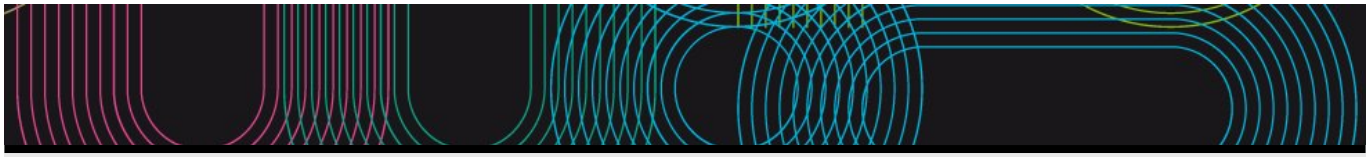

DATOS IDENTIFICATIVOS				
Seguridade en comunicacións				
Asignatura	Seguridade en comunicacións			
Código	V05M175V01103			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OB	1	1c
Lengua Impartición	Castellano			
Departamento	Dpto. Externo Ingeniería telemática			
Coordinador/a	Rodríguez Rubio, Raúl Fernando			
Profesorado	Fernández Iglesias, Diego Rodríguez Pérez, Miguel Rodríguez Rubio, Raúl Fernando			
Correo-e	rrubio@det.uvigo.es			
Web				
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.			

Competencias	
Código	
A2	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
A4	Que los estudiantes sepan comunicar sus conclusiones ---y los conocimientos y razones últimas que las sustentan--- a públicos especializados y no especializados de un modo claro y sin ambigüedades
A5	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
B1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
B3	Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones
B5	Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
C1	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras
C2	Conocer en profundidad las técnicas de ciberataque y ciberdefensa
C4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
C8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
D5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

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

Conocer 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	A5 B1 C1 D4 D5
Comprender que otros protocolos, siendo auxiliares (no relativos al mundo de la seguridad), presentan vulnerabilidades explotables; y podrán describir los ataques más comunes que tratan de aprovecharlas, y sus posibles contramedidas	A5 C4 D4 D5
Saber identificar qué solución/protocolo es el adecuado para asegurar un entorno determinado	A5 B1 B3 B5 C1 C2 C4 D4 D5
Conocer las soluciones que se esconden tras ciertos servicios de red y/o aplicaciones universalmente utilizadas	A5 C2 C8 D4 D5
Ser capaces de configurar las diferentes herramientas (paquetes software) que los distintos sistemas operativos/plataformas nos aportan para activar la seguridad en las comunicaciones.	A2 A5 B5 D4 D5
Adquirir la capacidad de redactar informes técnicos justificando la idoneidad de una solución de ciberseguridad para un problema o entorno determinado	A4 B1 B3

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: IEEE 802.11i IEEE 802.11w Passpoint/HotSpot2.0
Seguridad en el nivel de red	IPsec Protocolos de seguridad Gestión dinámica de claves Mecanismos de autenticación IPsec y NAT
Asegurando la infraestructura de Internet	Seguridad en protocolos de encaminamiento Seguridad en DNS Seguridad en TCP
Seguridad en la transmisión de los datos	El protocolo TLS Suites criptográficas Infraestructura WebPKI Validación de certificados HTTP Public Key Pinning
Seguridad en redes móviles	Arquitectura del sistema LTE 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 autónomas a través de TIC	0	58	58
Examen de preguntas objetivas	2	0	2
Informe de prácticas	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. Las prácticas que se plantearán serán dimensionadas para ser abordables dentro de sus respectivas sesiones presenciales; aunque el alumno que así lo necesite podrá reproducirlas en su casa con software libre que le permitirá virtualizar el comportamiento del hardware de red utilizado en el laboratorio. También se podrán proponer ejercicios optativos que el alumno podrá hacer en horas no presenciales; y revisar individualmente en horario de tutorías. Los alumnos deben adquirir en las prácticas las competencias CB2, CB4, CG1, CG3, CG5, CE1, CE4, CE8
Prácticas autónomas a través de 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.
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 autónomas a través de 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 item más general que denominamos "Prácticas autónomas a través de TIC"	0	A2 A4 A5	B5	C4 C8	D4 D5	
Prácticas autónomas a través de 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. Todo reto o actividad autónoma exigirá un informe escrito, cuya estructura, composición y legibilidad tendrán su peso en la valoración final. Algunas de las actividades propuestas podrán completar, como trabajo autónomo, algunas de las sesiones expositivas abordadas con los profesores en el laboratorio.	40	A2 A4 A5	B5	C1 C4 C8	D4 D5	
Examen de preguntas objetivas	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.	60	A4		C1 C2 C4	D4	
Informe de prácticas	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	A4	B1 B3		D4 D5	

Otros comentarios sobre la Evaluación

La evaluación de la materia podrá seguir el canal de evaluación continua o bien evaluación única. Un alumno elegiría 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, 40%) y la calificación correspondiente al examen de preguntas objetivas (E, 60%). 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.

NOTA FINAL(EC)=(TA^0.4)×(E^0.6)

Para poder superar la materia, el alumno deberá asistir a todas las sesiones prácticas del laboratorio (a no ser que medien causas justificadas). En el caso de que esto no se cumpla, la nota será la mínima de entre la nota del examen escrito (E) y 3.

Los alumnos que opten por la evaluación única 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 segunda oportunidad (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 asistieron a todas las sesiones del laboratorio.

Fuentes de información

Bibliografía Básica

I. Ristic, **Bulletproff 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

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