Guia docente					
Datos Identificativos					2023/24
Asignatura (*)	Redes Seguras			Código	614530105
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Periodo	Curso		Tipo	Créditos
Máster Oficial	1º cuatrimestre	Primero		Obligatoria	5
Idioma	CastellanoGallego				
Modalidad docente	Presencial				
Prerrequisitos					
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións				
Coordinador/a	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				
Descripción general	La materia Redes Seguras tiene como objetivo principal que los estudiantes aprendan a diseñar e implementar infraestructuras de red que sean capaces de proporcionar los servicios de seguridad necesarios en un entorno corporativo moderno. Deberán conocer las arquitecturas de seguridad de referencia y ser capaces de configurarlas y administrarlas, utilizando para ello tecnologías como IDS/IPS y Firewalls, entre otras. La materia esta concebida para que las prácticas de laboratorio, con equipos físicos y virtuales tengan una importancia capital en el proceso de aprendizaje.				

Competencias del título	
Código	Competencias del 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 de aprendizaje			
Resultados de aprendizaje	Competencias del título		
Comprenderán el papel de un cortafuegos en la estrategia de seguridad de un dispositivo final o de la red a la que protege	AP25	BP21	
Serán capaces de describir qué son las políticas de acceso y de diseñar/especificar el conjunto de las mismas que requiere un escenario o caso particular			CP7 CP15
Conocerán los diferentes tipos de filtrado de paquetes (con/sin estado) y los cortafuegos de nivel de aplicación, y sabrán configurarlos en diversas plataformas	AP25		
Podrán diseñar y describir, para un escenario/topología concreto, configuraciones alternativas para emplazar el cortafuegos dentro de la red corporativa (sistema fortificado, DMZ, cortafuegos distribuido)	AP25		CP7 CP10

Serán capaces de describir los principios básicos que sustentan la detección de intrusiones, los sensores habituales que utilizan para la recopilación de información, y las técnicas de análisis (detección de anomalías versus detección heurística) que deciden cuándo disparar una alarma. Conocerán posibles soluciones técnicas (HIDS/NIDS, IPS, SIEM, honeypot), que sabrán instalar y configurar para algunas plataformas e implementaciones particulares	AP25		CP15
Estarán familiarizados con los conceptos de túnel y virtualización de redes, y serán capaces de elegir e implementar la tecnología de red privada virtual más apropiada para diferentes escenarios	AP25	BP21	CP15
Podrán explicar los principios sobre los que se construyen las redes anónimas			CP7

Contenidos	
Tema	**Subtema**
1.- Diseño de Redes Seguras	1.1. Arquitecturas de Red Corporativa 1.2. Patrones de diseño 1.3. Aproximaciones de seguridad perimetral
2.- Fundamentos de IPv6	2.1. Direcciones de red IPv6 2.2. Configuración de direcciones IPv6 2.3. Direcciones multicast en IPv6 2.4. ICMPv6 2.5. Protocolos de enrutamiento en IPv6
3.- Fortificación de los Dispositivos de Red	3.1. Arquitectura Interna de los Dispositivos de Red 3.2. Protección en el Plano de datos 3.3. Protección en el Plano de control 3.4. Protección en el Plano de gestión
4.- Firewalls	4.1. Filtrado de paquetes estático 4.2. Filtrado dinámico de paquetes 4.3. Filtrado en capa de aplicación. 4.4. Firewalls basados en zonas de seguridad 4.5. Next-generation Firewalls 4.6. NAT/NATP
5.- IDS/IPS	5.1. Sistemas en red 5.2. Sistemas para equipos finales
6.- Monitorización	6.1 Syslog 6.2 SNMP 6.3 Netflow 6.4 SIEM
7. VPNs sobre MPLS	7.1 Introducción a la tecnología MPLS 7.2 VPNs sobre MPLS

Planificación				
Metodologías / pruebas	**Competéncias**	**Horas presenciales**	**Horas no presenciales / trabajo autónomo**	**Horas totales**
Prácticas a través de TIC	C10 C15	21	39	60
Prueba objetiva	A25 B21 C7 C10	1	0	1
Prueba práctica	A25 B21 C7	2	0	2
Prueba de ensayo/desarrollo	C7	1	0	1
Sesión magistral	A25 B21 C15	21	38	59
Atención personalizada		2	0	2
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	**Descripción**
Prácticas a través de TIC	En las que el alumno verá el funcionamiento en la práctica de alguno de los contenidos teóricos vistos en las clases magistrales. En estas prácticas, el alumno utilizará diferentes herramientas (equipamiento de red, simuladores de red, herramientas de monitorización, etc.) propuestas por el profesor, que le permitirán profundizar y afianzar sus conocimientos sobre diferentes aspectos de la seguridad en redes. Además de las prácticas básicas que todos los alumnos tendrán que hacer, se propondrán prácticas adicionales que los alumnos interesados podrán realizar de forma opcional.
Prueba objetiva	Al final de la exposición de la materia, se llevará a cabo una prueba tipo test que permitirá valorar los conocimientos teóricos y habilidades prácticas adquiridas durante la evolución del curso.
Prueba práctica	Al final de la realización de los laboratorios de prácticas, se realizará una prueba en la que el alumno deberá demostrar las competencias adquiridas. Partiendo de un escenario inicial (red no segura) se solicitará al estudiante que la proteja utilizando las estrategias y técnicas abordados en la materia, especialmente en los laboratorios prácticos.
Prueba de ensayo/desarrollo	Al final de la exposición de la materia y de la realización de las prácticas a través de TIC, se llevará a cabo una prueba de desarrollo de uno o dos temas abordados en la materia, donde el alumno deberá demostrar una comprensión avanzada de éste o ser capaz de resolver un problema complejo.
Sesión magistral	En las que se expondrá el contenido teórico del temario, incluyendo ejemplos ilustrativos y con el soporte de medios audiovisuales. El alumno dispondrá del material de apoyo (apuntes, copias de las transparencias, artículos, etc.) con anterioridad y el profesor promoverá una actitud activa, recomendando la lectura previa de los puntos del temario a tratar cada día en clase, así como realizando preguntas que permitan aclarar aspectos concretos y dejando cuestiones abiertas para la reflexión del alumno. Las sesiones magistrales se complementarán con la realización de conferencias en las que se traerá a algún experto externo para tratar algún tema con mayor profundidad.

Atención personalizada	
Metodologías	**Descripción**
Prácticas a través de TIC	La atención personalizada durante las prácticas servirá para orientar y comprobar el trabajo que vayan haciendo los alumnos según las indicaciones que se les proporcionen, dependiendo de la fase concreta de la práctica de la que se trate. Todos los profesores de la materia propondrán además un horario de tutorías e el que los alumnos podrán resolver cualquier duda relacionada con el desarrollo de la misma. Se recomendará a los alumnos la asistencia a las tutorías como parte fundamental del apoyo al aprendizaje. El horario de tutorías de Francisco Javier Nóvoa está disponible en https://pdi.udc.es/es/File/Pdi/HB9HJ y el del profesor Raúl Rodríguez Rubio en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/raul-fernando-rodriguez-rubio Se facilitará la realización de las prácticas y la atención en la tutorización de trabajos a alumnos que, por estar matriculados a tiempo parcial no puedan asistir a las sesiones prácticas o a las sesiones de tutoría establecidas oficialmente.

Evaluación			
Metodologías	**Competéncias**	**Descripción**	**Calificación**
Prueba práctica	A25 B21 C7	Al final de la realización de los laboratorios de prácticas, se realizará una prueba en la que el alumno deberá demostrar las competencias adquiridas. Partiendo de un escenario inicial (red no segura) se solicitará al estudiante que la proteja utilizando las estrategias y técnicas abordados en la materia, especialmente en los laboratorios prácticos.	30

Prueba de ensayo/desarrollo	C7	Al final de la exposición de la materia y de la realización de las prácticas a través de TIC, se llevará a cabo una prueba de desarrollo de uno o dos temas abordados en la materia, donde el alumno deberá demostrar una comprensión avanzada de éste o ser capaz de resolver un problema complejo.	10
Prácticas a través de TIC	C10 C15	Las prácticas de la materia consistirán en diferentes actividades relacionadas con el diseño e implementación de Redes Seguras. Se llevará a cabo una memoria de las prácticas para valorar el nivel de comprensión y el trabajo desarrollado por el alumno	20
Prueba objetiva	A25 B21 C7 C10	Al final de la exposición de la materia, se realizará una prueba objetiva tipo test sobre los contenidos tratados, tanto en las sesiones teóricas como en las prácticas	40

Observaciones evaluación

Será necesario obtener como mínimo el 50% de la nota para aprobar la materia. Además para superar la materia, será preciso (en cualquier oportunidad) obtener un mínimo de un 40% de la nota total en la prueba objetiva, en la prueba de ensayo y en las prácticas (prácticas a través de TIC y prueba práctica). En caso contrario, la nota máxima que se podrá obtener es de 4.5.

PRIMERA OPORTUNIDAD - CONVOCATORIA ORDINARIA

La evaluación de las prácticas de laboratorio a través de TIC se realizará mediante la presentación de cuatro memorias de prácticas relacionadas con los ejercicios de laboratorio y tendrá un peso total del 20% de la nota final. Se realizará también un examen de prácticas que tendrá un peso de un 30% sobre la nota final. Será necesario obtener un mínimo de un 40% en prácticas (prácticas a través de TIC y prueba práctica) para superar la materia.

Un 40% de la nota de la primera oportunidad se podrá conseguir por medio de la realización de una prueba objetiva (examen), que podrá contener preguntas relacionadas con los conceptos desarrollados en clase de teoría, prácticas, tutoriales proporcionados y material bibliográfico básico.

El 10% de la nota restante de la primera oportunidad se podrá conseguir por medio de la realización de una prueba de ensayo, que podrá contener preguntas relacionadas con los conceptos desarrollados en clase de teoría, prácticas, tutoriales proporcionados y material bibliográfico básico.

SEGUNDA OPORTUNIDAD - CONVOCATORIA EXTRAORDINARIA

Podrán conservar la nota obtenida en prácticas de la primera oportunidad siempre y cuando hayan obtenido una valoración igual o superior al 50% de su peso en la nota final.

La evaluación de las prácticas (50% de la nota final) se llevará a cabo mediante una prueba práctica.

Un 40% de la nota se podrá conseguir por medio de la realización de una prueba objetiva (examen), que podrá contener preguntas relacionadas con los conceptos desarrollados en clase de teoría, prácticas, tutoriales proporcionados y material bibliográfico básico.

El 10% de la nota restante se podrá conseguir por medio de la realización de una prueba de ensayo, que podrá contener preguntas relacionadas con los conceptos desarrollados en clase de teoría, prácticas, tutoriales proporcionados y material bibliográfico básico.

CONVOCATORIA ADELANTADA

La evaluación de las prácticas se llevará a cabo mediante una prueba práctica (50% de la nota).

Un 40% de la nota se podrá conseguir por medio de la realización de una prueba objetiva (examen), que podrá contener preguntas relacionadas con los conceptos desarrollados en clase de teoría, prácticas, tutoriales proporcionados y material bibliográfico básico.

El 10% de la nota restante se podrá conseguir por medio de la realización de una prueba de ensayo, que podrá contener preguntas relacionadas con los conceptos desarrollados en clase de teoría, prácticas, tutoriales proporcionados y material bibliográfico básico.

ESTUDIANTES CON MATRÍCULA A TIEMPO PARCIAL O CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA: Deberán ponerse en contacto con los profesores de la asignatura para posibilitar la realización de las tareas fuera de la organización habitual de la materia.

La realización fraudulenta de pruebas o actividades de evaluación, una vez comprobada, supondrá directamente la calificación de suspenso en la convocatoria en la que se cometa: el alumno será calificado con "suspenso" (calificación numérica 0) en la correspondiente convocatoria del curso académico, tanto si la infracción se comete en la primera oportunidad como en la segunda. Para ello, se modificará su calificación en el acta de la primera oportunidad, en caso de ser necesario

Fuentes de información

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
Complementária	- Kulbir Saini (2011). Squid Proxy Server 3.1 Beginner's Guide. Packt Publishing

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Test de Intrusión/614530008 Seguridad en Comunicaciones/614530004
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías