratorio prácticas de seguridade da información con ordenador, e un proxecto de programación sobre cifrado, firma, anonimato ou forensia. As prácticas e proyectos estarán supervisados polos profesores.
Lección maxistral	Exposición sistemática dos contidos do curso: conceptos, resultados, algoritmos, exemplos e casos de uso.

Atención personalizada	
Metodoloxías	**Descrición**
Resolución de problemas	Atenderanse individualmente as consultas sobre a resolución de problemas e ejercicios planteados las clases ou traballados de xeito autónomo. O horario de tutorías pode consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Prácticas de laboratorio	Responderanse individualmente as cuestión relativas ás prácticas de laboratorio e ao desenvolvemento dos proxectos O horario de tutorías pode consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Lección maxistral	Ofrecerase atención individual aos estudantes que precisen orientación para o estudo, explicacións adicionáis sobre os contados da disciplina, aclaración ou guía sobre resolución de problemas. O horario de tutorías pode consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Resolución de problemas	4 conxjuntos de problemas, exercicios ou cuestións ao longo do curso, para resolución individual polos estudantes. Entrega por escrito	30	
Prácticas de laboratorio	Desenvolvemento de proxectos de implementación dun sistema de protección da información. Probas funcionais e de rendemento.	30	
Exame de preguntas de desenvolvemento	Exame escrito. Resolución de cuestións, ejercicios ou problemas.	40	

Outros comentarios sobre a Avaliación

Déixanse a discreción dos alumnos dous métodos de avaliación alternativos na materia: avaliación continua e avaliación

global.

A avaliación continua consistirá na realización dun exame final (40% da cualificación) e no desenvolvemento de proxectos

de enxeñaría a escala (30% da cualificación). A avaliación global consistirá na realización dun exame fina escrito (40% da cualificación) e no desenvolvemento de

proxectos de enxeñaría a escala (dous, 30% da cualificación cada un) que se presentará antes do último día hábil anterior ao período

oficial de exames. As probas escritas das modalidades de avaliación global e continua non serán necesariamente iguais.

Os alumnos optarán por unha ou outra modalidade de avaliación ata a data do exame escrito do curso.

Quen non superen a materia na oportunidade ordinaria da convocatoria dispoñen dunha convocatoria extraordinaria ao final do

curso na que se reavaliarán os seus coñecementos cunha proba escrita ou se reavaliará o seu proxecto se se mellorou ou

modificou. Os pesos de cada unha das probas (exame e proxecto) serán os mesmos que no período ordinario de avaliación

conforme á modalidade que se elixiu.

A cualificación das probas só fornece efecto no curso académico en que se obteñan, con independencia do itinerario de avaliación escollido.

Bibliografía. Fontes 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

Recomendacións

Outros comentarios

A materia impártese en inglés. É recomendable ser capacidade para o razoamento matemático

DATOS IDENTIFICATIVOS				
Análise de malware				
Materia	Análise de malware			
Código	V05M175V11109			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de 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			
Descrición xeral	O malware utiliza os sistemas e as redes de comunicacións para propagar virus, secuestrar dispositivos ou robar datos confidenciais. O obxectivo desta asignatura é dotar o estudiante da capacidade para analizar, detectar e eliminar malware. Para elo se explorarán y exemplificarán, de forma práctica e con casos reais, as técnicas actuais de ocultación e persistencia de malware, así como as tendencias máis novedosas para a sua detección e eliminación. Esta materia impartirase en inglés.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introducción a enxeñaría do malware.	a) Que é o malware? b) Cómo detectalo e eliminalo? c) En qué consiste a enxeñaría de malware?
Tipos de malware.	a) Estructura. b) Compoñentes. c) Vectores de infección.
Enxeñaría de malware.	a) Técnicas de propagación. b) Procesos de infección. c) Persistencia do malware. d) Técnicas de ocultación.
Enxeñaría inversa de malware.	a) Cómo analizar e inferir o funcionamiento do malware? b) Comprensión do funcionamiento de novos tipos de malware.
Ferramentas de análise de malware.	a) Ferramentas para a detección de malware. b) Ferramentas para a eliminación de malware.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Actividades introdutorias	2	2	4
Lección maxistral	10	30	40
Prácticas de laboratorio	15	40	55
Foros de discusión	0	2	2
Estudo de casos	5	4	9
Exame de preguntas obxectivas	2	4	6
Resolución de problemas e/ou exercicios	3	6	9

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

Metodoloxía docente

	Descrición
Actividades introdutorias	Faremos unha introdución xenérica aos obxectivos, contidos globais xenerais da materia e resultados esperados. Esta actividade realizarase individualmente.
Lección maxistral	Introduciremos os distintos temas da materia proporcionando o material docente necesario para o seu seguimento. Con esta metodoloxía se traballa o coñecemento B2, a destreza C2 e a competencia D6. Esta actividade realizarase individualmente.
Prácticas de laboratorio	Realizaranse prácticas no laboratorio para comprender mellor os contenidos explicados nas lecciones maxistrais. Con esta metodoloxía trabállase o coñecemento B2, a destreza C2 e as competencias D3 e D6. Algunhas prácticas realizaranse de forma individual e outras en grupos (dependendo do número de estudiantes).
Foros de discusión	Os alunos/as deben participar no foro dentro da plataforma MOOVI. Con esta metodoloxía se traballa o coñecemento B2 e a competencia D6. Esta actividade realizarase individualmente.
Estudo de casos	Durante as clases maxistrais presentaranse casos de estudio típicos de ameazas, problemas de seguridade coñecidos ou tecnoloxías actuáis. Con esta metodoloxía se traballa o coñecemento B2 e as competencias D3 e D6. Esta actividade realizarase en grupo.

Atención personalizada

Metodoloxías	Descrición
Actividades introdutorias	Nas actividades formativas prácticas e titorías, os profesores da materia ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contidos e materias do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Lección maxistral	Nas actividades formativas prácticas e titorías, os profesores da materia ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contidos e materias do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Prácticas de laboratorio	Nas actividades formativas prácticas e titorías, os profesores da materia ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contidos e materias do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Foros de discusión	Nas actividades formativas prácticas e titorías, os profesores da materia ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contidos e materias do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Estudo de casos	Nas actividades formativas prácticas e titorías, os profesores da materia ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con otros contidos e materias do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Prácticas de laboratorio	Os estudantes realizarán prácticas de laboratorio (3 x 15% = 45%), onde se traballará cos conceptos introducidos nas clases teóricas.	45	

Foros de discusión	Os estudantes deben participar no foro da plataforma MOOVI.	5
Estudo de casos	Os estudantes realizarán presentacións de casos de estudo, seleccionados por eles, para analizar amenazas actuáis.	15
Exame de preguntas obxectivas	Dous test de avaliación sucesivos para o contido parcial da materia impartida ata ese momento. Os tests serán individuáis e de tempo limitado.	30
Resolución de problemas e/ou exercicios	Durante as clases maxistrais realizaranse preguntas aos estudantes para coñecer a súa comprensión do tema baixo estudo.	5

Outros comentarios sobre a Avaliación

Os elementos que forman parte da avaliación da materia son os seguintes:

- **Cuestionarios**: ao longo do curso realizaranse dous cuestionarios que achegarán un 15% da nota final (cada un).

- **Presentación de casos de estudo**: cada alumno (de forma individual o en grupo) deberá realizar unha presentación orixinal que aportará un 15% da nota final.

- **Prácticas de laboratorio**: cada alumno deberá realizar un conxunto de prácticas (por defecto 3, cunha ponderación de 15% cada unha) propostas no laboratorio e que achegarán un 45% da nota final.

- **Participación en clase**: os estudiantes participarán e discutirán sobre as exposiciones realizadas polo profesor e esto contribuirá ata un 5% a nota final.

- **Participación no foro**: os estudiantes deben participar no foro da asignatura, de forma individual, e isto contribuirá ata un 5% a nota final; proporcionando, como mınimo, dúas contribucions relevantes.

Así temos:

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

Os estudantes deben obter o menos 4 puntos sobre 10 na nota dos cuestionarios, os casos de estudio e todas as prácticas para poder calcular a nota media final. Si algunha das notas é inferior a 4, entón a notal final non poderá superar 4.9 puntos sobre 10.

A planificación das diferentes probas de avaliación intermedia aprobarase nunha Comisión Académica de Máster (CAM) e estará dispoñible ao principio do cuatrimestre.

Seguindo as directrices propias da titulación ofrecerase aos alumnos que cursen esta materia dous sistemas de avaliación: avaliación continua e avaliación final (fin do cuadrimestre).

Avaliación continua: o estudante segue a avaliación continua dende o momento en que se presenta os dous cuestionarios da materia. Un alumno que opta pola avaliación continua considérase que se presentou á materia, independentemente de que se presente ou non ao exame final.

Avaliación global: o alumno deberá realizar un exame teórico que substitúe aos cuestionarios realizados ao longo do curso, ademais de entregar as prácticas e os traballos equivalentes aos que se realizaron como parte da avaliación continua.

Avaliación extraordinaria: o alumno deberá realizar a parte que non superase. No caso de non superar os cuestionarios deberá realizar un exame 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 copia en calquera das probas (probas curtas, exames parciais ou exame final), a cualificación final será de SUSPENSO (0) e o feito será comunicado á dirección do Centro para os efectos oportunos.

Os traballos e tarefas prácticas propostas e realizadas neste curso non son recuperables e só son válidas para o curso actual.

Bibliografía. Fontes 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

Recomendacións

Materias que se recomenda cursar simultaneamente

Análise forense/V05M175V11216

DATOS IDENTIFICATIVOS				
Privacidade e anonimidade				
Materia	Privacidade e anonimidade			
Código	V05M175V11110			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de 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			
Descrición xeral	Nesta materia preséntanse as principais técnicas para proporcionar privacidade e anonimidade en redes, sistemas e aplicacións. Estúdanse conceptos e métodos de privacidade diferencial, técnicas de mellora da privacidade (PET), privacidade na xeolocalización, privacidade para aprendizaxe máquina e técnicas de anonimidade. Tamén se exploran as implicacións da privacidade desde o deseño e aspectos éticos e legais da privacidade.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introdución. Ataques.	Introdución á privacidade e a anonimidade. Ataques de inferencia. Ataques de análises de tráfico. Rastrexo online.
Privacidad diferencial.	Privacidade diferencial. Mecanismos para a privacidade diferencial. Teoremas de composición.
Técnicas de mantemento e mellora da privacidade.	Primitivas con mantemento da privacidade: recuperación de información, intersección de conxuntos. Técnicas de mellora da privacidade con cifrado homomórfico e computación multipartita segura. Filtros de Bloom.
Anonimidade.	Conceptos básicos. K-anonimidade, l-diversidade e t-proximidade.
Aplicacións en privacidade e anonimidade.	Privacidade da xeolocalización. Comunicacións anónimas. Encamiñamento en cebola. Mixes. Autenticación anónima. Privacidade en aprendizaxe máquina.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Prácticas de laboratorio	19	38	57
Lección maxistral	19	38	57
Resolución de problemas	2	0	2
Resolución de problemas e/ou exercicios	0	5	5
Exame de preguntas obxectivas	2	0	2
Informe de prácticas, prácticum e prácticas externas	0	2	2

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

Metodoloxía docente	
	Descrición
Prácticas de laboratorio	Os estudantes desenvolverán no laboratorio prácticas de privacidade e anonimidade como aplicacións das técnicas presentadas nas leccións maxistrais. As prácticas ou proxectos serán supervisadas polos profesores.
Lección maxistral	Exposición sistemática dos contidos do curso: conceptos, resultados, algoritmos, exemplos e casos de uso.

Resolución de problemas	Resolución de problemas na aula por parte dos docentes.

Atención personalizada

Metodoloxías	Descrición
Prácticas de laboratorio	Responderanse individualmente as cuestións relativas ás prácticas de laboratorio e ao desenvolvemento do proxecto. O horario de tutorías establecerase ao principio do curso e publicarase na páxina web da materia.
Lección maxistral	Dispensarase atención individual aos estudantes que precisen orientación para o estudo, explicación adicional sobre os contidos da disciplina, aclaración ou guía sobre a resolución de problemas. O horario de tutorías establecerase ao principio do curso e publicarase na páxina web da materia.
Resolución de problemas	Atenderanse individualmente as consultas sobre a resolución de problemas e exercicios expostos nas clases ou traballados de forma autónoma. O horario de tutorías establecerase ao principio do curso e publicarase na páxina web da materia.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Resolución de problemas e/ou exercicios	Resolución de cuestións, problemas e exercicios ao longo do curso. Entrega individual por escrito.	30	
Exame de preguntas obxectivas	Exame escrito. Resolución de cuestións, problemas ou exercicios.	40	
Informe de prácticas, prácticum e prácticas externas	Informes sobre as prácticas realizadas individualmente ou por parellas.	30	

Outros comentarios sobre a Avaliación

Déixase a discreción dos alumnos dous métodos de avaliación alternativos na materia: avaliación continua e avaliación global.

A avaliación continua consistirá na realización dun exame final (40% da cualificación), o desenvolvemento de prácticas e proxectos (30% da cualificación) e na entrega ao longo do curso e nos prazos establecidos de exercicios resoltos (30%).
A avaliación única consistirá na realización dun exame final escrito (70% da cualificación) e no desenvolvemento de prácticas e proxectos (30%).
As probas escritas das modalidades de avaliación global e continua non serán necesariamente iguais.
Os alumnos poderán optar por unha ou outra modalidade de avaliación até a data do exame escrito do curso.
Quen non superen a materia na convocatoria ordinaria dispoñen dunha segunda oportunidade extraordinaria ao final do curso na que se reavaliarán os seus coñecementos cunha proba escrita.
A cualificación das probas só fornece efecto no curso académico en que se obteñan, con independencia do itinerario de avaliación escollido

Bibliografía. Fontes 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**,

Recomendacións

DATOS IDENTIFICATIVOS

Seguridade de aplicacións

Materia	Seguridade de aplicacións			
Código	V05M175V11111			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de 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			
Descrición xeral	Desenvolver aplicacións seguras non é unha tarefa trivial. Coñecer as vulnerabilidades que habitualmente sofren as aplicacións, os mecanismos de autenticación, autorización e control de acceso, así como a incorporación da seguridade ó ciclo de vida de desenrolo, é esencial para poder construír e manter aplicacións seguras con éxito. Nesta materia estúdanse de forma práctica todos estes aspectos, con especial énfase no desenvolvemento de aplicacións e servizos web.			

Resultados de Formación e Aprendizaxe

Código

Resultados previstos na materia

Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

	Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS

Redes seguras

Materia	Redes seguras			
Código	V05M175V11112			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de 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			
Descrición xeral	A materia Redes Seguras ten como obxectivo principal que os estudantes aprendan a deseñar e implementar infraestruturas de rede capaces de proporciona-los servizos de seguridade precisos nun contorno corporativo moderno. Deberán coñecer as arquitecturas de seguridad de referencia e seren quen de configuralas en mantelas, utilizando para iso tecnoloxías como IDS/IPS e Firewalls entre outros. A materia esta concebida para que as prácticas de laboratorio, con equipos físicos e virtuáis teñan unha importancia capital no proceso de aprendizaxe.			

Resultados de Formación e Aprendizaxe

Código

Resultados previstos na materia

Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

	Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Tecnoloxías de rexistro distribuído e Blockchain				
Materia	Tecnoloxías de rexistro distribuído e Blockchain			
Código	V05M175V11113			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de 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			
Descrición xeral	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 na materia	Resultados de Formación e Aprendizaxe

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Seguridade en comunicacións				
Materia	Seguridade en comunicacións			
Código	V05M175V11211			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	2c
Lingua de impartición	Castelán			
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			
Descrición xeral	Esta materia realiza un repaso polas capas da arquitectura de comunicacións de Internet, mostrando as súas principais debilidades desde o punto de vista da seguridade, e proporcionando as técnicas e ferramentas necesarias para mitigalas. Os estudantes coñecerán en detalle os protocolos de rede que provén de seguridade á transmisión da información, e as implicacións derivadas do lugar que ocupan dentro da arquitectura en que se organiza o software de comunicacións.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Arquitectura e protocolos de Internet	Conceptos fundamentais.
Seguridade no nivel de enlace	Seguridade en redes cableadas/Ethernet: Control de acceso e autenticación baseada en portos Confidencialidade en redes Ethernet Seguridade en redes sen fíos/WiFi: WPA/2/3 seguridade persoal WPA/2/3 seguridade empresarial
Seguridade no nivel de rede	IPsec Protocolos de seguridade Xestión dinámica de chaves Mecanismos de autenticación
Asegurando a infraestrutura de Internet	Encamiñamento seguro Seguridade en DNS Seguridade en TCP
Seguridade na transmisión dos datos	O protocolo TLS Suites criptográficas Infraestrutura WebPKI Validación de certificados
Seguridade en redes móbiles	Arquitectura do sistema Asociación e autenticación do terminal/usuario Privacidade

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	21	21	42
Prácticas de laboratorio	19	19	38
Prácticas con apoio das TIC	0	58	58
Exame de preguntas de desenvolvemento	2	0	2
Informe de prácticas, prácticum e prácticas externas	0	10	10

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

Metodoloxía docente	
	Descrición
Lección maxistral	As sesións maxistrais seguen o esquema habitual para este tipo de docencia. Nestas sesións trabállanse as competencias CG3, CE1, CE2, CE4, CE8
Prácticas de laboratorio	Realizaranse varias sesións prácticas guiadas polos profesores onde se asentarán os conceptos apresos nas clases teóricas. En ditas prácticas utilizaranse dispositivos de rede reais (routers e switches) e/ou software de virtualización que permitirá ao alumno a súa instrución e adestramento na súa propia casa. De forma natural, as actividades definidas poderán incluír apartados/retos adicionais que complementarán o traballo autónomo do estudante, que se describe no seguinte item. Os alumnos deben adquirir nas prácticas as competencias CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
Prácticas con apoio das TIC	Máis aló das prácticas guiadas, o alumno terá que despregar/configurar/implementar algunhas solucións particulares, para certos escenarios, de forma autónoma. Nestas actividades trabállanse as competencias CB2, CB4, CB5, CG1, CG3, CG5, CE1, CE4, CE8

Atención personalizada	
Metodoloxías	**Descrición**
Lección maxistral	Durante as horas de titoría os docentes realizarán unha atención personalizada para fortalecer ou orientar ao alumno na comprensión dos conceptos teóricos explicados nas clases maxistrais ou nas sesións demostrativas de carácter práctico; e para corrixir ou reorientar os pequenos traballos prácticos optativos derivados de devanditas clases de laboratorio. Titorías: 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 actividade é interactiva por definición, polo que se espera que as cuestións flúan con naturalidade entre docentes e estudantes, podendo involucrar a outros estudantes nas respostas buscadas.
Prácticas con apoio das TIC	Aínda que o traballo autónomo está orientado a que o estudante resolva pola súa conta situacións/retos que se atopará nos sistemas reais, nas horas de titoría os docentes poderán orientalo cuestionando as solucións elixidas ou suxerindo camiños alternativos.

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Prácticas de laboratorio	Serán cualificadas como apto/non apto. O alumno será apto se asiste a todas as sesións deste tipo. Se por algún motivo perdera algunha, deberá suplila realizando algunha práctica complementaria que o profesor definirá no seu momento. Nalgunhas das sesións/actividades poderase solicitar ao alumno un traballo autónomo adicional (e o seu informe asociado) que se avaliará cuantitativamente dentro do ítem máis xeral que denominamos "Prácticas autónomas a través de TIC"	0	
Prácticas con apoio das TIC	Os estudantes terán que realizar, ante os profesores, a demostración práctica que mostre a resolución dos distintos retos técnicos abordados, enfrontándose a preguntas sobre as solucións adoptadas e o seu grao de finalización. Esta defensa/entrevista terá lugar, por termo xeral, tras a entrega da última tarefa encargada e antes do periodo oficial de exames de cada convocatoria; consensuándose a data concreta entre alumnos e profesores con antelación suficiente. Todo reto ou actividade autónoma esixirá un informe escrito, cuxa estrutura, composición e claridade terán o seu peso na valoración final.	60	
Exame de preguntas de desenvolvemento	Realizarase un exame escrito ao final do cuadrimestre, onde se avaliarán tanto os conceptos teóricos impartidos nas sesións maxistrais, como os fundamentos prácticos derivados das clases/traballos prácticos acometidos.	40	
Informe de prácticas, prácticum e prácticas externas	O traballo autónomo do alumno deberá ser recollido nos informes de prácticas pertinentes, e a súa valoración formará parte da valoración integral daquel.	0	

Outros comentarios sobre a Avaliación

A avaliación da materia poderá seguir a canle de avaliación continua ou ben avaliación global. Un alumno elixirá avaliación continua ao entregar a solución e informe do primeiro reto ou traballo autónomo que se lle esixa durante o devir normal do curso. As porcentaxes expresadas no epígrafe anterior só reflicten o máximo conseguible en cada tipo de proba na modalidade de avaliación continua; e son só orientativos. A forma de avaliación detallada exprésase a continuación:

Para a avaliación continua (primeira oportunidade), a nota final será a media xeométrica ponderada entre a nota do traballo autónomo (TA, 60%) e a cualificación correspondente ao exame de preguntas de desenvolvemento (E, 40%). A nota TA será a media aritmética das cualificacións asociadas a cada un dos retos/prácticas autónomas que o alumno terá que resolver ao longo do cuadrimestre, que nunca serán menos de dous.

NOTA FINAL(EC)=(TA^0.6)x(E^0.4)

Se as prácticas de laboratorio foron cualificadas como non aptas, a nota será a mínima entre a nota do exame escrito (E) e 3.

Os alumnos que opten pola avaliación global deberán presentarse a un exame final que consistirá de tres partes: unha proba escrita análoga á proba de avaliación continua (E), unha proba de aptitude no laboratorio e un ou varios traballos prácticos (T). A nota final, neste caso, é a media xeométrica ponderada entre a nota de teoría (E, 80%) e o traballo práctico (T, 20%), coa condición de que se supere a proba de aptitude. Se o alumno non supera a proba de aptitude, a nota final será o mínimo entre E e 3.

NOTA FINAL(EU)=(T^0.2)x(E^0.8)

Finalmente, para a aviación extraordinaria (xuño/xullo), o alumno poderá proseguir co modo de avaliación que xa elixira (conservándoselle a nota da parte -E ou TA/T- que superase, e afrontando unicamente a parte suspensa - con posibles modificacións nas especificacións dos traballos prácticos), ou encarar desde cero unha avaliación que terá as mesmas características que o exame final que acabamos de describir. A proba de aptitude só será necesaria se non asistiu a todas as sesións do laboratorio.

Bibliografía. Fontes 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,

Recomendacións

DATOS IDENTIFICATIVOS				
Fortificación de sistemas				
Materia	Fortificación de sistemas			
Código	V05M175V11212			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	2c
Lingua de impartición	Castelán			
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			
Descrición xeral	Un sistema operativo recentemente instalado é inherentemente inseguro. Presenta certas vulnerabilidades dependendo de factores tales como a idade do S.O., a existencia de portas traseiras sen parchear, os servizos que proporciona e o uso de políticas por defecto que non teñen como primeiro obxectivo a seguridade. Por fortificación dun S.O. referímonos ó acto de configurar dito S.O. coa intención de facelo tan seguro como sexa posible, intentanto minimizar o risco de que quede comprometido a ser explotada algunha das vulnerabilidades. Isto xeralmente implica a aplicación de parches de seguridade, o cambio de certas políticas por defecto del S.O. e a eliminación (ou deshabilitación) de aplicacións e servizos non esenciais. A guía da asignatura está dispoñible no vínculo correspondente da UDC.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Ciberseguridade industrial e IoT				
Materia	Ciberseguridade industrial e IoT			
Código	V05M175V11213			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	2c
Lingua de 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				
Descrición xeral	(*)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 e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introdución á ciberseguridade industrial.	Introdución á ciberseguridade industrial.
Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud	Introdución aos sistemas ciberfísicos e IoT: hardware, firmware, comunicacións e cloud
Ciberseguridade de sistemas de control e comunicacións industriais.	Ciberseguridade de sistemas de control e comunicacións industriais.
Ciberseguridade de tecnoloxías da Industria 4.0/5.0.	Ciberseguridade de tecnoloxías da Industria 4.0/5.0.
Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.	Ciberseguridade de dispositivos IoT/IIoT hardware, firmware e middleware.
Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.	Ciberseguridade en contornas IIoT: sistemas de posicionamento e sensórica.
Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.	Ciberseguridade en comunicacións inalámbricas para dispositivos IoT/IioT.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Aprendizaxe baseado en proxectos	5	45	50
Lección maxistral	14	20	34
Prácticas con apoio das TIC	15	25	40
Exame de preguntas obxectivas	1	0	1

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

Metodoloxía docente	
	Descrición
Aprendizaxe baseado en proxectos	Implementación grupal do deseño, implementación e probas dun sistema IoT, con especial énfase na seguridade. Realizar ataques grupales á seguridade dos sistemas implementados por outros compañeiros ou terceiros.
Lección maxistral	Presentación, por parte do profesorado, dos principais contidos teóricos relacionados coa seguridade industrial e IoT (seguridade embebida, en comunicacións e backends, con especial foco en contornas industriais)
Prácticas con apoio das TIC	Realización por parte dos alumnos de prácticas guiadas e supervisadas.

Atención personalizada	
Metodoloxías	**Descrición**
Aprendizaxe baseado en proxectos	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará ao alumnado durante a realización do proxecto. As dúbidas resolveranse durante as titorías en grupo, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Lección maxistral	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. As dúbidas resolveranse durante a propia sesión maxistral, ou no horario establecido para as titorías. O horario de titorías establecerase ao comezo do curso e publicarase na web da materia.
Prácticas con apoio das TIC	O profesorado da materia prestará unha atención individual e personalizada ao alumnado durante o curso, resolvendo as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que lles foron asignadas, tanto nas prácticas. As dúbidas resolveranse ben durante as propias clases ou ben no horario establecido para as titorías.

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Aprendizaxe baseado en proxectos	O alumnado dividirase en grupos para a realización do deseño, implementación e proba dun sistema IoT, pondo unha énfase especial na seguridade e/ou realizará ataques á seguridade dos sistemas implementados por outros compañeiros/as ou por terceiros. O proxecto realizado, e o informe que contén o resultado dos ataques completados (en canto á súa calidade e ao seu éxito) serán avaliados despois da súa entrega valorando aspectos como a corrección, a calidade, as prestacións e as funcionalidades. Deberase entregar o código, prototipos e documentación realizados. Así mesmo, será necesario realizar unha presentación dos resultados. Durante a realización do proxecto realizarase un seguimento continuo do deseño e da evolución da implementación. Si os resultados intermedios non son satisfactorios, poderase aplicar unha penalización de até o 20% da nota. O seguimento será grupal e individual: cada un do membros do grupo debe documentar as tarefas desenvolvidas dentro do seu equipo e responder sobre elas.	40	
Prácticas con apoio das TIC	Resolución de prácticas e realización de informes cos resultados obtidos.	30	
Exame de preguntas obxectivas	Exame escrito sobre os contidos teóricos e prácticos impartidos durante o curso.	30	

Outros comentarios sobre a Avaliación

Para superar a materia é necesario completar as distintas partes nas que se divide (exame ou exámenes acerca dos contidos expostos na sesión maxistral e o proxecto). A nota final será o resultado de aplicar a **media xeométrica ponderada** da nota de cada unha das partes.

Así, se a nota das sesións maxistrais é NT, a nota do proxecto é NP e a nota das prácticas é NL, a nota final será:

Nota = NT^0.3 × NP^0.4 × NL^0.3

Durante o primeiro mes, o estudiantado deberá indicar explícitamente e por escrito o seu desexo de cursar a materia seguindo a evaluación global. Noutro caso se considerará que seguen a availiación continua. Quen sigan a avaliación continua non se podrán considerar "non presentados" así que realicen a entrega do primeiro cuestionario ou tarefa.

O alumnado que opte pola avaliación global deberá presentar adicionalmente un *dossier* que deberá defender presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, e moi especialmente o proxecto. No caso de seguir a avaliación global, os alumnos/as deberán realizar o traballo de forma individual, salvo que o profesorado comuníquelles explícitamente a autorización para realizalo en grupo.

Avaliación extraordinaria

Só podrán optar á avaliación extraordinaria quen non supere a primeira oportunidade (ao finalizar o cuadrimestre). A avaliación será a descrita nos apartados anteriores, pero adicionalmente será necesario presentar un *dossier,* que deberá ser defendido presencialmente ante o profesorado, no que se inclúan todos os detalles sobre a realización das distintas tarefas, moi especialmente o proxecto.

Quen seguise a avaliación continua pode optar por manter as notas obtidas na primeira oportunidade para as distintas partes da materia ou descartalas.

Outros comentarios

As puntuacións obtidas só son válidas para o curso académico en vigor. Aínda que o proxecto se desenvolverá (na medida do posible) en grupos, o alumnado debe gardar evidencias do seu traballo individual dentro do grupo. No caso no que o rendemento dun alumno ou alumna non sexa acorde ao dos seus compañeiros de grupo, se considerará a súa expulsión do mesmo e/ou podrá ser avaliado/a de forma completamente individual nesta parte.

O uso de calquera material durante a realización dos exámenes tendrá que ser autorizado explícitamente polo profesorado.

En caso de detección de plaxio ou de comportamento non ético nalgún dos traballos/probas realizadas, a calificación da materia será de "suspenso (0)" e os profesores comunicarán o asunto ás autoridades académicas para que tomen as medidas oportunas.

Bibliografía. Fontes 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

Recomendacións

DATOS IDENTIFICATIVOS				
Hacking ético e Test de intrusión				
Materia	Hacking ético e Test de intrusión			
Código	V05M175V11214			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	2c
Lingua de impartición	Castelán			
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			
Descrición xeral	Non hai mellor forma de probar a forza dun sistema que atacalo. As probas de intrusión serven para reproducir os intentos de acceso dun atacante usando as vulnerabilidades que poden existir nunha infraestrutura dada. Neste curso abordaranse os temas fundamentais orientados ás probas de intrusión (pentesting), que abarcan as diferentes fases dun ataque e explotación (desde o recoñecemento e control do acceso á eliminación de pistas).			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS

Negocio en ciberseguridade e emprendemento

Materia	Negocio en ciberseguridade e emprendemento			
Código	V05M175V11215			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	4	OB	1	2c
Lingua de 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			
Descrición xeral	Na materia Negocio en ciberseguridade e emprendemento abordase a seguridade como elemento transversal na organización, dende o punto de vista estratéxico e de xeración de negocio. Presentanse distintos enfoques para a monetización dos datos e da seguridade dos mesmos, así como os distintos perfís profesionais presentes na organización, centrándonos no funcionamento dun Security Operation Centre (SOC) e as suas ferramentas asocidas. Finalmente abordanse distintos casos de éxito e oportunidades de negocio orientados a diferentes sectores productivos, con especial atención ao emprendemento.			

Resultados de Formación e Aprendizaxe

Código

Resultados previstos na materia

Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos

Tema

Planificación

	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente

	Descrición

Atención personalizada

Avaliación

Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Análise forense				
Materia	Análise forense			
Código	V05M175V11216			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán			
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			
Descrición xeral	A análise forense de equipos consiste na aplicación de técnicas científicas e analíticas para identificar, preservar, analizar e presentar datos que sexan válidos dentro dun proceso legal. Esta materia ten unha forte compoñente práctica. Comezarase con unha introdución á informática forense, explicando conceptos clave. A continuación, estudiaranse fundamentos e metodoloxías de análise forense dende un punto de vista xenérico e aplicable a novos casos, pero tamén se estudiarán exemplos concretos baseados en casos reais. Nas prácticas de laboratorio, o/a alumno/a aprenderá a manexar diferentes ferramentas de análise forense e realizará prácticas simulando problemas reais.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente	
	Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Seguridade en centros de datos				
Materia	Seguridade en centros de datos			
Código	V05M175V11217			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán			
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			
Descrición xeral	A seguridade nun centro de procesamento de datos implica a implantación dunha variedade de medidas físicas e lóxicas para protexer a infraestrutura e os datos almacenados no CPD, co obxectivo de garantir a dispoñibilidade, confidencialidade e integridade da información e sistemas críticos para unha organización. Nesta materia farase unha introdución ás diferentes arquitecturas de centros de datos así como ás instalacións físicas auxiliares necesarias para o seu funcionamento. Traballaremos coas tecnoloxías de virtualización máis estendidas no mundo empresarial e confiaremos nelas para fortalecer o noso centro de procesamento de datos, os servizos que se ofrecen dende el e os datos que nel se aloxan.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos
Tema

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais

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

Metodoloxía docente
Descrición

Atención personalizada

Avaliación		
Descrición	Cualificación	Resultados de Formación e Aprendizaxe

Outros comentarios sobre a Avaliación

Bibliografía. Fontes de información
Bibliografía Básica
Bibliografía Complementaria

Recomendacións

DATOS IDENTIFICATIVOS				
Seguridade en dispositivos móviles				
Materia	Seguridade en dispositivos móviles			
Código	V05M175V11218			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán Galego 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			
Descrición xeral	Nesta materia móstrase unha visión xeral da seguridade en dispositivos móbiles con diferentes características. Partindo do estudo da arquitectura destes dispositivos, descubriremos o seu funcionamento interno e cales son as principais ferramentas de seguridade que inclúen, xunto cos riscos e ameazas que sofren. Estudiaremos como atopar, analizar e mitigar as vulnerabilidades que afectan aos dispositivos móbiles, usando ferramentas de análise forense, de desenvolvemento de aplicacións seguras e de xestión de dispositivos en contornos empresariais. A documentación desta materia estará en inglés.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introdución: Ameazas e vulnerabilidades que afectan aos dispositivos móbiles	
Arquitecturas de dispositivos móbiles	
Modelos de seguridade de dispositivos móbiles	
Desenvolvemento de aplicacións seguras	Permisos Xestión de paquetes Xestión de usuarios APIs
Seguridade dos datos	
Seguridade dos dispositivos	
Seguridade da rede	
Vulnerabilidades, exploits e aplicacións maliciosas	
Análise forense de sistemas operativos móbiles	
Sistemas de Xestión de Mobilidade Empresarial (EMM)	

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	9	9	18
Prácticas con apoio das TIC	12	12	24
Exame de preguntas obxectivas	2	14	16
Resolución de problemas e/ou exercicios	0	5	5
Informe de prácticas, prácticum e prácticas externas	0	12	12

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

Metodoloxía docente	
	Descrición
Lección maxistral	Exposición, por parte do profesorado, dos principais contidos teóricos relacionados coa seguridade en dispositivos móbiles. Con esta metodoloxía contribuirase á adquisición das competencias B14 e C14.
Prácticas con apoio das TIC	Realización por parte do alumnado de prácticas guiadas e supervisadas. Con esta metodoloxía traballaranse as competencias C14, D3, D8 e D9.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas con apoio das TIC	O conxunto de profesores da materia proporcionará atención individual e personalizada aos alumnos e alumnas durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que teñen asignadas nas prácticas con apoio das TIC. As dúbidas atenderanse de forma presencial ou telemática (durante as propias prácticas, ou durante o horario de titorías). O horario de titorías establecerase ao inicio do curso e publicarase na páxina web da materia. Fora dese horario, será preciso reservar as titorías mediante cita previa.
Lección maxistral	O conxunto de profesores da materia proporcionará atención individual e personalizada aos alumnos e alumnas durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial e telemática (durante a propia sesión maxistral, ou durante o horario de titorías). O horario de titorías establecerase ao inicio do curso e publicarase na páxina web da materia. Fora dese horario, será preciso reservar as titorías mediante cita previa.

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Exame de preguntas obxectivas	Exame de preguntas cortas sobre os contidos teóricos e prácticos revisados ao longo do curso, tanto nas sesións maxistrais, como nas prácticas de laboratorio. Este exame realizarase ao finalizar o cuadrimestre.	40	
Resolución de problemas e/ou exercicios	Resolución de problemas nos que se faga uso dos coñecementos adquiridos tanto nas sesións de teoría como de prácticas. Esta proba realizarase ao longo do cuadrimestre, con entregas parciais nas datas indicadas polo profesorado.	25	
Informe de prácticas, prácticum e prácticas externas	O alumnado completará de forma individual cuestionarios e/ou informes de prácticas onde mostrarán a correcta realización e comprensión das prácticas.	35	

Outros comentarios sobre a Avaliación

PRIMEIRA OPORTUNIDADE

Seguindo as directrices propias da titulación ofertaranse a quen curse esta materia dous sistemas de avaliación: avaliación continua e avaliación única.

Antes de que finalice a cuarta semana do curso, os e as estudantes deberán indicar

ao profesorado da materia o sistema de avaliación elixido. Quen opte polo sistema de avaliación continua non poderá ser cualificado como "non presentado" se realiza unha entrega ou proba de avaliación con posterioridade á comunicación da súa decisión.

Sistema de avaliación continua

A cualificación global da materia será igual á media aritmética ponderada das probas indicadas previamente. Para superar a materia a cualificación global debe ser maior ou igual que cinco.

Sistema de avaliación global

A cualificación global da materia será igual á media aritmética ponderada das probas indicadas previamente. Neste caso, a proba de resolución de problemas farase nunha única proba ao finalizar o bimestre. Para superar a materia, a cualificación global debe ser maior ou igual que

cinco.

SEGUNDA OPORTUNIDADE

A avaliación consistirá en realizar un exame de preguntas obxectivas, un exame de resolución de problemas e entregar os informes de prácticas de todas as prácticas realizadas ao longo do curso.

OUTROS COMENTARIOS

As puntuacións obtidas solo son válidas para o curso académico en vigor.

O uso de calquera material durante a realización dos exames e probas de avaliación deberá ser autorizado explicitamente polo profesorado da materia.

No caso de detección de plaxio nalgún dos traballos/probas realizadas, a cualificación final da materia será de suspenso (0) e os profesores comunicarán o asunto á dirección da escola para que tome as medidas que considere oportunas.

Bibliografía. Fontes 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

Recomendacións

Outros comentarios

Recoméndase ter coñecementos básicos sobre o S.O. Linux e coñecementos de programación en Java. Así mesmo, se ben non é imprescindible, recoméndase ter coñecementos de programación de dispositivos móbiles Android.

DATOS IDENTIFICATIVOS				
Smart Contracts e dApps				
Materia	Smart Contracts e dApps			
Código	V05M175V11219			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OP	1	2c
Lingua de impartición	Castelán			
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				
Descrición xeral	Esta materia ofrece unha visión introdutoria dos conceptos e prácticas relacionados co desenvolvemento e despregamento de contratos intelixentes e aplicacións descentralizadas seguras. Os e as estudantes explorarán as especificidades da programación de contratos intelixentes e examinarán diversas vulnerabilidades e ameazas de seguridade específicas dos contratos intelixentes e as aplicacións descentralizadas. A través de exercicios prácticos, exemplos de casos reais e explicacións na aula, o alumnado aprenderá a empregar as mellores prácticas para mitigar os riscos e protexerse contra os ataques no ecosistema blockchain. Ao final do curso, dispoñerase de coñecementos e habilidades para desenvolver contratos intelixentes seguros e deseñar aplicacións descentralizadas robustas que poidan soportar os desafíos que presentan estas tecnoloxías.			

Resultados de Formación e Aprendizaxe	
Código	

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Conceptos básicos	Presentación dos conceptos básicos relacionados co desenvolvemento de contratos intelixentes e aplicacións descentralizadas.
Deseño e desenvolvemento de contratos intelixentes	Abordarse o desenvolvemento de contratos intelixentes, tendo en conta os aspectos relacionados coa seguridade máis relevantes no seu desenvolvemento.
Sistemas de arquivos peer-to-peer	Preséntanse as características básicas das redes peer-to-peer, para a continuación describir os elementos esenciais dos sistemas de arquivos descentralizados e a súa relación coas tecnoloxías blockchain. Preséntase IPFS como caso de estudo.
Oráculos. Boas prácticas	reséntanse os oráculos como servizos de terceiros que proporcionan datos ou eventos externos a un contrato intelixente nunha blockchain. Identifícanse boas prácticas para o seu desenvolvemento e utilización.
Tokens non funxibles	Preséntase un caso de uso concreto moi popular no mundo dos contratos intelixentes e as aplicacións decentralizadas: os tokens non funxibles ou NFT.
BaaS como modelo de externalización	Preséntanse os elementos básicos de Blockchain como servizo (Blockchain as a Service, BaaS) para desenvolver, despregar e xestionar aplicacións blockchain sen necesidade de configurar e manter infraestrutura de cadea de bloques.
Aspectos relacionados coa ciberseguridade	Realízase unha recapitulación dos elementos crave para o deseño de contratos intelixentes, oráculos e aplicacións descentralizadas seguras.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	10.5	22.5	33

Prácticas con apoio das TIC	2.5	5.5	8
Prácticas con apoio das TIC	4	8.5	12.5
Prácticas con apoio das TIC	4	8.5	12.5
Exame de preguntas de desenvolvemento	1.5	3	4.5
Exame de preguntas de desenvolvemento	1.5	3	4.5

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

Metodoloxía docente

	Descrición
Lección maxistral	Expoñeranse en clase os conceptos teóricos e a súa aplicación práctica. Tentarase que o alumnado participe intercalando a resolución de supostos prácticos (estudo de casos), de tal forma que en cada sesión de clase combínese a presentación do profesorado coa participación do alumnado.
Prácticas con apoio das TIC	Exporanse pequenos proxectos ou exercicios de programación de contratos intelixentes ou aplicacións descentralizadas, a realizar no laboratorio e/ou mediante traballo autónomo, baixo a supervisión do profesorado. Utilizaranse plataformas e linguaxes de referencia no ámbito das cadeas de bloques.
Prácticas con apoio das TIC	Exporanse pequenos proxectos ou exercicios de programación de contratos intelixentes ou aplicacións descentralizadas, a realizar no laboratorio e/ou mediante traballo autónomo, baixo a supervisión do profesorado. Utilizaranse plataformas e linguaxes de referencia no ámbito das cadeas de bloques.
Prácticas con apoio das TIC	Exporanse pequenos proxectos ou exercicios de programación de contratos intelixentes ou aplicacións descentralizadas, a realizar no laboratorio e/ou mediante traballo autónomo, baixo a supervisión do profesorado. Utilizaranse plataformas e linguaxes de referencia no ámbito das cadeas de bloques.

Atención personalizada

Metodoloxías	Descrición
Lección maxistral	O alumnado terá ocasión de acudir a titorías personalizadas de acordo co procedemento que se establecerá para ese efecto ao principio do curso. Dito procedemento publicarase na web da materia.
Prácticas con apoio das TIC	O alumnado terá ocasión de acudir a titorías personalizadas de acordo co procedemento que se establecerá para ese efecto ao principio do curso. Dito procedemento publicarase na web da materia.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Prácticas con apoio das TIC	Avaliarase a solución ofrecida á primeira práctica da materia, tendo en conta a corrección da solución proposta, a calidade do código, a eficiencia do mesmo, as habilidades de resolución de problemas e a documentación do código.	10	
Prácticas con apoio das TIC	Avaliarase a solución ofrecida á segunda práctica da materia, tendo en conta a corrección da solución proposta, a calidade do código, a eficiencia do mesmo, as habilidades de resolución de problemas e a documentación do código.	20	
Prácticas con apoio das TIC	Avaliarase a solución ofrecida á tercera práctica da materia, tendo en conta a corrección da solución proposta, a calidade do código, a eficiencia do mesmo, as habilidades de resolución de problemas e a documentación do código.	20	
Exame de preguntas de desenvolvemento	Cada estudante realizará, individualmente e sen ningún tipo de material de apoio, un exame de teoría a metade do cuatrimestre (a data exacta publicarase a principio de curso na web da materia) sobre oscontidos que se explicaron ata a semana anterior á proba.	20	
Exame de preguntas de desenvolvemento	Cada estudante realizará, individualmente e sen ningún tipo de material de apoio, un exame de teoría a final do cuadrimestre (a data exacta publicarase a principio de curso na web da materia) sobre a totalidade dos contidos da materia.	30	

Outros comentarios sobre a Avaliación

Existen dous mecanismos de avaliación, avaliación continua (AC) e avaliación global (AG), rexidos polas seguintes condicións:

- A modalidade de avaliación elixida (AC ou AG) será única e, por tanto, aplicable tanto á teoría como ás prácticas.
- A AC inclúe as probas descritas no apartado anterior: dous puntuables de teoría, e tres prácticas.
- O alumnado confirmará a modalidade de avaliación definitiva a través da entrega das prácticas, en función do prazo (de AC ou AG) ao que se acolla. Dita modalidade de avaliación será a que se aplicará tamén na parte de teoría: no caso de que un/unha estudante opte finalmente por AG, a nota do primeiro puntuable de teoría, de ser o caso, quedaría anulada.
- Con independencia da modalidade elixida, as prácticas realizaranse sempre individualmente.
- Establécese unha nota mínima de 2 puntos (sobre 5) tanto en teoría como en prácticas para poder aprobar a materia.
- Se a nota resultante de sumar as cualificacións de teoría e prácticas é igual ou maior que 5 puntos pero o/a estudante non alcanza a nota mínima esixida nalgunha delas, a súa cualificación final será suspenso (4.5).
- Se o alumnado se presenta a algunha das probas de avaliación da materia non poderá figurar na acta como "non presentado".
- As probas de AC só se levarán a cabo nas datas estipuladas polo equipo docente, non podendo repetirse máis tarde.
- En caso de plaxio, asignarase a nota suspenso (0) e este feito será notificado á dirección do Centro para os efectos oportunos.

Procedemento de avaliación na oportunidade ordinaria para o alumnado que opte por AC:

- **Parte teórica (50%)**: A nota desta parte resulta de sumar as cualificacións dos dous puntuables de teoría descritos anteriormente (a metade e a final de cuadrimestre), cuxas cualificacións máximas son 2 e 3 puntos, respectivamente.
- **Parte práctica (50%)**: A nota desta parte depende das cualificacións obtidas nas practicas (ata 1, 2 e 2 puntos respectivamente, ata 5 puntos en total).

O estudantado que non aprobe a materia na oportunidade ordinaria, poderá conservar a cualificación obtida tanto en teoría como en prácticas para a oportunidade extraordinaria, sempre que alcanzase a nota mínima esixida na parte que desexen gardar (2 puntos sobre 5, en ambos os casos).

Procedemento de avaliación na oportunidade ordinaria para o alumnado que opte por AG:

- **Parte teórica (50%)**: A nota desta parte corresponde ao exame final realizado na data aprobada pola Xunta de Escola, sobre un máximo de 5 puntos.
- **Parte práctica (50%)**: A nota desta parte depende das cualificacións obtidas nas prácticas (ata 1, 2 e 2 puntos respectivamente, ata 5 puntos en total). Os entregables poderán ser idénticos aos esixidos en AC ou incluír modificacións nas funcionalidades para desenvolver. Entregaranse en formato electrónico e serán avaliados polo profesorado fóra de clase.

Procedemento de avaliación na oportunidade extraordinaria e na convocatoria fin de carreira:

- **Parte teórica (50%)**. A nota desta parte corresponde ao exame final na data que aprobará a Xunta de Escola, sobre un máximo de 5 puntos.
- **Parte práctica (50%)**. Entregaranse as 3 prácticas en formato dixital. As funcionalidades esixidas poderán ser as mesmas que na oportunidade ordinaria ou incluír modificacións que serán publicadas coa debida antelación. Dado que non existe a modalidade de AC, as condicións de avaliación son idénticas ás descritas no apartado de AG da oportunidade ordinaria.

Bibliografía. Fontes 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

Recomendacións

Materias que se recomenda ter cursado previamente

Tecnoloxías de rexistro distribuído e Blockchain/V05M175V11113