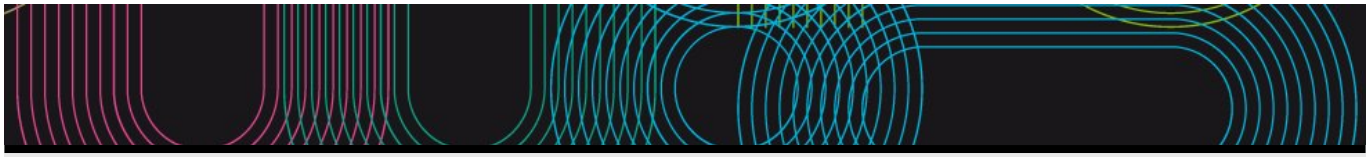

DATOS IDENTIFICATIVOS				
Seguridad en redes				
Asignatura	Seguridad en redes			
Código	O06M132V03312			
Titulacion	Máster Universitario en Ingeniería Informática			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OP	2	1c
Lengua Impartición	Castellano Gallego			
Departamento				
Coordinador/a	Diaz-Cacho Medina, Miguel Ramón			
Profesorado	Diaz-Cacho Medina, Miguel Ramón			
Correo-e	mcacho@uvigo.es			
Web	http://moovi.uvigo.gal			
Descripción general	La seguridad en redes de computadoras es un campo de la ciencia y tecnología que abarca desde conceptos matemáticos hasta conceptos prácticos de programación y sistemas. Su importancia es crucial en el funcionamiento global de los sistemas de comunicaciones e Internet. La materia presentará los conceptos básicos y orientará los mismos hacia una componente eminentemente práctica.			

Resultados de Formación y Aprendizaje	
Código	
A2	(CB7) 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
B1	Capacidad para proyectar, calcular y diseñar productos, procesos y instalaciones en todos los ámbitos de la Ingeniería Informática
B8	Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos
C4	Capacidad para modelar, deseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes, sistemas, servicios y contenidos informáticos.
C9	Capacidad para diseñar y evaluar sistemas operativos y servidores, y aplicaciones y sistemas basados en computación distribuida.
C19	Capacidad para optimizar las políticas de seguridad de la infraestructura de la red de una entidad
C20	Capacidad para manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones
C21	Capacidad para diseñar, desarrollar y gestionar mecanismos de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido
D2	Capacidad para la dirección de equipos y organizaciones
D3	Capacidad de liderazgo
D6	Habilidades de relaciones interpersonales
D7	Capacidad de razonamiento crítico y creatividad
D8	Responsabilidad y compromiso ético en el desempeño de la actividad profesional
D9	Respeto y promoción de los derechos humanos, los principios democráticos, los principios de igualdad entre hombres y mujeres, de solidaridad, de accesibilidad universal y diseño para todos
D10	Orientación a la calidad y a la mejora continua
D11	Capacidad de aprendizaje autónomo
D13	Capacidad para integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información incompleta

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
RA1: Ser capaz de ejecutar políticas preventivas en base a resultados de monitorización	A2 B8 C4 C19 D2 D3 D6 D10 D11
RA2: Comprender las diferentes técnicas que se pueden emplear para la detección de intrusos en un sistema informático y saber cómo se pueden implementar.	B1 C4 C9 C21 D10 D11 D13
RA3: Entender las problemáticas de seguridad y los ataques a redes LAN y conocer los mecanismos que permiten minimizarlos	B1 B8 C4 C9 C19 C20 D7 D8 D9 D10
RA4: Conocer qué es un sistema de cortafuegos, cuál es su sistema de funcionamiento y cómo se puede utilizar para dotar de seguridad a una red informática.	B1 C4 C21 D7 D8 D9 D10 D11

Contenidos

Tema	
Vulnerabilidades y ataques en las redes de ordenadores.	- Conceptos generales: escucha, escaneo, técnicas activas, poissoning, HoneyPot, Red/Blue team - Ataque fuerza bruta WPA. - Otros
Protocolos de seguridad	Redes IP Seguridad en Redes IP. SSL/TLS
Mecanismos de defensa en redes	Medidas preventivas Medidas correctivas
Técnicas y herramientas de seguridad	Firewalls, iptables Accesos seguros VPN

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	10	20	30
Prácticas de laboratorio	28	40	68
Actividades introductorias	4	0	4
Trabajo tutelado	2	44	46
Examen de preguntas objetivas	2	0	2

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción

Lección magistral	Se realizarán clases expositivas para el desarrollo de los contenidos fundamentales de la materia y, para conseguir la participación activa de los estudiantes, se llevarán la acabo actividades individuales o en grupo que permitan aplicar los conceptos expuestos y resolver problemas. La asistencia es optativa.
Prácticas de laboratorio	Se realizarán sesiones de laboratorio guiadas que ayuden al alumno a conseguir los objetivos propuestos. La asistencia es optativa.
Actividades introductorias	Se presentarán ejemplos y casos de uso de los contenidos de la materia para despertar la curiosidad práctica del alumnado. La asistencia es optativa.
Trabajo tutelado	Se tutelará un trabajo práctico a realizar por el estudiante. La realización es voluntaria.

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	Se realizarán sesiones de laboratorio guiadas que ayuden al alumno a conseguir los objetivos propuestos.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje			
Prácticas de laboratorio	Resolución de prácticas y realización de informes con los resultados obtenidos. Los resultados del aprendizaje son: RA1, RA2, RA3, RA4	40	A2	B1 B8	C4 C9 C20	D2 D3 D6 D7 D8 D9 D10 D11 D13
Trabajo tutelado	Trabajo guiado que complementa los contenidos de la materia. Los resultados del aprendizaje son: RA1, RA2, RA3, RA4	40	A2	B1 B8	C4 C9 C20	D2 D3 D6 D7 D8 D9 D10 D11 D13
Examen de preguntas objetivas	Se realizará una prueba de conocimientos tanto teóricos cómo prácticos adquiridos a lo largo del curso. Los resultados del aprendizaje son: RA1, RA2, RA3, RA4	20	A2	B1 B8	C4 C9 C19 C21	D2 D3 D6 D7 D8 D9 D10 D11 D13

Otros comentarios sobre la Evaluación

Se ofrecerán dos alternativas de evaluación: continua y global.

SISTEMA DE EVALUACIÓN CONTÍNUA

La evaluación continua implicará:

- la realización de las prácticas(con la entrega de los informes de realización en las fechas marcadas. Tendrá una ponderación del 40%.

- la realización de un trabajo práctico propuesto por el alumno o por el profesor. Tendrá una ponderación del 40%

- la realización de una prueba tipo test de conocimientos generales de la materia. Tendrá una ponderación del 20%.

SISTEMA DE EVALUACIÓN GLOBAL

Se considera que el estudiantado opta por el sistema de evaluación global si no realiza el 50% de las prácticas.

Primera edición de las actas: este sistema se utilizará para el alumnado que no opte por la evaluación contínua.

Segunda edición de las actas y edición Fin de Carrera: este sistema se utilizará para todo el alumnado.

Prueba única: prueba tipo test y de respuesta larga.

Calificación: esta prueba puntuará 100%.

PROCESO DE CUALIFICACIÓN DE ACTAS

Independientemente de la convocatoria, la calificación en actas será la suma de los puntos obtenidos en cada una de las partes evaluadas. En el caso de no haber una puntuación mayor o igual que 5, se conservará la puntuación de las partes superadas para la 2ª convocatoria.

FECHAS DE EVALUACIÓN

El calendario de exámenes de evaluación aprobado oficialemente por la Xunta de Centro de la ESEI. Publicado en:https://esei.uvigo.es/docencia/exames/

EMPLEO DE DISPOSITIVOS MÓVILES

Se recuerda a todo el alumnado la prohibición del uso de dispositivos móviles en ejercicios y prácticas, en cumplimiento del artículo 13.2.d) del Estatuto del Estudiante Universitario, relativo a los deberes del estudiantado universitario, que establece el deber de "Abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad."

CONSULTA/SOLICITUD DE TUTORÍAS

Las tutorías pueden consultarse a través de la página personal del profesorado, accesible a través de https://esei.uvigo.es/docencia/profesorado/

OTROS COMENTARIOS

No se conservará ninguna de las notas obtenidas para os cursos académicos posteriores.

En caso de detección de plagio durante alguna de las entregas, se calificará al estudiante con un suspenso (0) y se comunicará la situación a la Dirección del Máster y a las autoridades universitarias correspondientes de cara a tomar las medidas oportunas.

Fuentes de información

Bibliografía Básica

William Stallings, **Cryptography and Networ k Security. Principles and Practices.**, Prentice Hall, 2010

Gert Schauwers, **Network Security Fundamentals**, Cisco Press, 2004

Bibliografía Complementaria

Recomendaciones