Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación
30353 - Seguridad en redes y servicios

Guía docente para el curso 2012 - 2013

Curso: 3, Semestre: 2, Créditos: 6.0

Información básica

Profesores

- **Álvaro Alesanco Iglesias** alesanco@unizar.es
- **Miguel Eguizabal Alonso** meguizab@unizar.es
- **José Luis Salazar Riaño** jsalazar@unizar.es

Recomendaciones para cursar esta asignatura

Para seguir con normalidad esta asignatura es especialmente recomendable que el alumno que quiera cursarla haya cursado previamente, aparte de las asignaturas básicas de primero, las asignaturas de *Fundamentos de Redes, Tecnologías de interconexión de redes* y *Comunicaciones digitales*.

Para el óptimo aprovechamiento de la asignatura se recomienda al alumno la asistencia activa a clase (tanto de teoría como de problemas). Del mismo modo se recomienda al alumno el aprovechamiento y respeto de los horarios de tutorías del profesorado para la resolución de posibles dudas de la asignatura y un correcto seguimiento de la misma.

Actividades y fechas clave de la asignatura

La asignatura consta de un total de 6 créditos ECTS. Las actividades se dividen en clases teóricas, resolución de problemas o casos prácticos en clase y prácticas de laboratorio. Las actividades tienen como objetivo facilitar la asimilación de los conceptos teóricos complementándolos con los prácticos, de forma que se adquieran los conocimientos y las habilidades básicas relacionadas con las competencias previstas en la asignatura.

Las fechas de inicio y finalización del curso y las horas concretas de impartición de la asignatura así como las fechas de realización de las prácticas de laboratorio e impartición de seminarios se harán públicas atendiendo a los horarios fijados por la Escuela.

Inicio

Resultados de aprendizaje que definen la asignatura

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados...

1:

R1 Sabe clasificar los diferentes operadores criptográficos mediante diferentes métricas de complejidad, seguridad, eficacia, eficiencia, versatilidad, etc. Conoce la complejidad de los problemas computacionales que sustentan a dichos operadores criptográficos.

2:
R2 Sabe caracterizar los protocolos criptográficos básicos: confidencialidad, autenticidad e integridad. Es capaz de aplicarlos a diferentes aplicaciones distribuidas.

3:
R3 Identifica las prácticas básicas para securizar sistemas operativos, así como la importancia de los sistemas redundantes.

4:
R4 Conoce las vulnerabilidades del protocolo TCP/IP y los protocolos de nivel de aplicación y sabe utilizar herramientas para paliar estas vulnerabilidades.

5:
R5 Conoce y es capaz de proponer un esquema seguro de red en una Intranet.

6:
R6 Conoce y aplica la gestión de seguridad a través de un Sistema de Gestión de la Seguridad de la Información (SGSI).

7:
R7. Desarrolla la habilidad de trabajar en equipo para realizar los diseños y configuraciones consideradas, repartiendo la carga de trabajo para afrontar problemas complejos, intercambiando información entre distintos grupos, de manera coordinada y organizada.

8:
R8. Plantea correctamente el problema a partir del enunciado propuesto e identifica las opciones para su resolución. Aplica el método de resolución adecuado e identifica la corrección de la solución.

Introducción

Breve presentación de la asignatura

La asignatura presenta la seguridad de redes y servicios desde el concepto moderno, ampliamente admitido en la actualidad por los expertos, de que la seguridad es un proceso más que una cualidad o un sistema. Por ello, abordamos la mayoría de los aspectos involucrados en la misma. Empezamos tratando la información de forma segura, analizando los operadores criptográficos como una herramienta a utilizar en el diseño de protocolos de servicios de seguridad que abarcan desde la confidencialidad más básica hasta la posibilidad de juegos de azar en red. Después de plantear la protección de los equipos y los protocolos de comunicación como agentes implicados en el proceso comunicativo, ya podremos pensar en el diseño de una red segura, ya sea general o ad-hoc para un fin concreto. Acabaremos recalcando la importancia de asegurar todos los detalles del **proceso** y plasmarlo en un plan integral de seguridad, puesto que un punto débil en la cadena implica la debilidad del conjunto,

---

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

El objetivo principal de la asignatura es ofrecer al alumno un perspectiva de trabajo realista en redes y servicios de comunicaciones, lugar donde la seguridad juega un papel central y no puede ser dejada de lado so pena de incurrir en resultados desastrosos e incluso en delitos penales. Para ello se presentan, primero, las herramientas criptográficas actuales capaces de ofrecer los 3 pilares básicos de la seguridad: confidencialidad, integridad y autenticidad de origen. Como segundo paso, se muestra cómo los protocolos de comunicaciones de la pila TCP/IP han de utilizar esas herramientas para ofrecer a los usuarios esos 3 requerimientos básicos. En un tercer paso, se exponen los peligros más relevantes a los que se

enfrentan los servicios de comunicaciones y cómo se pueden afrontar, para acabar, en un cuarto paso, con el objetivo de que el alumno aprenda la manera de juntar todas estas piezas en un marco de gestión común y poder así securizar un sistema de manera correcta.

Contexto y sentido de la asignatura en la titulación

La asignatura de *Seguridad en Redes y Servicios* se imparte en el tercer curso de la titulación, más concretamente en el semestre de primavera y tiene una carga de trabajo de 6 ECTS. La asignatura forma parte de la materia denominada Diseño de servicios telemáticos que cubre competencias obligatorias dentro de la titulación del grado en Ingeniería de Tecnologías y Servicios de Telecomunicación en la tecnología específica de Telemática.

Los resultados de aprendizaje de esta asignatura servirán de complemento a las asignaturas de Redes de Acceso, Redes de Transporte y Diseño y Evaluación de Redes que forman parte de la materia Arquitectura de redes y servicios, proporcionando al alumno la visión global que éste necesita sobre la seguridad en las redes de telecomunicación, aspecto fundamental para el funcionamiento correcto de cualquier red.

Al superar la asignatura, el estudiante será más competente para...

1:
Concebir, diseñar y desarrollar proyectos de Ingeniería (C1)

2:
Planificar, presupuestar, organizar, dirigir y controlar tareas, personas y recursos (C2)

3:
Combinar los conocimientos generalistas y los especializados de Ingeniería para generar propuestas innovadoras y competitivas en la actividad profesional (C3)

4:
Resolver problemas y tomar decisiones con iniciativa, creatividad y razonamiento crítico (C4)

5:
Comunicar y transmitir conocimientos, habilidades y destrezas en castellano (C5)

6:
Usar las técnicas, habilidades y herramientas de la Ingeniería necesarias para la práctica de la misma (C6).

7:
La gestión de la información, manejo y aplicación de las especificaciones técnicas y la legislación necesarias para la práctica de la Ingeniería (C9)

8:
Aprender de forma continuada y desarrollar estrategias de aprendizaje autónomo (C10)

9:
Aplicar las tecnologías de la información y las comunicaciones en la Ingeniería (C11)

10:
Construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos (CT1)

11:
Aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos. (CT2)

12:
Seguir el progreso tecnológico de transmisión, conmutación y proceso para mejorar las redes y servicios telemáticos. (CT5)

13: Diseñar arquitecturas de redes y servicios telemáticos (CT6)

14:
La programación de servicios y aplicaciones telemáticas, en red y distribuidas (CT7)

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

Aunque la asignatura la podemos calificar como útil para cualquier itinerario de la titulación, resulta imprescindible dentro de la materia en la que se ubica, ya que no se puede entender un servicio telemático sin una capa mínima de seguridad. También resulta de gran interés dentro de la otra materia dominante en el itinerario como es la *Arquitectura de redes y servicios*, para proveer de seguridad a dichas redes. La asignatura permite al alumno conocer y ser capaz de diseñar tanto un sistema de comunicaciones seguro a través de una red, como suministrar seguridad a un servicio en fase de diseño o existente ya.

Evaluación

Actividades de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluacion

1:
El alumno dispondrá de una prueba global en cada una de las convocatorias establecidas a lo largo del curso. Las fechas y horarios de las pruebas vendrán determinadas por la Escuela. La calificación de dicha prueba se obtendrá de la siguiente forma:

E1: Examen final (100%). Puntuación de 0 a 10 puntos. Consta de dos partes:

E1A: Examen de contenidos teórico/prácticos (80%). Puntuación de 0 a 10 puntos. Se trata de un examen escrito. Mediante esta prueba se evalúan los resultados de aprendizaje desde R1 a R8. En consecuencia, el examen incluye tanto preguntas teóricas como preguntas que implican la resolución de problemas, con resultados numéricos concretos.

Para superar la asignatura es necesaria una puntuación mínima de 4,5 puntos sobre 10 en el Examen de Contenidos Teórico/Prácticos.

E1B: Prueba final de prácticas de laboratorio (20%). Puntuación de 0 a 10 puntos. Sólo deberá ser realizada por los estudiantes que no hayan superado las prácticas durante el periodo docente. Consiste en la resolución de un ejercicio práctico en el laboratorio que será evaluado oralmente y mediante un cuestionario escrito. Este ejercicio podrá incluir contenidos de todas las prácticas realizadas durante el periodo docente, sin excluir aspectos específicamente relacionados con el manejo de las herramientas utilizadas en las mismas. La prueba se realizará en el laboratorio el mismo día en el que se realicé el examen de contenidos teórico/práctico, si bien, dado el carácter individualizado de la evaluación, podría ser necesario programar estas pruebas en días diferentes, lo que será notificado a los estudiantes afectados con suficiente antelación. En cualquier caso, un alumno que tiene liberada esta parte, siempre puede optar por realizar la prueba final. En ese caso, la calificación obtenida será la de la prueba final.

Para superar la asignatura es necesaria una puntuación mínima de 4,5 puntos sobre 10 en la Prueba final de prácticas de laboratorio.

E2: Pruebas intermedias de evaluación

E2B: Prácticas de laboratorio (20%): Puntuación de 0 a 10 puntos. Se recomienda encarecidamente a los alumnos matriculados la realización de las prácticas de laboratorio a lo largo del curso. La evaluación de las prácticas de laboratorio, en las sesiones programadas durante el curso, se realizará, para los alumnos que asistan a todas ellas, mediante la presentación de estudios o trabajos previos cuando estos sean necesarios para el desarrollo de la práctica, el informe de seguimiento de la misma y la resolución de una serie de cuestiones al finalizar la práctica (unidad completa de una o más sesiones). Estas pruebas tienen por objeto

evaluar todas las competencias de la asignatura, con especial énfasis en las competencias C4, C6, CT2, CT5 y CT6. La calificación de estas pruebas representará el 20% de la nota final. La obtención de una calificación igual o superior a 4,5 puntos eximirá al alumno de realizar la prueba final práctica en el laboratorio. Los alumnos que no asistan a las prácticas deberán realizar la prueba final de prácticas de laboratorio de acuerdo con el procedimiento descrito en E1B.

En resumen:

La nota final se calculará mediante la siguiente expresión:

0,8´E1A+0,2´EB siempre que se cumplan las tres condiciones siguientes:

(0,8´E1A+0,2´EB) ³5 y E1A³4,5 EB³4,5

Donde

EB corresponde a la nota de las prácticas de laboratorio obtenida bien mediante la asistencia a las sesiones programadas y la evaluación continua (E2B) o bien mediante la prueba final de prácticas de laboratorio (E1B) de acuerdo a los procedimientos descritos anteriormente. Así:

EB=E1B si realiza la prueba final de laboratorio.

EB=E2B si NO realiza la prueba final de laboratorio.

Si no se cumplen las condiciones anteriores, en la nota final figurará suspenso.

Las notas de E2B se mantendrán para su cómputo en la siguiente convocatoria del mismo año académico. No se guardarán las notas de la prueba final de la primera convocatoria para segunda convocatoria.

Actividades y recursos

Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

Las metodologías de enseñanza-aprendizaje que se realizarán para conseguir los resultados de aprendizaje propuestos son las siguientes:

M1: Clase magistral participativa (30 horas). Exposición por parte del profesor de los principales contenidos de la asignatura, combinada con la participación activa del alumnado. Esta actividad se realizará en el aula de forma presencial. Esta metodología, apoyada con el estudio individual del alumno (M14) está diseñada para proporcionar a los alumnos los fundamentos teóricos del contenido de la asignatura.

M8: Prácticas de aula (15 horas). Resolución de problemas y casos prácticos propuestos por el profesor, con posibilidad de exposición de los mismos por parte de los alumnos de forma individual o en grupos autorizada por el profesor. Esta actividad se realizará en el aula de forma presencial, y puede exigir trabajo de preparación por parte de los alumnos (M13).

M9: Prácticas de laboratorio (15 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración cada semana. Esta actividad se realizará de forma presencial en el Laboratorio de Prácticas 2.03 (Laboratorio de Telemática), del edificio Ada Byron. El trabajo a desarrollar se realizara en pequeños grupos.

M10: Tutoría. Horario de atención personalizada al alumno con el objetivo de revisar y discutir los materiales y temas presentados en las clases tanto teóricas como prácticas.

M11: Evaluación (4 horas). Conjunto de pruebas escritas teórico-prácticas y presentación de informes o trabajos utilizados en la evaluación del progreso del estudiante. El detalle se encuentra en la sección correspondiente a las actividades de evaluación

Actividades de aprendizaje programadas (Se incluye programa)

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades...

1:

La distribución en unidades temáticas de la teoría de la asignatura será la siguiente:

TEMA 1. CRIPTOLOGÍA.

1.1. Introducción a la criptografía.

1.1.1. Criptografía clásica.

1.1.2. Criptografía moderna.

1.2. Criptografía simétrica

1.2.1. Cifrado en flujo.

1.2.2. Cifrado en bloque.

1.3. Criptografía asimétrica.

1.3.1. Cifrado.

1.3.2. Firma digital.

1.3.3. Infraestructura de clave pública.

TEMA 2. SEGURIDAD EN REDES

2.1. Asegurando las capas

2.1.1. Nivel de aplicación: Protocolos criptográficos

2.1.2. Nivel de transporte: Transport Layer Security (TLS)

2.1.3. Nivel de red: IPSec y redes privadas virtuales (VPN’s)

2.1.4. Nivel físico: Acceso a redes, IEEE 802.11x, Redes celulares, etc.

2.2. Cortafuegos.

2.3. Sistemas de detección de intrusos.

TEMA 3. SEGURIDAD DE SERVICOS Y SISTEMAS

3.1. Prácticas básicas de seguridad

3.2. Seguridad en Sistemas Operativos. Virus & Malware

3.3. Seguridad en aplicaciones web

3.4 Seguridad en el correo electrónico: SPAM

3.6. Seguridad en bases de datos

3.7. Delitos informáticos e Informática Forense

TEMA 4. GESTIÓN INTEGRAL DE LA SEGURIDAD

4.1. Legislación aplicable

4.2. Gestión de la Seguridad: SGSI, Respuesta ante incidentes y Continuidad de negocio

Prácticas de Laboratorio:

Esta actividad se realizará de forma presencial en un aula informática. Comprenderá 7 sesiones de 2 horas de duración cada una de ellas. Los alumnos presentarán posteriormente los resultados exigidos para cada una de las prácticas.

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

El calendario de la asignatura, tanto de las horas presenciales, como las sesiones de laboratorio estará definido por el centro en el calendario académico del curso correspondiente.

Bibliografía y recursos

- Kurose, J.F.; Ross, K.W. COMPUTER NETWORKING. A TOP-DOWN APPROACH FEATURING THE INTERNET. TERCERA EDICIÓN, Ed. Addison Wesley, Año 2004. (808 páginas).

- Pastor, José; Sarasa, Miguel Ángel; Salazar, José Luis. CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES SEGUNDA EDICIÓN. Prensas Universitarias de Zaragoza. Año 2001 (697 páginas).

- Fúster, Amparo; De la Guía, Dolores; Hernández, Luis; Montoya, Fausto; Muñoz, Jaime. TÉCNICAS CRIPTOGRÁFICAS DE PROTECCIÓN DE DATOS. TERCERA EDICIÓN. Editorial Ra-Ma. Año 2004 (416 páginas).

- Caballero, Pino. INTRODUCCIÓN A LA CRIPTOGRAFÍA. SEGUNDA EDICIÓN. Editorial Ra-Ma, Textos Universitarios, Madrid. Año 2002 (133 páginas).

- Stallings, William. CRYPTOGRAPHY AND NETWORK SECURITY. PRINCIPLES AND PRACTICE. FIFTHD EDITION. Prentice-Hall Inc. Año 2010 (744 páginas).

- Menezes, Alfred; Oorsschof, Paul; Vanstone, Scott. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC Press Inc. Año 2001 (816 páginas) (http://cacr.uwaterloo.ca/hac/)

- Schneier, Bruce. APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C. SECOND EDITION. John Wiley & Sons, Inc., New York. Año 1996 (758 páginas)

Referencias bibliográficas de la bibliografía recomendada

- 1. Kurose, James F.. Computer networking : a top-down approach / James F. Kurose, Keith W. Ross ; international edition adapted by Bhojan Anand . - 4th ed. Boston : Pearson, cop. 2008
- 2. Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001
- 3. Técnicas criptográficas de protección de datos / Amparo Fúster Sabater...[et al.] . - 2a. ed. rev. y act. Madrid : Ra-ma, D.L. 2000
- 5. Stallings, William. Cryptography and network security : principles and practice / Williams Stallings . - 3rd ed. Upper

Saddle River : Prentice Hall , cop. 2003
- 6. Menezes, Alfred J.. Handbook of applied cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone . - [1st ed.] Boca Raton [etc.] : CRC, cop. 1997
- 7. Schneier, Bruce. Applied cryptography : protocols, algorithms and source code in C / Bruce Schneier New York [etc.] : John Wiley and Sons, cop. 1994
- Caballero Gil, Pino. Introducción a la criptografía / Caballero, Pino Madrid: RA-MA, 2002