PROYECTO DOCENTE ASIGNATURA "REDES INALÁMBRICAS Y SEGURIDAD EN REDES"

DATOS BÁSICOS DE LA ASIGNATURA

Titulación:
MASTER EN INGENIERIA DE COMPUTADORES Y REDES

Asignatura:
REDES INALÁMBRICAS Y SEGURIDAD EN REDES

Código:

Curso:
0

Año del plan de estudio:
2010

Tipo:
OPTATIVA

Período de impartición:
2

Ciclo:
2

Departamento:
TECNOLOGÍA ELECTRÓNICA

Área:
TECNOLOGÍA ELECTRÓNICA

Centro:
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

Horas totales (ECTS):
150
Horas presenciales (ECTS):
30
Horas no presenciales (ECTS):
120
Créditos totales (ECTS):
6

PROFESORADO

Dr. Alejandro Carrasco Muñoz (COORDINADOR)
Dr. Jorge Ropero Rodríguez

OBJETIVOS Y COMPETENCIAS

Objetivos docentes específicos

El mundo de la informática evoluciona cada día más rápido. Un ejemplo de este espectacular avance podemos encontrarlo en las tecnologías inalámbricas (WLAN). Las WLAN proporcionan

todos los beneficios que facilitan las redes de área local tradicionales (LAN), pero sin las limitaciones que provocan los cables, lo que redunda en una mayor flexibilidad, movilidad y escalabilidad para el usuario.

Igualmente la utilización de servicios informáticos en todas las tareas cotidianas de nuestra vida es cada vez mayor. Con esta gran dependencia es normal que también nos preocupe la seguridad de todos estos servicios. En esta gran variedad de servicios y utilidades que nos ofrecen las redes es donde los hackers sacan su mayor partido y aprovechan los más mínimos fallos de seguridad para cometer sus actos delictivos.

Esta asignatura persigue dos objetivos principales:

Por una parte, dar a conocer al alumno la tecnología inalámbrica, centrándonos en el estándar 802.11, así como sus usos y aplicaciones, diseñar redes y estudiar las tecnologías inalámbricas emergentes.

Por otro lado proporcionar los fundamentos de la seguridad en redes, obtener una amplia visión de las amenazas y riesgos a los que están sometidos los servidores; y cómo los futuros administradores y responsables de seguridad deberemos ser capaces a su vez de implantar las medidas oportunas para minimizar los riesgos en lo que a seguridad informática se refiere. Para ello estudiaremos las técnicas de intrusión, monitorización y administración de los dispositivos de seguridad.

Competencias

Generales

G01. Comprensión sistemática del campo de la Informática Industrial, así como el dominio de las habilidades y métodos de investigación relacionados con dicho campo. Esta competencia incluye las capacidades de aplicar los conocimientos avanzados a la práctica profesional, aprender y trabajar de forma autónoma y en equipo, adaptarse a nuevas situaciones, generar nuevas ideas (creatividad), iniciarse en el liderazgo y la gestión de proyectos de investigación o profesionales en este campo, y adquirir iniciativa y espíritu emprendedor e inquietud por el compromiso ético, la calidad y el éxito.

G02. Capacidad de concebir, diseñar, poner en práctica y adoptar un proceso sustancial de investigación con seriedad académica. Esta competencia incluye las capacidades de análisis y síntesis, de organizar y planificar, de resolver problemas, de trabajar en equipo y de tomar decisiones.

G04. Análisis crítico, evaluación y síntesis de ideas nuevas y complejas. Esta competencia incluye las capacidades de búsqueda y selección de las aportaciones más significativas en las líneas científico-técnicas asociadas a esas ideas.

G07. Capacidad para la integración de tecnologías, aplicaciones, servicios y sistemas propios de la Ingeniería Informática, con carácter generalista, y en contextos más amplios y multidisciplinares.

Específicas

E01. Capacidad para modelar, diseñar, definir la arquitectura, implantar, gestionar, operar, administrar y mantener aplicaciones, redes y sistemas.

E02. Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet,

las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.

E03. Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos en ingeniería de computadores y redes.

E04. Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido, conforme a la legislación y normativa vigentes.

E05. Capacidad para analizar las necesidades de información que se plantean en un entorno de ingeniería de computadores y redes y llevar a cabo su proceso de construcción.

E14. Conocer y aplicar tecnologías, componentes y herramientas de modelado, diseño, simulación y desarrollo de computadores, circuitos integrados, sistemas empotrados y redes, y de aplicaciones específicas.

CONTENIDOS DE LA ASIGNATURA

Relación sucinta de los contenidos (bloques temáticos en su caso)

Bloque 1: Presentación de la Asignatura

Tema 1: Presentación de la asignatura

Bloque 2: Redes Inalámbricas

Tema 1: Introducción a las LAN inalámbricas

Tema 2: IEEE 802.11. Tecnología inalámbrica

Tema 3: Topologías inalámbricas

Tema 4: Seguridad

Tema 5: Aplicaciones, diseño y preparación de la planificación (Site Survey) de una red inalámbrica.

Tema 6: Tecnologías emergentes

Bloque 3: Seguridad en Redes

Tema 1: Introducción a la seguridad informática

Tema 2: Peligros, amenazas y defensas

Tema 3: Seguridad perimetral

Tema 4: Control - Firewalls

Tema 5: Monitorización – IDS´s

Tema 6: Sistemas de decepción. Honeypots

Relación detallada y ordenación temporal de los contenidos

Bloque 1: Presentación de la Asignatura

Tema 1: Presentación de la asignatura

1. Profesores, datos de contacto, responsabilidades.
2. Objetivos de la asignatura.
3. Justificación en el contexto del programa de estudios.
4. Competencias desarrolladas.
5. Metodología docente.
6. Planificación del curso.

Bloque 2: Redes Inalámbricas

Tema 1: Introducción a las LAN inalámbricas.

1. Introducción.
2. Motivaciones.
3. Espectro inalámbrico.

Tema 2: IEEE 802.11. Tecnología inalámbrica

1. Estándar 802.11
2. Capas física y de enlace de datos.
3. Tecnología inalámbrica.
4. Usos y aplicaciones.
5. Tecnología y matemática en la comunicación por radio.

Tema 3: Topologías inalámbricas.

1. Implementación práctica.
2. Tecnología y componentes.
3. Topología, canales y aplicaciones.
4. Puntos de acceso (AP). Puertos y servicios.
5. Puentes.
6. Antenas.

Tema 4: Seguridad

1. Seguridad en redes inalámbricas.

Tema 5: Aplicaciones, diseño y preparación de la planificación (Site Survey) de una red inalámbrica.

1. Soluciones WLAN.
2. Pruebas.
3. Uso de la documentación.
4. Planificación (Site survey).
5. Topología y estructura física.
6. Instalación y montaje: áreas de cobertura y topología celular.
7. Solución de problemas. Herramientas.

Tema 6: Tecnologías emergentes.

1. Aplicaciones.
2. Voz sobre IP (VoIP).
3. Bluetooth.
4. WiMax.
5. Mobile IP.

Bloque 3: Seguridad en Redes

Tema 1: Introducción a la seguridad informática

1. ¿Qué es la seguridad informática?
2. Gestión de la seguridad: políticas, la rueda de la seguridad, análisis de riesgos.
3. La seguridad en Redes.

Tema 2: Peligros, amenazas y defensas

1. Peligros y modos de ataque
2. Atacantes
3. Malware
4. Métodos de defensas
5. Protocolos de interés

Tema 3: Seguridad perimetral
1. Introducción
2. Elementos que componen la seguridad perimetral
3. Buenas prácticas
4. Objetivos

Tema 4: Dispositivos de protección perimetral. CONTROL - Firewalls
1. Elementos que componen un firewall
2. Soft vs Hard
3. Características de diseño
4. Topologías del firewall

Tema 5: Dispositivos de protección perimetral. MONITORIZACIÓN – IDS´s
1. Clasificación de los IDS
2. Requisitos de un IDS
3. Arquitectura de un IDS
4. Topologías de un IDS
5. Productos

Tema 6: Sistemas de decepción. Honeypots
1. Introducción
2. Clasificación de los honeypots
3. WiFi – Honeypots
4. HoneyNets

ACTIVIDADES FORMATIVAS

Relación de actividades formativas del primer semestre

Clase teóricas

Horas presenciales:
12
Horas no presenciales:
36
Competencias que desarrolla:
G01, G02, G07 y todas las específicas.

Metodología de enseñanza-aprendizaje:

Con carácter general, el desarrollo de cada tema se centra en una o varias clases teóricas en las que el profesor expone y reflexiona sobre los contenidos teóricos del mismo. De manera intercalada, el profesor estimulará el debate sobre decisiones de diseño y planteará ejercicios o casos prácticos relativos al tema en cuestión.

Prácticas de Laboratorio

Horas presenciales:
12
Horas no presenciales:
24
Competencias que desarrolla:
G01, G02 y todas las específicas.

Metodología de enseñanza-aprendizaje:
Las prácticas de laboratorio reforzarán los conocimientos adquiridos en clases teóricas, por lo que es imprescindible que el alumno previamente haya trabajado y comprendido la materia que se desarrollará en la sesión práctica.

Exámenes

Horas presenciales:
2
Horas no presenciales:

10

Tipo de examen:

Test en papel y lápiz o a través de la plataforma WebCT.

Actividades académicas dirigidas sin presencia del profesor

Horas presenciales:

4

Horas no presenciales:

50

Competencias que desarrolla:

Todas las generales y específicas.

Metodología de enseñanza-aprendizaje:

Los alumnos deberán desarrollar un trabajo individual o en grupo basado en casos de estudio y posteriormente realizar una defensa oral del mismo.

BIBLIOGRAFÍA Y OTROS RECURSOS DOCENTES

Bibliografía general

Título Fundamentos de redes inalámbricas
Autor Cisco Networking Academy
Edición 1
Editor Cisco Press, 2008
ISBN 84-8322-287-6

Título 802.11 Wireless Networks: The Definitive Guide, Second Edition
Autor Matthew Gast
Edición 1
Editor O'Reilly Media, 2005
ISBN 978-0-596-10052-0

Título 802.11 Security
Autor Bruce Potter, Bob Fleck
Edición 1
Editor O'Reilly Media, 2008
ISBN 978-0-596-00290-9

Título Building Wireless Community Networks
Autor Rob Flickenger
Edición 2
Editor O'Reilly Media, 2003
ISBN 978-0-596-00502-3

Título Fundamentos de Seguridad en Redes
Autor Cisco Networking Academy
Edición 1
Editor Cisco Press, 2005
ISBN 9788420545400

Título Fundamentos de seguridad en redes. Aplicaciones y Estándares
Autor William Stalling
Edición 2
Editor Pearson Prentice Hall, 2004
ISBN 84-205-4002-1

Título Seguridad de Redes
Autor Chris McNab
Edición 2
Editor Anaya Multimedia, 2008
ISBN 978-84-415-2402-6

Título La biblia del Hacker 2009
Autor Míguez Pérez, Carlos y Matas García, Abel Mariano
Edición 1
Editor Anaya Multimedia, 2009
ISBN 9788441524842

Título	Cryptography and network security : principles and practices
Autor	Stallings, William
Edición	4
Editor	Pearson Prentice Hall, 2006
ISBN	0131873164

SISTEMAS Y CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN
Sistema de evaluación

Actividades de evaluación continua

Las actividades de evaluación continua pueden comprender algunas de las siguientes actividades:

1. Asistencia y participación en clase. Se exigirá un mínimo del 80%.
2. Pruebas teórico/prácticas.
3. Ensayo, trabajo individual o en grupo.
4. Exposiciones o demostraciones.
5. Informes de prácticas.

Exámenes finales

Exámenes que podrán coincidirán con las fechas determinadas para cada una de las convocatorias.

Criterios de calificación

La nota final de la asignatura procurará reflejar, de manera objetiva, los conocimientos adquiridos por el alumno a lo largo del curso. Para ello, se evaluará de forma independiente los conocimientos teóricos adquiridos por el alumno, y su experiencia práctica.

a) Evaluación por curso:

La nota final por curso se obtendrá de la siguiente forma:

Nota Final (NF) = PTP x 0,2 + IP x 0,3 + TF x0 ,5

Siendo:
PTP.- Nota media de las pruebas teorico/prácticas y resolución de casos de estudio.
IP.- Nota media de los informes de las prácticas.
TF.- Nota del trabajo final.

La asignatura se considerará aprobada por curso cuando NF sea mayor o igual a 5

A continuación se describe cada una de las partes que serán evaluadas por curso:
1.- Pruebas teorico/prácticas (PTP)
La teoría de cada uno de los temas será evaluada de manera individual mediante un cuestionario tipo test de corta duración que se realizará en clase o mediante la resolución de casos prácticos.
2.- Informes Prácticas (IP)
Para cada práctica de laboratorio realizada habrá que entregar un informe. La media obtenida de todos los informes de las práctica que se realicen formará la nota IP.
3.- Trabajo Final (TF)

Se realizará un trabajo final basado en un caso de estudio, individual o en grupo, sobre la temática de la asignatura. Este caso estudio será evaluado mediante la entrega de una memoria y la defensa de la misma.

b) Evaluación en Convocatoria oficial:

La nota final por curso se obtendrá de la siguiente forma:

Nota Final (NF) = ET x 0,35 + EP x 0,35 + TF x 0,3

Siendo:
ET.- Nota examen de teoría.
EP.- Nota examen práctico.
TF.- Nota del trabajo final.
La asignatura se considerará aprobada cuando NF sea mayor o igual a 5.

CALENDARIO DE EXÁMENES

1 ª Convocatoria
CENTRO: Escuela Técnica Superior de Ingeniería Informática
Fecha:
Hora:
Aula:

2 ª Convocatoria
CENTRO: Escuela Técnica Superior de Ingeniería Informática
Fecha:
Hora:
Aula:

3 ª Convocatoria
CENTRO: Escuela Técnica Superior de Ingeniería Informática
Fecha:
Hora:
Aula:

Anotaciones relativas al calendario de exámenes

TRIBUNALES ESPECÍFICOS DE EVALUACIÓN Y APELACIÓN

Presidente:
Vocal:
Secretario:
Primer suplente:
Segundo suplente:
Tercer suplente:

ANEXO 1:

HORARIOS DE LOS GRUPOS NO PRINCIPALES DE LA ASIGNATURA Y DEL GRUPO DEL PROYECTO DOCENTE
GRUPO
Calendario del grupo