Guía Docente				
Datos Identificativos				2023/24
Asignatura (*)	Redes Seguras		Código	614530105
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	1º cuadrimestre	Primeiro	Obrigatoria	5
Idioma	CastelánGalego			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións			
Coordinación	Nóvoa Manuel, Francisco Javier	Correo electrónico	francisco.javier.novoa@udc.es	
Profesorado	Nóvoa Manuel, Francisco Javier	Correo electrónico	francisco.javier.novoa@udc.es	
Web	moovi.uvigo.gal			
Descrición xeral	A materia Redes Seguras ten como obxectivo principal que os estudantes aprendan a deseñar e implementar infraestruturas de rede capaces de proporciona-los servizos de seguridade precisos nun contorno corporativo moderno. Deberán coñecer as arquitecturas de seguridad de referencia e seren quen de configuralas en mantelas, utilizando para iso tecnoloxías como IDS/IPS e Firewalls entre outros. A materia esta concebida para que as prácticas de laboratorio, con equipos físicos e virtuáis teñan unha importancia capital no proceso de aprendizaxe			

Competencias / Resultados do título	
Código	Competencias / Resultados do título
A25	HD-05 - Diseñar e implementar redes seguras, seleccionando y configurando los dispositivos adecuados para cada sección de la red y utilizando proactivamente la monitorización de red como de modo que se implemente correctamente la política de seguridad de la organización
B21	K-05 - Conocer de las vulnerabilidades en los dispositivos y tecnologías de acceso de red, las herramientas para explorarlas y las medidas de protección para obtener redes de comunicaciones seguras, así como comprender el concepto de política de seguridad aplicado a redes, la seguridad perimetral y los cortafuegos
C7	C-02 - Demostrar autonomía e iniciativa para resolver problemas complejos que involucren múltiples tecnologías en el ámbito de las redes o los sistemas de comunicaciones, y desarrollar soluciones innovadoras en el campo de las comunicaciones y la computación distribuida privadas.
C10	C-05 - Analizar la seguridad de los protocolos de comunicación en la capa física; de enlace; de red y de transporte, así como evaluar en una red corporativa las medidas de seguridad que es necesario implantar para la protección de sus activos internos y sus comunicaciones
C15	C-10 - Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Comprenderán o papel dun firewall na estratexia de seguridade dun dispositivo final ou da rede á que protexe	AP25	BP21	
Serán quen de describir que son as políticas de acceso e de deseñar/especificar o conxunto das mesmas que son requiridas nun escenario ou caso particular			CP7 CP15
Coñecerán os diferentes tipos de filtrado de paquetes (con/sen estado) e os firewalls de nivel de aplicación, e saberán configuralos en diversas plataformas	AP25		
Poderán deseñar e describir, para un escenario/topoloxía concretos, configuracións alternativas para coloca-lo firewall dentro da rede corporativa (sistema fortificado, DMZ, tornalumes distribuído)	AP25		CP7 CP10

Serán quen de describi-los principios básicos que sustentan a deteción de intrusións, os sensores habituais que se usan para a recopilación de información, e as técnicas de análise (deteción de anomalías, versus deteción heurística) que deciden cando disparar unha alarma. Coñecerán posibles solucións técnicas (HIDS, NIDS, IPS, SIEM, honeypot), que saberán instalar e configurar para algunhas plataformas e implementacións particulares	AP25		CP15
Estarán familiarizados cos conceptos de túnel e virtualización de redes, e serán quen de elixir e implementar a tecnoloxía de rede privada virtual máis axeitada para diferentes escenarios	AP25	BP21	CP15
Poderán explica-los principios sobre os que se constrúen as redes anónimas			CP7

Contidos	
Temas	Subtemas
1.- Deseño de Redes Seguras	1.1. Arquitecturas de Rede Corporativa 1.2. Patróns de deseño 1.3. Aproximacións de seguridade perimetral
2.- Fundamentos de IPv6	2.1. Enderezos de rede IPv6 2.2. Configuración de enderezos IPv6 2.3. Enderezos multicast en IPv6 2.4. ICMPv6 2.5. Protocolos de encamiñamento en IPv6
3.- Fortificación dos Dispositivos de Rede	3.1. Arquitectura interna dos Dispositivos de Rede 3.2. Protección do Plano de datos 3.3. Protección do Plano de control 3.4. Protección do Plano de xestión
4. Firewalls	4.1. Filtrado de paquetes estático 4.2. Filtrado dinámico de paquetes 4.3. Filtrado en capa de aplicación 4.4. Firewalls baseados en zonas de seguridade 4.5. Next-Generation Firewalls 4.6. NAT/NATP
5. IDS/IPS	5.1. Sistemas baseados en rede 5.2. Sistemas baseados en equipo final
6. Monitorización	6.1. Syslog 6.2. SNMP 6.3. Netflow 6.4. SIEM
7. VPNs sobre MPLS	7.1 Introdución a tecnoloxía MPLS 7.2 VPNs de MPLS

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Prácticas a través de TIC	C10 C15	21	39	60
Proba obxectiva	A25 B21 C7 C10	1	0	1
Proba práctica	A25 B21 C7	2	0	2
Proba de ensaio	C7	1	0	1
Sesión maxistral	A25 B21 C15	21	38	59
Atención personalizada		2	0	2
*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado				

Metodoloxías

Metodoloxías	Descrición
Prácticas a través de TIC	Nas que o estudante verá o funcionamento na práctica dalgún dos contidos teóricos vistos nas clases maxistrais. Nestas prácticas, o alumno utilizará diferentes ferramentas (equipamento de rede, simuladores de rede, ferramentas de monitorización, etc.) propostas polos profesores, que lle van permitir afondar e afianzar os seus coñecementos sobre diferentes aspectos das redes seguras. Ademais das prácticas básicas que todos os alumnos terán que facer, proporanse prácticas adicionais que os alumnos interesados poderán realizar de forma opcional.
Proba obxectiva	Ao remate da exposición da materia, llevarase a cabo unha proba tipo test que permitirá valorar os coñecementos teóricos e habilidades prácticas acadadas durante o desenvolvemento do curso..
Proba práctica	Ao remate da realización dos laboratorios de prácticas, realizarase unha proba na que o alumno deberá demostrar-las competencias adquiridas. Partindo dun escenario inicial (rede non segura) solicitarase ao estudante que a protexa utilizando estratexias e técnicas abordados na materia, especialmente nos laboratorios prácticos.
Proba de ensaio	Ao remate da exposición da materia e da realización das prácticas a través de TIC, levarase a cabo unha proba de desenvolvemento de un ou dous temas abordados na materia, onde alumno deberá demostrar unha comprensión avanzada de este ou ser quen de resolver un problema complexo.
Sesión maxistral	Nas que se exporá o contido teórico do temario, incluíndo exemplos ilustrativos e con soporte de medios audiovisuais. O alumno disporá do material de apoio (apuntes, copia das transparencias, artigos, etc.) con anterioridade e o profesor promoverá unha actitude activa, recomendando a lectura previa dos puntos do temario a tratar cada día en clase, así como realizando preguntas que permitan aclarar aspectos concretos e deixando cuestións abertas para a reflexión do alumno. As sesións maxistrais poderán ser complementadas coa realización de conferencias nas que acudirá algún experto externo para tratar algún tema con maior profundidade.

Atención personalizada	
Metodoloxías	Descrición
Prácticas a través de TIC	A atención personalizada durante as prácticas servirá para orientar e comprobar o traballo que os alumnos vaian realizando segundo as indicacións que se lles proporcionen, dependendo da práctica concreta da que se trate. Todos os profesores da materia proporán ademais un horario de titorías no que os alumnos poderán resolver calquera dúbida relacionada co desenvolvemento da mesma. Recomendarase aos alumnos a asistencia a titorías como parte fundamental do apoio á aprendizaxe. O horario de titorías de Francisco Javier Nóvoa está dispoñible en https://pdi.udc.es/es/File/Pdi/HB9HJ e o do profesor Raúl Rodríguez Rubie en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/raul-fernando-rodriguez-rubio Facilitarase a realización das prácticas e a atención na titorización de traballos aos alumnos que, por estar matriculados a tempo parcial no poidan asistir ás sesións prácticas ou ás sesiones de titoría establecidas oficialmente.

Avaliación			
Metodoloxías	Competencias / Resultados	Descrición	**Cualificación**
Proba práctica	A25 B21 C7	Ao remate da realización dos laboratorios de prácticas, realizarase unha proba na que o alumno deberá demostrar-las competencias adquiridas. Partindo dun escenario inicial (rede non segura) solicitarase ao estudante que a protexa utilizando estratexias e técnicas abordados na materia, especialmente nos laboratorios prácticos.	30

Proba de ensaio	C7	Ao remate da exposición da materia e da realización das prácticas a través de TIC, levarase a cabo unha proba de desenvolvemento de un ou dous temas abordados na materia, onde alumno deberá demostrar unha comprensión avanzada de este ou ser quen de resolver un problema complexo.	10
Prácticas a través de TIC	C10 C15	As prácticas da materia consistirán en diferentes actividades relacionadas co deseño e implementación de Redes Seguras. Levarase a cabo unha memoria das prácticas para valorar o nivel de comprensión e o traballo desenvolvido polo alumno	20
Proba obxectiva	A25 B21 C7 C10	Ao final da exposición da materia, realizarase unha proba obxectiva tipo test sobre os contidos tratados, tanto nas sesións teóricas como nas prácticas	40

Observacións avaliación

Será necesario obter como mínimo o 50% da nota para aprobar a materia. Ademais, para supera-la materia será preciso (en calquera oportunidade) obter un mínimo dun 40% da nota final na proba obxectiva, na proba de ensaio e nas prácticas (prácticas a través de TIC e proba práctica). En caso contrario, a nota máxima que se poderá obter é de 4.5.

PRIMEIRA OPORTUNIDADE - CONVOCATORIA ORDINARIA

A avaliación das prácticas de laboratorio realizarase mediante a presentación de catro memorias de prácticas relacionadas cos exercicios de laboratorio e terá un peso total do 20% da nota final. Realizarase tamén unha proba práctica que terá un peso do 30% sobre a nota final. Será preciso obter un mínimo dun 40% en prácticas (prácticas a través de TIC e proba práctica) para supera-la materia.

O 40% da nota da primeira oportunidade poderase acadar por medio da realización dunha proba obxectiva (exame), que poderá conter preguntas relacionadas cos conceptos desenvolvidos nas clases de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

O 10% da nota restante da primeira oportunidade poderase acadar por medio da realización dunha proba de ensaio, que poderá conter preguntas relacionadas cos conceptos desenvolvidos nas clases de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

SEGUNDA OPORTUNIDADE - CONVOCATORIA EXTRAORDINARIA

Poderán conservar a nota obtida nas prácticas ou na proba obxectiva da primeira oportunidade sempre e cando obtiveran unha valoración igual ou superior ao 50% do seu peso na nota final.

A avaliación das prácticas na segunda oportunidade levarase a cabo mediante a defensa dun exercicio único en laboratorio, á finalización da proba obxectiva da segunda oportunidade.

O 40% da nota da primeira oportunidade poderase acadar por medio da realización dunha proba obxectiva (exame), que poderá conter preguntas relacionadas cos conceptos desenvolvidos nas clases de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

O 10% da nota restante da primeira oportunidade poderase acadar por medio da realización dunha proba de ensaio, que poderá conter preguntas relacionadas cos conceptos desenvolvidos nas clases de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

CONVOCATORIA ADIANTADA

Poderán conserva-la nota obtida en prácticas, sempre e cando obtiveran unha valoración igual ou superior ó 50% do seu peso final.

A avaliación das prácticas (50% da nota final) levarase a cabo mediante unha proba práctica.

O 40% da nota da primeira oportunidade poderase acadar por medio da realización dunha proba obxectiva (exame), que poderá conter preguntas relacionadas cos conceptos desenvolvidos nas clases de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

O 10% da nota restante da primeira oportunidade poderase acadar por medio da realización dunha proba de ensaio, que poderá conter preguntas relacionadas cos conceptos desenvolvidos nas clases de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

ESTUDANTES CON MATRÍCULA A TEMPO PARCIAL OU CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA: Deberán poñerse en contacto cos profesores da materia para posibilitar a realización das tarefas fóra da organización habitual de materia.

Fontes de información

Bibliografía básica	- Anthony Bruno; Steve Jordan (2020). CCNP Enterprise Design ENSLD 300-420 Official Cert Guide: Designing Cisco Enterprise Networks. Cisco Press - Omar Santos (2020). CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. Cisco Press - Brad Edgeworth, Kevin Wallace, Jason Gooley, David Hucaby, Ramiro Garza Rios (2019). CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. Cisco Press - Wendell Odom (2019). CCNA 200-301 Official Cert Guide Library. Cisco Press
Bibliografía complementaria	- Kulbir Saini (2011). Squid Proxy Server 3.1 Beginner's Guide. Packt Publishing

Recomendacións
Materias que se recomenda ter cursado previamente
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Test de Intrusión/614530008 Seguridade en Comunicacións/614530004
Observacións