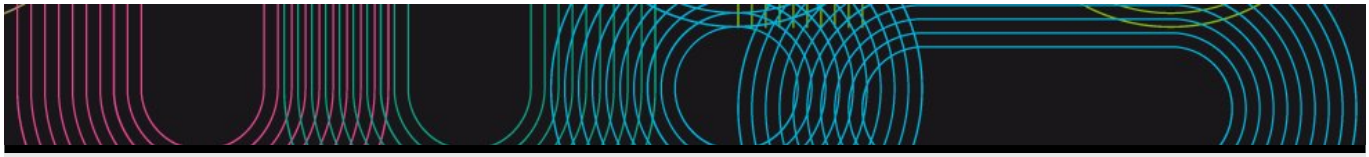

DATOS IDENTIFICATIVOS				
Seguridade en redes				
Materia	Seguridade en redes			
Código	O06M132V03312			
Titulación	Máster Universitario en Enxeñaría Informática			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OP	2	1c
Lingua de impartición	Castelán Galego			
Departamento				
Coordinador/a	Diaz-Cacho 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.			

Resultados de Formación e Aprendizaxe	
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 previstos na materia

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.	- Conceptos xerais: escoita, escaneo, técnicas activas, poissoning, HoneyPot, Red/Blue team - Ataque forza bruta WPA. - Outros
Protocolos de seguridade	Redes IP Seguridade en Redes IP. SSL/TLS
Mecanismos de defensa en redes	Medidas preventivas Medidas correctivas
Técnicas e ferramentas de seguridade	Firewalls, iptables Accesos seguros VPN

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	10	20	30
Prácticas de laboratorio	28	40	68
Actividades introdutorias	4	0	4
Traballo tutelado	2	44	46
Exame de preguntas obxectivas	2	0	2

*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. A asistencia é optativa.
Prácticas de laboratorio	Realizaranse sesións de laboratorio guiadas que axuden ao alumno a conseguir os obxectivos propostos. A asistencia é optativa.
Actividades introdutorias	Presentaránse exemplos e casos de uso dos contidos da materia para despertar a curiosidade práctica do alumnado. A asistencia é optativa.
Traballo tutelado	Tutelarase un traballo práctico a realizar polo estudante. A realización é voluntaria.

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.	40	A2	B1 B8	C4 C9 C20	D2 D3 D6 D7 D8 D9 D10 D11 D13
Traballo tutelado	Traballo guiado que complementa os contidos da materia. Os resultados da aprendizaxe son: *RA1, *RA2, *RA3, *RA4	40	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	20	A2	B1 B8	C4 C9 C19 C21	D2 D3 D6 D7 D8 D9 D10 D11 D13

Outros comentarios sobre a Avaliación

Ofreceranse dúas alternativas de avaliación: continua e global.

SISTEMA DE AVALIACIÓN CONTINUA

A avaliación continua consistirá en:

- Realización das prácticas (coa entrega dos informes de realización nas datas sinaladas. Terá unha ponderación do 40 %).

- Realización dun traballo práctico proposto polo alumno ou o profesor. Terá unha ponderación do 40%

- Realización dunha proba tipo test de coñecementos xerais da materia. Terá unha ponderación do 20%.

SISTEMA DE AVALIACIÓN GLOBAL

Considérase que o alumnado opta polo sistema de avaliación global se non realiza o 50% das prácticas.

Primeira edición das actas: este sistema empregarase para o alumnado que non opte pola avaliación continua.

Segunda edición das actas e edición de Fin de Grao: este sistema será empregado para todo o alumnado.

Proba única: proba de opción múltiple e resposta longa. Puntuación: Esta proba puntuará o 100%.

REGISTRO PROCESO DE CUALIFICACIÓN

Independentemente da convocatoria, a cualificación en actas será a suma dos puntos obtidos en cada unha das partes avaliadas. No caso de non ter unha puntuación superior ou igual a 5, a puntuación das partes superadas conservarase para a 2a convocatoria.

DATAS DE AVALIACIÓN

O calendario de exames de avaliación aprobado oficialmente pola Xunta de Centro da ESEI. Publicado en: https://esei.uvigo.es/docencia/exames/

EMPREGO DE DISPOSITIVOS MÓBILES

Lémbrase a todo o alumnado a prohibición do uso de dispositivos móbiles en exercicios e prácticas, en cumprimento do artigo 13.2.d) do Estatuto do Estudante Universitario, relativo aos deberes do estudantado universitario, que establece o deber de "Absterse da utilización ou cooperación en procedementos fraudulentos nas probas de avaliación, nos traballos que se realicen ou en documentos oficiais da universidade."

CONSULTA/SOLICITUDE DE TITORÍAS

As titorías poden consultarse a través da páxina persoal do profesorado, accesible a través de https://esei.uvi

OUTROS COMENTARIOS

Non se conservará ningunha das cualificacións obtidas para cursos académicos posteriores. No caso de detectarse plaxio durante algunha das entregas, o alumno ou alumna será cualificada cun suspenso (0) e a situación será comunicada ao Departamento de Máster e ás autoridades universitarias correspondentes para que adopten as medidas oportunas.

Bibliografía. Fontes 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

Recomendacións