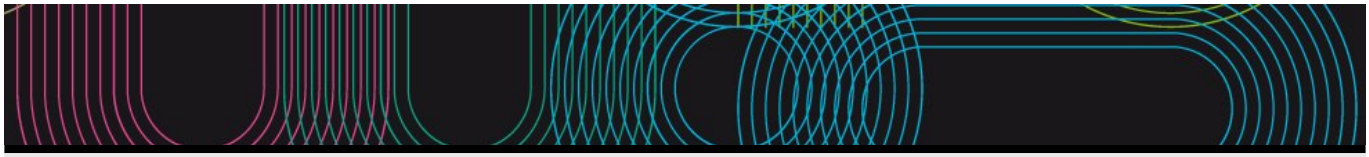

DATOS IDENTIFICATIVOS				
Seguridade en comunicacións				
Materia	Seguridade en comunicacións			
Código	V05M175V11211			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	2c
Lingua de impartición	Castelán			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Rodríguez Rubio, Raúl Fernando			
Profesorado	Fernández Iglesias, Diego Rodríguez Rubio, Raúl Fernando Suárez González, Andrés			
Correo-e	rrubio@det.uvigo.es			
Web	http://https://moovi.uvigo.gal			
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 (oportunidade ordinaria), 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 oportunidade 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