Universidad Zaragoza

Curso : 2020/21

30353 - Seguridad en redes y servicios

Información del Plan Docente

Año académico: 2020/21
Asignatura: 30353 - Seguridad en redes y servicios
Centro académico: 110 - Escuela de Ingeniería y Arquitectura
Titulación: 438 - Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Créditos: 6.0
Curso: 3
Periodo de impartición: Segundo semestre
Clase de asignatura: ---
Materia: ---

1.Información Básica

1.1.Objetivos 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 y controlar un sistema de manera correcta.

1.2.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.

1.3.Recomendaciones para cursar la 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.

2.Competencias y resultados de aprendizaje

2.1.Competencias

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

Concebir, diseñar y desarrollar proyectos de Ingeniería (C1)

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

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

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

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

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

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

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

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

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)

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)

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

Diseñar arquitecturas de redes y servicios telemáticos (CT6)

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

2.2.Resultados de aprendizaje

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

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.

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

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

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

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

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

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.

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.

2.3.Importancia de los resultados de aprendizaje

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.

3.Evaluación

3.1.Tipo de pruebas y su valor sobre la nota final y criterios de evaluación para cada prueba

El alumno podrá superar la asignatura mediante evaluación continua, consistente en la realización y entrega de trabajos y problemas, prácticas y la realización de una prueba de evaluación.

Los trabajos y problemas representan el 40% de la nota final.

La prueba de evaluación representará el 20% de la nota final.

Las prácticas representarán el 40% de la nota final.

Para superar la asignatura por evaluación continua es necesario que la calificación de los trabajos y problemas sea superior a 3 puntos sobre 10, que la calificación de la prueba de evaluación sea superior a 3 puntos sobre 10 y que la nota de las prácticas sea superior a 3 puntos sobre 10.

El alumno que no haya superado la asignatura por evaluación continua 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. Se trata de una prueba escrita que puede incluir tanto la resolución de problemas como preguntas teóricas y prácticas formuladas en modo de test de respuesta múltiple (las respuestas incorrectas penalizarán como 1/(N-1) siendo N el nº de posibles respuestas). Mediante esta prueba se evalúan todos los resultados de aprendizaje definidos para la asignatura.

Para superar la asignatura es necesaria una puntuación mínima de 5 puntos sobre 10 en E1.

4.Metodología, actividades de aprendizaje, programa y recursos

4.1.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:

Clase magistral participativa (20 horas). Exposición por parte del profesor de los principales contenidos de la asignatura, combinada con la participación activa del alumnado. 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.

Prácticas de laboratorio (40 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración durante 20 sesiones.

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.

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

4.2.Actividades de aprendizaje

Como se ha descrito en la metodología, las actividades se dividen en Clases magistrales (20 horas) y prácticas de laboratorio (40 horas) en las que los alumnos podrán manejar y desarrollar programas relacionados con la seguridad en los que deberán resolver planteamientos de escenarios de seguridad aplicando los conocimientos adquiridos en las clases magistrales.

De manera complementaria, el alumnado cuenta con horas de tutoría en las que poder consultar aquellas dudas personales que le hayan podido surgir.

4.3.Programa

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

1. Introducción a la seguridad en redes y servicios

2. Criptografía práctica

3. Seguridad en Sistemas Operativos

4. Sistemas Redundantes

5. Malware

6. Botnets: SPAM + Fraude + DDoS

7. Seguridad en la arquitectura TCP/IP

8. Protocolos de seguridad y VPNs + Práctica con OpenVPN

9. Seguridad perimetral: Firewalls + Práctica de programación de Firewalls

10. Sistemas de detección de intrusos + Práctica con OSSEC, Suricata y ArpWatch

11. Security Information and Event Management (SIEM) + Práctica con ElasticSearch, Logstash y Kibana (ELK)

Prácticas de Laboratorio:

Comprenderá 20 sesiones de 2 horas de duración cada una de ellas. Los alumnos presentarán posteriormente los resultados exigidos para cada una de las prácticas.

4.4.Planificación de las actividades de aprendizaje y calendario de fechas clave

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.

La asignatura consta de un total de 6 créditos ECTS. Las actividades se dividen en clases teóricas 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.

4.5.Bibliografía y recursos recomendados

http://biblos.unizar.es/br/br_citas.php?codigo=30353&year=2019