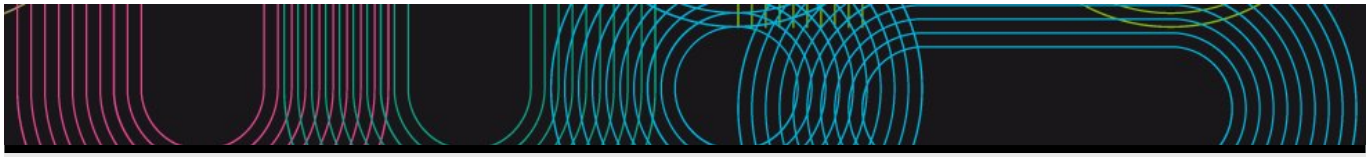

DATOS IDENTIFICATIVOS				
Seguridade en redes				
Materia	Seguridade en redes			
Código	O06M132V03312			
Titulación	Máster Universitario en Enxeñaría Informática			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OP	2	1c
Lingua de impartición	#EnglishFriendly Castelán Galego			
Departamento				
Coordinador/a	Diaz-Cacho Medina, Miguel Ramón			
Profesorado	Diaz-Cacho Medina, Miguel Ramón			
Correo-e	mcacho@uvigo.es			
Web	http://moovi.uvigo.gal			
Descrición xeral	A seguridade en redes de computadoras é un campo da ciencia e a tecnoloxía que abarca desde conceptos matemáticos até conceptos prácticos de programación e sistemas. A súa importancia é crucial no funcionamento global dos sistemas de comunicacións e Internet. A materia presentará os conceptos básicos e orientará os mesmos cara a unha compoñente eminentemente práctica.			

Competencias	
Código	
A2	(CB7) Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornos novos ou pouco coñecidos dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo
B1	Capacidade para proxectar, calcular e deseñar produtos, procesos e instalacions en todos os ámbitos da Enxeñería Informática
B8	Capacidade para a aplicación dos coñecementos adquiridos e de resolver problemas en entornos novos ou pouco coñecidos dentro de contextos máis amplos e multidisciplinares, sendo capaces de integrar estos coñecementos
C4	Capacidade para modelar, deseñar, definir a arquitectura, implantar, xestionar, operar, administrar e manter aplicacións, redes, sistemas, servizos e contidos informáticos.
C9	Capacidade para deseñar e avaliar sistemas operativos e servidores, e aplicacións e sistemas baseados en computación distribuida.
C19	Capacidade para optimizar as políticas de seguridade da infraestrutura da rede dunha entidade
C20	Capacidade para manexar correctamente sistemas operativos, redes e linguaxes de programación dende o punto de vista da seguridade informática e das comunicacións
C21	Capacidade para deseñar, desenvolver e xestionar mecanismos de seguridade no tratamento e acceso á información nun sistema de procesamiento local ou distribuido
D2	Capacidade para a dirección de equipos e organizacións
D3	Capacidade de liderado
D6	Habilidades de relacións interpersonales
D7	Capacidade de razonamiento crítico e creatividade
D8	Responsabilidade e compromiso ético no desempeño da actividade profesional
D9	Respecto e promoción dos dereitos humanos, os principios democráticos, os principios de igualdade entre homes e mulleres, de solidariedade, de accesibilidade universal e diseño para todos
D10	Orientación a a calidade e a mellora continua
D11	Capacidade de aprendizaxe autónomo
D13	Capacidade para integrar coñecementos e enfrontarse a complexidade de formular xuízos a partir dunha información incompleta

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
RA1: Ser capaz de executar políticas preventivas en base a resultados de monitorización	A2 B8 C4 C19 D2 D3 D6 D10 D11
RA2: Comprender as diferentes técnicas que se poden empregar para a deteción de intrusos nun sistema informático e saber como se poden implementar.	B1 C4 C9 C21 D10 D11 D13
RA3: Entender as problemáticas de seguridade e os ataques a redes LAN e coñecer os mecanismos que permiten minimizalos	B1 B8 C4 C9 C19 C20 D7 D8 D9 D10
RA4: Coñecer qué e un sistema de cortalumes, cal é o seu sistema de funcionamento e como se poder empregar para dotar de seguride a unha rede informática.	B1 C4 C21 D7 D8 D9 D10 D11

Contidos	
Tema	
Vulnerabilidades e ataques nas redes de computadores.	Escucha Escaneo Técnicas activas Poissoning. Ataque forza bruta *WPA. Outros
Protocolos de seguridade	Redes IP Seguridade en Redes IP.
Mecanismos de defensa en redes	Medidas preventivas Medidas correctivas
Técnicas e ferramentas de seguridade	Estado do arte

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	10	20	30
Prácticas de laboratorio	30	54	84
Actividades introdutorias	4	16	20
Exame de preguntas obxectivas	2	14	16

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

Metodoloxía docente	
	Descrición
Lección maxistral	Realizaranse clases expositivas para o desenvolvemento dos contidos fundamentais da materia e, para conseguir a participación activa dos estudantes, levaranse a cabo actividades individuais ou en grupo que permitan aplicar os conceptos expostos e resolver problemas.

Prácticas de laboratorio	Realizaranse sesións de laboratorio guiadas que axuden ao alumno a conseguir os obxectivos propostos.
Actividades introdutorias	Presentaránse exemplos e casos de uso dos contidos da materia para despertar a curiosidade práctica do alumnado.

Atención personalizada

Metodoloxías	Descrición
Prácticas de laboratorio	Realizaranse sesións de laboratorio guiadas que axuden ao alumno a conseguir os obxectivos propostos.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe			
Prácticas de laboratorio	Resolución de prácticas e realización de informes cos resultados obtidos.	50	A2	B1 B8	C4 C9 C20	D2 D3 D6 D7 D8 D9 D10 D11 D13
Exame de preguntas obxectivas	Se realizará una proba de coñecementos tanto teóricos como prácticos adquiridos ao longo do curso	50	A2	B1 B8	C4 C9 C19 C21	D2 D3 D6 D7 D8 D9 D10 D11 D13

Outros comentarios sobre a Avaliación

PRIMEIRA OPORTUNIDADE

Ofreceranse dúas alternativas de avaliación: continua e única.

A avaliación contínua implicará a realización das prácticas e unha proba mixta que serán avaliados nas porcentaxes arriba indicadas (50, 50), sendo necesario obter un cinco sobre dez na avaliación total. Igualmente, será necesario obter un dous e medio sobre cinco no exame de preguntas obxetivas para poder aprobar a materia. No caso de optar á avaliación contínua, o alumnado que realice calqueira tipo de entrega, non poderá calificarse como "non presentado".

No caso da avaliación única, toda a puntuación virá dada por unha única proba mixta que incluirá parte teórica e práctica. Dita proba realizarase ao final do bimestre e deberá obterse en total a lo menos un cinco sobre dez para poder aprobar a asignatura.

A selección da alternativa de avaliación deberá indicarse como moi tarde ao remate da segunda semana de clase.

Para cualquera das dúas alternativas darase flexibilidade horaria para o alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia.

SEGUNDA OPORTUNIDADE E CONVOCATORIAS EXTRAORDINARIAS

Os alumnos que optaran na primeira oportunidade pola avaliación contínua, terán a opción de conservar as notas de prácticas realizadas durante o curso académico. Dito alumnado realizará unha proba mixta, establécendose a nota nas porcentaxes indicadas arriba (50,50). O resto de alumnos (incluido o alumnado con recoñecmento de dedicación a tempo parcial e dispensa académica de exención de asistencia) trataranse coma alumnos de avaliación única e realizarán unha proba mixta que mesture parte teórica e práctica.

PROCESO DE CUALIFICACIÓN DE ACTAS.

Independentemente da convocatoria, na cualificación en actas sumaranse os puntos obtidos en cada unha das partes avaliadas. No caso de non obter unha puntuación >5, conservaranse as cualificacións das partes superadas para a 2a convocatoria.

DATAS DE AVALIACIÓN
O calendario de probas de avaliación aprobado oficialmente pola Xunta de Centro da ESEI atópase publicado na páxina webhttps://esei.uvigo.es/docencia/exames/

OUTROS COMENTARIOS

Non se conservará ningunha das notas obtidas para os cursos académicos posteriores.

No caso de detección de plaxio durante algunha das entregas, calificarse ao alumno/a cun suspenso (0) e comunicarase a situación á dirección do máster e ás autoridades universitarias correspondentes de cara a tomar as medidas oportunas.

Bibliografía. Fontes de información

Bibliografía Básica

William Stallings, **Cryptography and Networ k Security. Principles and Practices.**, ISBN13 9781292158587 ISBN 1292158581, Prentice Hall,

Gert Schauwers, **Network Security Fundamentals**, ISBN 1587051672, Cisco Press,

Bibliografía Complementaria

Recomendacións

Plan de Continxencias

Descrición

=== MEDIDAS EXCEPCIONAIS PLANIFICADAS ===

ESCENARIO 1: DOCENCIA MIXTA

Debido á situación excepcional, ante a imposibilidade de poder impartir a docencia dun modo completamente presencial, utilizaranse medios virtuais para a impartición das clases non presenciais.

Para a parte non presencial utilizaranse os medios proporcionados pola Universidade, actualmente o "Campus Remoto" e FAITIC. No entanto poderase complementar con outros medios.

ESCENARIO 2: DOCENCIA NON PRESENCIAL

Debido á situación excepcional, ante a imposibilidade de poder impartir a docencia dun modo presencial, utilizaranse medios virtuais para a impartición das clases.

Utilizaranse os medios proporcionados pola Universidade, actualmente o "Campus Remoto" e FAITIC. No entanto poderase complementar con outros medios.

=== ADAPTACIÓN DAS METODOLOXÍAS ===

Para as prácticas de laboratorio, substituiranse as prácticas que requiran de equipamento específico por outro simulado ou virtualizado. Eventualmente proporanse prácticas alternativas que non requiran de devandito equipamento. Estas prácticas poderán ter un formato autónomo en previsión de problemas de conciliación e/ou conectividade.

As sesións de tutorización (atención ao alumnado) realizaranse por medios telemáticos (Correo electrónico, Foros de FAITIC, Campus Remoto), que se poderán complementar entre si e con outras ferramentas. Nalgunhas delas utilizarase unha modalidade de concertación previa.

=== ADAPTACIÓN DA AVALIACIÓN ===

A avaliación realizarase de xeito contínuo, mantendo a mesma metodoloxía en ambos escenarios coa seguinte adaptación:

- a proba presencial sustituirase por unha proba online utilizando Campus Remoto e FAITIC.
- as entregas de resultados das prácticas e/ou traballos sustitutivos das mesmas realizaranse online.