UNIVERSIDADE DA CORUÑA

Guía Docente					
Datos Identificativos					2018/19
Asignatura (*)	Redes Seguras			Código	614530006
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Período	Curso		Tipo	Créditos
Mestrado Oficial	1º cuadrimestre	Primeiro		Obrigatoria	6
Idioma	CastelánGalego				
Modalidade docente	Presencial				
Prerrequisitos					
Departamento	ComputaciónTecnoloxías da Información e as Comunicacións				
Coordinación	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	www.munics.es				
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 VPN, 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 do título	
Código	Competencias do título
A2	CE2 - Coñecer en profundidade as técnicas de ciberataque e ciberdefensa
A4	CE4 - Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
A8	CE8 - Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
A12	CE12 - Coñecer o papel da ciberseguridade no deseño das novas industrias, así como as particularidades, restricciones e limitacións que teñen que acometerse para obter unha infraestructura industrial segura
B2	CB2 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
B4	CB4 - Que os estudantes saiban comunicar as súas conclusións ---e os coñecementos e razóns últimas que as sustentan--- a públicos especializados e non especializados de un modo claro e sen ambigüidades
B5	CB5 - Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en gran medida autodirixido ou autónomo
B6	CG1 - Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
B8	CG3 - Capacidade para o razonamiento crítico e a evaluación crítica de calquera sistema de protección da información, calquera sistema de seguridade da información, da seguridade das redes e/ou os sistemas de comunicacións
C4	CT4 - Valorar a importancia da seguridade da información no avance socioeconómico da sociedade

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias do título		
Comprenderán o papel dun firewall na estratexia de seguridade dun dispositivo final ou da rede á que protexe	AP2 AP8	BP2 BP6	
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	AP8 AP12	BP2 BP4 BP6 BP8	CP4

Coñecerán os diferentes tipos de filtrado de paquetes (con/sen estado) e os firewalls de nivel de aplicación, e saberán configuralos en diversas plataformas	AP2	BP6 BP8	
Poderán deseñar e describir, para un escenario/topoloxía concretos, configuracións alternativas para coloca-lo firewall dentro da rede corporativa (sistema fortificado, DMZ, tornalumes distribuído)	AP8	BP2 BP6 BP8	
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	AP2 AP8	BP6 BP8	
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	AP2 AP4	BP6	
Poderán explica-los principios sobre os que se constrúen as redes anónimas	AP2	BP4 BP5	CP4

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 1.4. Aproximacións para BYOD
2.- Fortificación dos Dispositivos de Rede	2.1. Arquitectura interna dos Dispositivos de Rede 2.2. Protección do Plano de datos 2.3. Protección do Plano de control 2.4. Protección do Plano de xestión
3. Firewalls	3.1. Filtrado de paquetes estático 3.2. Filtrado dinámico de paquetes 3.3. Filtrado en capa de aplicación 3.4. Firewalls baseados en zonas de seguridade 3.5. Next-Generation Firewalls 3.6. NAT/NATP
4. IDS/IPS	4.1. Sistemas baseados en rede 4.2. Sistemas baseados en equipo final
5. Proxies	5.1. Administración de proxies 5.2. Proxy inverso 5.3. Proxy transparente 5.4. Redes anónimas
6. Monitorización	6.1. Syslog 6.2. SNMP 6.3. Netflow 6.4. SIEM
7. Implantación de VPNs	7.1 VPNs baseadas en IPsec 7.2 VPNs baseadas en SSL 7.3 VPNs baseadas en MPLS

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Prácticas a través de TIC	A2 A8 B2 B5 B6	21	52.5	73.5

Proba obxectiva	A8 B2 B4 B6 B8	3	0	3
Traballos tutelados	B4 B6 B8	0.5	10	10.5
Sesión maxistral	A2 A4 A8 A12 B8 C4	21	42	63
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 conqueridas durante o desenvolvemento do curso..
Traballos tutelados	Proposta de traballos para a resolución individual e non presencial por parte dos alumnos. Estes traballos serán opcionais e permitirán que os estudantes interesados en facelos poidan afondar en aspectos do temario que lles interesen especialmente e que non se puideran tratar con detalle suficient durante as sesións maxistrais.
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 Traballos tutelados	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. Para a realización dos traballos tutelados os profesores proporcionarán as indicacións iniciais necesarias, bibliografía para consulta e realizarán un seguimento dos avances que o alumno vaia realizando para ofrecer as orientacións pertinentes en cada caso, de modo que se asegure a calidade dos traballos de acordo aos criterios que se indiquen. 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.

Avaliación			
Metodoloxías	**Competencias**	**Descrición**	**Cualificación**
Prácticas a través de TIC	A2 A8 B2 B5 B6	As prácticas da materia consistirán en diferentes actividades relacionadas co deseño e implementación de Redes Seguras. Levarase a cabo unha defensa das prácticas para valorar o nivel de comprensión e o traballo desenvolvido polo alumno	45
Proba obxectiva	A8 B2 B4 B6 B8	Ao final da exposición da materia, realizarase unha proba obxectiva tipo test sobre os contidos tratados, tanto nas sesións teóricas como nas prácticas	45

Traballos tutelados	B4 B6 B8	Os traballos tutelados serán opcionais e sobre algún tema a concertar entre os alumnos e os profesores	10

Observacións avaliación
Para supera-la materia, será preciso obter un mínimo dun 40% da nota total na proba obxectiva e nas prácticas. En caso contrario, a nota máxima que se poderá obter será de 4.5. ESTUDANTES CON MATRÍCULA A TEMPO PARCIAL OU CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA: Deberán poñerse en contacto cos profesores da asignatura para posibilitar a realización das tarefas fóra da organización habitual de materia.

Fontes de información	
Bibliografía básica	- Anthony Bruno; Steve Jordan (2016). CCDA 200-310 Official Cert Guide, Fifth Edition. Chapter 12. Managing Security. Cisco Press - Anthony Bruno; Steve Jordan (2016). CCDA 200-310 Official Cert Guide, Fifth Edition. Chapter 12. Managing Security. Chapter 13. Security Solutions. Cisco Press - Omar Santos, John Sutppi (2015). CCNA Security 210-260 Official Cert Guide. Cisco Press
Bibliografía complementaria	- 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

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