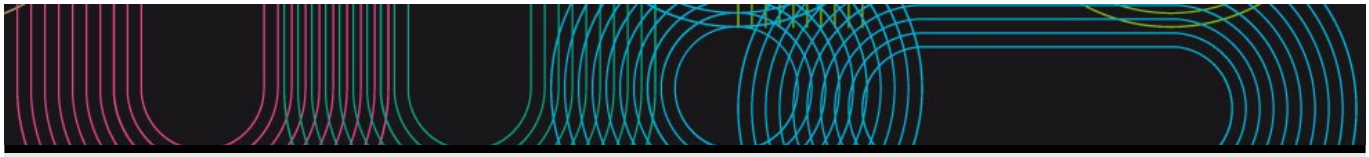

DATOS IDENTIFICATIVOS				
Seguridad en comunicaciones				
Asignatura	Seguridad en comunicaciones			
Código	V05M175V11211			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	2c
Lengua Impartición	Castellano			
Departamento				
Coordinador/a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

Resultados de Formación y Aprendizaje
Código

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

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

Seguridad en redes móviles	Arquitectura del sistema Asociación y autenticación del terminal/usuario Privacidad

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	21	21	42
Prácticas de laboratorio	19	19	38
Prácticas con apoyo de las TIC	0	58	58
Examen de preguntas de desarrollo	2	0	2
Informe de prácticas, prácticum y prácticas externas	0	10	10
*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado			

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

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

Evaluación			
	Descripción	Calificación	Resultados de Formación y Aprendizaje
Prácticas de laboratorio	Serán calificadas como apto/no apto. El alumno será apto si asiste a todas las sesiones de este tipo. Si por algún motivo se perdiese alguna, deberá suplirla realizando alguna práctica complementaria que el profesor definirá en su momento. En algunas de las sesiones/actividades se podrá solicitar al alumno un trabajo autónomo adicional (y su informe asociado) que se evaluará cuantitativamente dentro del ítem más general que denominamos "Prácticas autónomas a través de TIC"	0	

Prácticas con apoyo de las TIC	Los estudiantes tendrán que realizar, ante los profesores, la demostración práctica que muestre la resolución de los distintos retos técnicos planteados, enfrentándose a preguntas sobre las soluciones adoptadas y su grado de completitud. Esta defensa/entrevista tendrá lugar, por término general, tras la entrega de la última tarea encargada y antes del periodo oficial de exámenes de cada convocatoria; consensuándose la fecha concreta entre alumnos y profesores con antelación suficiente. Todo reto o actividad autónoma exigirá un informe escrito, cuya estructura, composición y legibilidad tendrán su peso en la valoración final.	60
Examen de preguntas de desarrollo	Se realizará un exámen escrito al final del cuatrimestre, donde se evalúan tanto los conceptos teóricos impartidos en las sesiones magistrales, como los fundamentos prácticos derivados de las clases/trabajos prácticos acometidos.	40
Informe de prácticas, prácticum y prácticas externas	El trabajo autónomo del alumno deberá ser recogido en el/los informes de prácticas pertinentes, y su valoración formará parte de la valoración integral de aquél.	0

Otros comentarios sobre la Evaluación

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

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

NOTA FINAL(EC)=(TA^0.6)×(E^0.4)

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

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

NOTA FINAL(EU)=(T^0.2)×(E^0.8)

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

Fuentes de información

Bibliografía Básica

I. Ristic, **Bulletproof SSL and TLS, ser. Computers/Security**, London: Fesity Duck, 2015

A. Liska and G. Stowe, **DNS Security: Defending the Domain Name System**, Boston: Syngress, 2016

Yago Fernández Hansen, Antonio Angel Ramos Varón, Jean Paul García-Moran Maglaya, **RADIUS / AAA / 802.1x**, RA-MA Editorial, 2008

Graham Bartlett, Amjad Inamdar, **IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS**, CISCO PRESS, 2016

Madhusanka Liyanage, Ijaz Ahmad, Ahmed Abro, Andrei Gurtov, Mika Ylianttila, **A Comprehensive Guide to 5G Security**, Wiley, 2018

Bibliografía Complementaria

D. J. D. Touch, **Defending TCP Against Spoofing Attacks**, IETF, 2007

R. R. Stewart, M. Dalal, and A. Ramaiah, **Improving TCP□s Robustness to Blind In-Window Attacks**, IETF, 2010

D. J. Bernstein, **SYN cookies**,

P. McManus, **Improving syncookies**, 2008
C. Pignataro, P. Savola, D. Meyer, V. Gill, and J. Heasley, **The Generalized TTL Security Mechanism (GTSM)**, IETF, 2007
D. J. D. Touch, R. Bonica, and A. J. Mankin, **The TCP Authentication Option**, IETF, 2010
S. Rose, M. Larson, D. Massey, R. Austein, and R. Arends, **DNS Security Introduction and Requirements**, IETF, 2005
R. Arends, R. Austin, M. Larson, D. Massey, S. Rose, **Resource Records for the DNS Security Extensions**, IETF, 2005
R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, **Protocol Modifications for the DNS Security Extensions**, IETF, 2005
Cloudflare Inc., **How DNSSEC works**,
P. E. Hoffman and P. McManus, **DNS Queries over HTTPS (DOH)**, IETF, 2018
E. Jones and O. L. Moigne, **OSPF security vulnerabilities analysis**, IETF, 2006
M. Khandelwal and R. Desetti, **OSPF security: Attacks and defenses**, 2016
J. Durand, I. Pepelnjak, and G. Doering, **BGP operations and security**, IETF, 2015
R. Kuhn, K. Sriram, and D. Montgomery, **Border gateway protocol security**, NIST, 2007
C. Pelsser, R. Bush, K. Patel, P. Mohapatra, and O. Maennel, **Making route flap damping usable**, IETF, 2014
Y. Rekhter, J. Scudder, S. S. Ramachandra, E. Chen, and R. Fernando, **Graceful restart mechanism for BGP**, IETF, 2007
IEEE 802.1 Working Group, **IEEE Std 802.1X - 2010. Port-Based Network Access Control**, IEEE Computer Society, 2010
Security Task group of IEEE 802.1, **IEEE Std 802.1AE. Medium Access Control Security**, IEEE Computer Society, 2018
S. Kent, K. Seo, **Security Architecture for the Internet Protocol**, IETF, 2005
S. Kent, **IP Authentication Header**, IETF, 2005
S. Kent, **IP Encapsulating Security Payload**, IETF, 2005
C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, **Internet Key Exchange Protocol Version 2 (IKEv2)**, IETF, 2014
J. Cichonski, J. M. Franklin, M. Bartock, **Guide to LTE Security**, NIST Special Publication 800-187,

Recomendaciones