VNIVERSITAT DE VALÈNCIA

Guía Docente
43861 Seguridad en redes

FICHA IDENTIFICATIVA

Datos de la Asignatura

Código	43861
Nombre	Seguridad en redes
Ciclo	Máster
Créditos ECTS	5.0
Curso académico	2022 - 2023

Titulación(es)

Titulación	Centro	Curso	Periodo
2174 - Máster Universitario Ingeniería Telecomunicación	Escuela Técnica Superior de Ingeniería	2	Primer cuatrimestre

Materias

Titulación	Materia	Carácter
2174 - Máster Universitario Ingeniería Telecomunicación	15 - Seguridad en redes	Obligatoria

Coordinación

Nombre	Departamento
GARCIA PINEDA, MIGUEL	240 - Informática

RESUMEN

Esta asignatura se centra en el estudio, desde un punto de vista tanto teórico como práctico, de los distintos mecanismos y herramientas existentes en la actualidad para garantizar la seguridad de una intranet corporativa, tanto frente a ataques exteriores como interiores, tanto para la red cableada como para la red inalámbrica.

La asignatura prepara al alumno para certificaciones oficiales relacionadas con la seguridad que poseen una gran demanda profesional en el sector de las telecomunicaciones. La certificación abre las puertas a un sector estratégico como es Internet en el mundo empresarial y de negocios.

La asignatura se ha diseñado siguiendo una metodología adaptada al nuevo Espacio Europeo de Educación Superior (EEES), y pretende centrar el aprendizaje en el estudiante. Este método mejora la implicación del estudiante y ayuda a su evaluación de forma continua, reforzando y complementando los conocimientos adquiridos en clases magistrales.

CONOCIMIENTOS PREVIOS

Relación con otras asignaturas de la misma titulación

No se han especificado restricciones de matrícula con otras asignaturas del plan de estudios.

Otros tipos de requisitos

Ser capaz de manejar los comandos de red de Linux y de Windows, así como entender los fundamentos de IP, TCP/IP, UDP/IP, DHCP, puntos de acceso y routers necesarios para configurar una pequeña LAN.

COMPETENCIAS (RD 1393/2007) // RESULTADOS DEL APRENDIZAJE (RD 822/2021)

2174 - Máster Universitario Ingeniería Telecomunicación

- Capacidad de análisis y pensamiento crítico, para investigar con independencia y autocrítica, y de buscar y utilizar información para documentar ideas.
- Que los/las 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.
- Que los/las estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
- Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
- Ser capaces de acceder a herramientas de información en otras áreas del conocimiento y utilizarlas apropiadamente.
- Ser capaces de valorar la necesidad de completar su formación científica, histórica, en lenguas, en informática, en literatura, en ética, social y humana en general, asistiendo a conferencias o cursos y/o realizando actividades complementarias, autoevaluando la aportación que la realización de estas actividades supone para su formación integral.
- Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.
- Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

- Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de Internet de nueva generación, los modelos de componentes, software intermediario y servicios.

RESULTADOS DE APRENDIZAJE (RD 1393/2007) // SIN CONTENIDO (RD 822/2021)

Una vez finalizado el curso, el alumno habrá adquirido los conocimientos para:

- Describir los conceptos comunes de seguridad de red
- Asegurar una infraestructura de routing y switching
- Desarrollar servicios de autenticación básica, autorización y auditoría
- Desarrollar servicios básicos de firewall
- Despliegue básico de sitio a sitio y los servicios de acceso remoto VPN
- Describir el uso de los servicios de seguridad más avanzadas, tales como la protección de intrusos, seguridad de contenido y gestión de identidades

DESCRIPCIÓN DE CONTENIDOS

1. Amenazas de seguridad en las redes

1.1. Principios fundamentales de las redes seguras
1.2. Gusanos, virus y troyanos
1.3. Metodologías de ataque

2. Asegurar los dispositivos de red

2.1. Asegurar el acceso y los ficheros de los dispositivos
2.2. CLI basada en roles
2.3. Dispositivos de monitorización
2.4. Utilización de características automatizadas

3. Autenticación, autorización y auditoria

3.1. Propósito de AAA
3.2. Configuración local de AAA
3.3. Configuración de AAA basada en servidor

4. Implementación de tecnologías de cortafuegos

4.1. Listas de control de acceso
4.2. Tecnologías de cortafuegos
4.3. Control de acceso basado en contexto
4.4. Políticas de cortafuegos

5. Implementación de la prevención de la intrusión

5.1. Tecnologías IPS
5.2. Implementación de IPS

6. Asegurando la red de área local

6.1. Consideraciones finales de seguridad
6.2. Consideraciones de seguridad de capa 2
6.3. Wireless, VoIP y consideraciones de seguridad SAN
6.4. Configuración de la seguridad del switch
6.5. SPAN y RSPAN

7. Criptografía

7.1. Servicios criptográficos
7.2. Resúmenes, firmas digitales y autentificación
7.3. Encriptación simétrica y asimétrica

8. Implementación de las redes privadas virtuales

8.1. VPNs
8.2. Componentes y operaciones de las VPNs IPSEC
8.3. Implementación de VPNs site-to-site.
8.4. Implementación de VPNs de acceso remoto
8.5. Implementación de SSLVPNs

9. Gestionar una red segura

9.1. Ciclo de vida de una red segura
9.2. Red de autodefensa
9.3. Construcción de una política integral de seguridad

VOLUMEN DE TRABAJO

ACTIVIDAD	Horas	% Presencial
Clases de teoría	21,00	100
Prácticas en aula	18,00	100
Prácticas en laboratorio	9,00	100
Tutorías regladas	2,00	100
Elaboración de trabajos individuales	30,00	0
Estudio y trabajo autónomo	30,00	0
Preparación de actividades de evaluación	5,00	0
Preparación de clases de teoría	5,00	0
Preparación de clases prácticas y de problemas	5,00	0
TOTAL	**125,00**	

METODOLOGÍA DOCENTE

Las actividades formativas se desarrollarán de acuerdo con la siguiente distribución:

El 40% de las horas de los créditos ECTS (1 crédito son 25 horas) se destinarán a las siguientes

actividades presenciales:

MD1. Actividades teóricas.

- Descripción: En las clases teóricas se desarrollarán los temas proporcionando una visión global e integradora, analizando con mayor detalle los aspectos clave y de mayor complejidad, fomentando, en todo momento, la participación del/la estudiante.

MD2. Actividades prácticas.

- Descripción: Complementan las actividades teóricas con el objetivo de aplicar los conceptos básicos y ampliarlos con el conocimiento y la experiencia que vayan adquiriendo durante la realización de los trabajos propuestos. Comprenden los siguientes tipos de actividades presenciales: Clases de problemas y cuestiones en aula; sesiones de discusión y resolución de problemas y ejercicios previamente trabajados por los estudiantes; prácticas de laboratorio; presentaciones orales; conferencias; tutorías programadas (individualizadas o en grupo)

Evaluación.

- Descripción: Realización de cuestionarios individuales de evaluación en el aula con la presencia del

- profesorado.

El 60% de las horas de los ECTS (25 horas por ECTS) se dedicarán a las siguientes actividades no presenciales:

Trabajo personal del/la estudiante.

- Descripción: Realización (fuera del aula) de trabajos monográficos, búsqueda bibliográfica dirigida, cuestiones y problemas, así como la preparación de clases y exámenes (estudio). Esta tarea se realizará de manera individual e intenta potenciar el trabajo autónomo.

Se utilizará la plataforma de e-learning (Aula Virtual) de la Universitat de València como soporte de comunicación con los estudiantes. A través de ella se tendrá acceso al material didáctico utilizado en clase, así como los problemas y ejercicios a resolver.

EVALUACIÓN

La asignatura se evaluará de la siguiente manera en evaluación continua:

1. SE1.-Parte teórica examen final (35%). Nota mínima 5. Como alternativa en evaluación continua se realizarán exámenes escritos promediados.
2. SE2.- Parte laboratorio (50%)
    1. Asistencia, preparación y realización de la práctica evaluada en el mismo laboratorio (10%).Las prácticas sonn obligatorias y no recuperables.
    2. Examen escrito de configuración con comandos (40%) . Nota mínima 5. Como alternativa se realizarán exámenes prácticos promediados.
3. SE3.- Ejercicios propuestos por el profesor (15%).

En segunda convocatoria, se aplicará lo mismo que en la primera.

En cualquier caso, el sistema de evaluación se regirá por lo establecido en el Reglamento de Evaluación y Calificación de la Universidad de Valencia para Grados y Másters (http://www.uv.es/graus/normatives/2017_108_Reglament_avaluacio_qualificacio.pdf).

REFERENCIAS

Básicas

- Stallings, Network Security Essential (5th edition), 2013
- Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg. Network Security: The Complete Reference
- Cisco Press: Designing Network Security
- Omar Santos, John Stuppi. CCNA Security 210-260 Official Cert Guide. Cisco Press, 2015