



| Guía Docente | | | | |
|-----------------------|---|--------------------|-------------------------------|----------|
| Datos Identificativos | | | | 2020/21 |
| Asignatura (*) | Redes Seguras | Código | 614530006 | |
| Titulación | Máster Universitario en Ciberseguridade | | | |
| Descritores | | | | |
| Ciclo | Período | Curso | Tipo | Créditos |
| Mestrado Oficial | 1º cuatrimestre | Primeiro | Obrigatoria | 6 |
| Idioma | CastelánGalego | | | |
| Modalidade docente | Presencial | | | |
| Prerrequisitos | | | | |
| Departamento | Ciencias da Computación e Tecnoloxías da InformaciónComputaciónTecnoloxías da Información e as Comunicaci3ns | | | |
| Coordinaci3n | Novoa De Manuel, Francisco Javier | Correo electr3nico | francisco.javier.novoa@udc.es | |
| Profesorado | Novoa De Manuel, Francisco Javier | Correo electr3nico | francisco.javier.novoa@udc.es | |
| Web | faitic.uvigo.es | | | |
| Descrici3n 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 seguridade 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 virtuais teñan unha importancia capital no proceso de aprendizaxe | | | |



| | |
|-----------------------------|--|
| Plan de continxencia | <p>Plan de continxencia A: confinamento total ou parcial de estudantes e/ou profesores</p> <ol style="list-style-type: none">1. Modificacións nos contidos: non hai2. Metodoloxías<ul style="list-style-type: none">*Metodoloxías docentes que se modifican- Sesión maxistral, impartida a través de videoconferencia- Prácticas a través de las TIC, impártese mediante o uso de simuladores e/ou acceso remoto ao equipamento da aula.- Proba obxectiva, a través de Faitic, Moodle ou outra ferramenta que proporcionen UVigo e/ou UDC.- Proba práctica, mantense usando simuladores, acceso remoto e ferramentas de videoconferencia3. Mecanismos de atención personalizada ao alumnado<ul style="list-style-type: none">- Moodle: sempre. Tódolos recursos docentes (diapositivas, enunciado da práctica, anuncios, software, etc.) están dispoñibles a través de Moodle.- Teams: semanalmente. As titorías aténdense por Teams nos horarios oficiais de cada profesor.- Correo electrónico: sempre. Para responder a calquera cuestión.4. Modificacións na avaliación: ningunha<ul style="list-style-type: none">*Observacións de avaliación:No caso de non poder realizarse presencialmente, levaranse a cabo:- Proba obxectiva: a través de Faitic e Campus Remoto ou Teams- Proba práctica: a través de simuladores e/ou mecanismos de acceso remoto.5. Modificacións da bibliografía ou webgrafía: ningunha <p>Plan de continxencia B: número de estudantes excede o aforo da aula</p> <ol style="list-style-type: none">1. Modificacións nos contidos: non hai2. Metodoloxías<ul style="list-style-type: none">*Metodoloxías docentes que se modifican- Sesión maxistral, estableceranse dous grupos que asistirán presencialmente semanas alternas. Artellarase unha solución de videoconferencia (Campus Remoto ou Teams) para acceder ás sesións remotamente.- Prácticas a través de las TIC, estableceranse dous grupos que asistirán presencialmente semanas alternas. Artellarase unha solución de acceso remoto ou simuladores para o grupo que non poida asistir presencialmente.- Proba obxectiva, habilitarase un aula con aforo suficiente- Proba práctica, estableceranse quendas para facer a proba.3. Mecanismos de atención personalizada ao alumnado<ul style="list-style-type: none">- Moodle: sempre. Tódolos recursos docentes (diapositivas, enunciado da práctica, anuncios, software, etc.) están dispoñibles a través de Moodle.- Teams: semanalmente. As titorías aténdense por Teams nos horarios oficiais de cada profesor.- Correo electrónico: sempre. Para responder a calquera cuestión.4. Modificacións na avaliación: ningunha<ul style="list-style-type: none">*Observacións de avaliación:No caso de non poder realizarse presencialmente, levaranse a cabo:- Proba obxectiva, habilitarase un aula con aforo suficiente- Proba práctica, estableceranse quendas para facer a proba. |
|-----------------------------|--|



5. Modificacións da bibliografía ou webgrafía: ningunha



| Competencias / Resultados do título | |
|-------------------------------------|---|
| Código | Competencias / Resultados 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, restricións e limitacións que teñen que acometerse para obter unha infraestrutura 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 máis 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 análise e síntesis. Ter capacidade para proxectar, modelar, calcular e deseñar 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 avaliación 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 / Resultados 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 detección de intrusións, os sensores habituais que se usan para a recopilación de información, e as técnicas de análise (detección de anomalías, versus detección 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 |



| | |
|--|--|
| 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. Introducción 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 | A2 A8 B2 B5 B6 | 21 | 60 | 81 |
| Proba obxectiva | A8 B2 B4 B6 B8 | 2 | 0 | 2 |
| Proba práctica | A8 B2 B6 | 2 | 0 | 2 |
| 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 | <p>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.</p> <p>Ademais das prácticas básicas que todos os alumnos terán que facer, proporanse prácticas adicionais que os alumnos interesados poderán realizar de forma opcional.</p> |
| 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. |



| | |
|------------------|--|
| 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 | <p>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.</p> <p>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.</p> |

Avaliación

| Metodoloxías | Competencias / Resultados | Descrición | Cualificación |
|---------------------------|---------------------------|---|---------------|
| Proba práctica | A8 B2 B6 | 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 |
| 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 memoria das prácticas para valorar o nivel de comprensión e o traballo desenvolvido polo alumno | 20 |
| 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 | 50 |

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 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

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 50% da nota restante 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.

SEGUNDA OPORTUNIDADE

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 45% da nota restante da segunda oportunidade poderase conseguir por medio da realización dunha proba obxectiva (examen), que poderá conter preguntas relacionadas cos conceptos desenvolvidos en clase de teoría, prácticas, tutoriais proporcionados e material bibliográfico básico.

CONVOCATORIA EXTRAORDINARIA

Os alumnos conservarán a nota do traballo titorizado realizado durante o proceso de avaliación continua da primeira oportunidade da convocatoria inmediatamente anterior. Poderán conserva-la nota obtida en prácticas ou na proba obxectiva da convocatoria inmediatamente anterior, 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 50% da nota restante poderá conseguirse por medio da realización dunha proba obxectiva (exame), que poderá conter preguntas relacionadas cos conceptos desenvolvidos en clase 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 | <ul style="list-style-type: none"> - 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 | <ul style="list-style-type: none"> - 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 Comunicacions/614530004

Observacións



(*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías