UNIVERSIDADE DA CORUÑA

Guia docente				
Datos Identificativos				2019/20
Asignatura (*)	Redes Seguras		Código	614530006
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	1º cuatrimestre	Primero	Obligatoria	6
Idioma	CastellanoGallego			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicacións			
Coordinador/a	Novoa De Manuel, Francisco Javier	Correo electrónico	francisco.javier.novoa@udc.es	
Profesorado	Novoa De Manuel, Francisco Javier	Correo electrónico	francisco.javier.novoa@udc.es	
Web	faitic.uvigo.es			
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 / Resultados del título	
Código	Competencias / Resultados del título
A2	CE2 - Conocer en profundidad las técnicas de ciberataque y ciberdefensa
A4	CE4 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información
A8	CE8 - Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
A12	CE12 - Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura
B2	CB2 - 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
B4	CB4 - Que los estudiantes sepan comunicar sus conclusiones, y los conocimientos y razones últimas que las sustentan, a públicos especializados y no especializados de un modo claro y sin ambigüedades
B5	CB5 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
B6	CG1 - Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
B8	CG3 - Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas 14 de comunicaciones
C4	CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados 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	AP2 AP8	BP2 BP6	
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	AP8 AP12	BP2 BP4 BP6 BP8	CP4

Conocerán los diferentes tipos de filtrado de paquetes (con/sin estado) y los cortafuegos de nivel de aplicación, y sabrán configurarlos en diversas plataformas	AP2	BP6 BP8	
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)	AP8	BP2 BP6 BP8	
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	AP2 AP8	BP6 BP8	
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	AP2 AP4	BP6	
Podrán explicar los principios sobre los que se construyen las redes anónimas	AP2	BP4 BP5	CP4

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.- Fortificación de los Dispositivos de Red	2.1. Arquitectura Interna de los Dispositivos de Red 2.2. Protección en el Plano de datos 2.3. Protección en el Plano de control 2.4. Protección en el Plano de gestión
3.- Firewalls	3.1. Filtrado de paquetes estático 3.2. Filtrado dinámico de paquetes 3.3. Filtrado en capa de aplicación. 3.4. Firewalls basados en zonas de seguridad 3.5. Next-generation Firewalls 3.6. NAT/NATP
4.- IDS/IPS	4.1. Sistemas en red 4.2. Sistemas para equipos finales
5.- Monitorización	5.1 Syslog 5.2 SNMP 5.3 Netflow 5.4 SIEM
6. VPNs sobre MPLS	6.1 Introducción a la tecnología MPLS 6.2 VPNs sobre MPLS

Planificación				
Metodologías / pruebas	**Competencias / Resultados**	**Horas lectivas (presenciales y virtuales)**	**Horas trabajo autónomo**	**Horas totales**
Prácticas a través de TIC	A2 A8 B2 B5 B6	21	52	73
Prueba objetiva	A8 B2 B4 B6 B8	2	0	2
Trabajos tutelados	B4 B6 B8	0	10	10
Sesión magistral	A2 A4 A8 A12 B8 C4	21	42	63
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.
Trabajos tutelados	Propuesta de trabajos para su resolución individual y no presencial por parte de los alumnos. Estos trabajos serán opcionales y les permitirán a los alumnos interesados en hacerlos, profundizar en aspectos del temario que les interesen especialmente y que no se hayan podido tratar con detalle suficiente durante las sesiones magistrales.
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 Trabajos tutelados	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. Para la realización de los trabajos tutelados, los profesores proporcionarán las indicaciones iniciales necesarias, bibliografía para consulta y realizarán un seguimiento de los avances que el alumno vaya realizando, para ofrecer las orientaciones pertinentes en cada caso, de modo que se asegure la calidad de los trabajos de acuerdo a los criterios que se indiquen. 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. 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	**Competencias / Resultados**	**Descripción**	**Calificación**
Prácticas a través de TIC	A2 A8 B2 B5 B6	Las prácticas de la materia consistirán en diferentes actividades relacionadas con el diseño e implementación de Redes Seguras. Se llevará a cabo una defensa de las prácticas para valorar el nivel de comprensión y el trabajo desarrollado por el alumno	45
Prueba objetiva	A8 B2 B4 B6 B8	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	45

Trabajos tutelados	B4 B6 B8	Los trabajos tutelados consistirán en la realización de tareas semanales de trabajo individual relacionadas con una temática propuesta por los profesores	10

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 y en las prácticas. En caso contrario, la nota máxima que se podrá obtener es de 4.5. PRIMERA OPORTUNIDAD En primera oportunidad esta materia se evaluará de forma continua, mediante la valoración del trabajo de prácticas y la realización de un trabajo tutelado. La evaluación de las prácticas de laboratorio se realizará mediante la defensa de cuatro ejercicios prácticos relacionados con los ejercicios de laboratorio (la planificación de las defensas se indicará en la presentación de la asignatura) y tendrá un peso total del 45% de la nota final. Será necesario obtener un mínimo de un 40% en cada ejercicio de defensa para poder superar la materia en esta primera oportunidad. El trabajo tutelado se centrará en una temática propuesta por los profesores y será realizado por los alumnos a lo largo de las primeras 10 semanas del cuatrimestre. Durante cada una de estas 10 semanas los profesores propondrán una tarea a desarrollar que los alumnos deberán abordar satisfactoriamente para obtener un 10% de la nota del trabajo tutelado. En caso de copia o plagio de alguna de estas tareas el alumno será calificado con un 0 en esta actividad. El 45% de la nota restante 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. SEGUNDA OPORTUNIDAD Los alumnos conservarán la nota del trabajo tutelado realizado durante el proceso de evaluación continua de la primera oportunidad. Podrán conservar la nota obtenida en prácticas o la prueba objetiva 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 se llevará a cabo mediante la defensa de un ejercicio único en laboratorio, a la finalización de la prueba objetiva de la segunda oportunidad. El 45% de la nota restante de la segunda 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. CONVOCATORIA EXTRAORDINARIA Los alumnos conservarán la nota del trabajo tutelado realizado en durante el proceso de evaluación continua de la primera oportunidad de la convocatoria inmediatamente anterior. Podrán conservar la nota obtenida en prácticas o la prueba objetiva de las oportunidades de la convocatoria inmediatamente anterior, siempre y cuando hayan obtenido una valoración igual o superior al 50% de su peso en la nota final. La evaluación de las prácticas en la segunda oportunidad se llevará a cabo mediante la defensa de un ejercicio único en laboratorio, a la finalización de la prueba objetiva de la convocatoria extraordinaria. El 45% de la nota restante 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. 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.

Fuentes de información	
Básica	- Anthony Bruno; Steve Jordan (2016). CCDA 200-310 Official Cert Guide, Fifth Edition. Chapter 12. Managing Security. Cisco Press - Omar Santos, John Sutppi (2015). CCNA Security 210-260 Official Cert Guide. Cisco Press

Complementária	- Marwan Al-shawi; André Laurent (2016). Designing for Cisco Network Service Architecture (ARCH) Foundation Learning Guide. Chapter 22. Designing Security Services and Infrastructure Protection. Cisco Press - Marwan Al-shawi; André Laurent (2016). Designing for Cisco Network Service Architecture (ARCH) Foundation Learning Guide. Chapter 23. Designing Firewall and IPS Solutions. Cisco Press - Marwan Al-shawi; André Laurent (2016). Designing for Cisco Network Service Architecture (ARCH) Foundation Learning Guide. Chapter 25. Network Access Control Solutions. Cisco Press - Kulbir Saini (2011). Squid Proxy Server 3.1 Beginner's Guide. Packt Publishing - Wendell Odom (2016). CCENT/CCNA ICND1 100-105 Official Certification Guide. Cisco Press - Wendell Odom (2019). CCNA Routing and Switching ICND2 Official Cert Guide. Cisco Press

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