Universidad Zaragoza

Curso Académico: 2021/22

60962 - Seguridad avanzada

Información del Plan Docente

Año académico: 2021/22
Asignatura: 60962 - Advanced security
Centro académico: 110 - Escuela de Ingeniería y Arquitectura
Titulación: 623 - Máster Universitario en Ingeniería de Telecomunicación
Créditos: 6.0
Curso: 1
Periodo de impartición: Segundo semestre
Clase de asignatura: Obligatoria
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 panorama de las diversas metodologías y modelos existentes para la generación de servicios de comunicaciones seguros. Además de conocer las herramientas básicas de seguridad (confidencialidad, integridad y autenticidad), ahora necesitamos adquirir la capacidad de poder diseñar y evaluar las posibilidades de servicios más complejos (pruebas de conocimiento cero, identificación anónima, juego de azar en línea, etc.) para tener la base de planificar aquellos que en un futuro profesional se le pueda plantear. Y todo esto, sin perder de vista los servicios y las redes que actualmente las sustentan, para seguir ofreciendo un nivel de eficacia y eficiencia óptimo, y un equilibrio adecuado con los niveles de seguridad requeridos en cada servicio propuesto.

Estos planteamientos y objetivos están alineados con algunos de los Objetivos de Desarrollo Sostenible, ODS, de la Agenda 2030 (https://www.un.org/sustainabledevelopment/es/) y determinadas metas concretas, de tal manera que la adquisición de los resultados de aprendizaje de la asignatura proporciona capacitación y competencia al estudiante para contribuir en cierta medida a su logro:

- Objetivo 16: Promover sociedades, justas, pacíficas e inclusivas.

  Meta 16.5 Reducir considerablemente la corrupción y el soborno en todas sus formas.

  Meta 16.6 Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas.

  Meta 16.7 Garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas que respondan a las necesidades.

1.2. Contexto y sentido de la asignatura en la titulación

La asignatura de *Seguridad Avanzada* se imparte en el primer 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 Redes y Servicios dentro del módulo de Tecnologías de Telecomunicación, que cubre competencias obligatorias dentro de la titulación del Máster Universitario en Ingeniería de Telecomunicación.

Los resultados de aprendizaje de esta asignatura servirán de complemento a las asignaturas Redes Heterogéneas e Internet de Nueva Generación que forman parte de la materia Redes y Servicios, proporcionando al alumno los conocimientos que éste necesita para la planificación de servicios seguros de las redes de telecomunicación, aspecto fundamental para el diseño 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, aparte de cumplir los requisitos exigidos para cursar el máster, tenga un sólido dominio en la aplicación de herramientas de seguridad en las comunicaciones y amplios conocimientos sobre sus fundamentos.

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

CB6 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.

CB7 Los estudiantes sabrán 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.

CB8 Los estudiantes serán capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

CB9 Los estudiantes sabrán comunicar sus conclusiones ?y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CB10 Los estudiantes poseerán las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CG1 Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería de telecomunicación.

CG4 Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería de Telecomunicación y campos multidisciplinares afines.

CG7 Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos electrónicos y de telecomunicaciones, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.

CG11 Capacidad para saber comunicar (de forma oral y escrita) las conclusiones- y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CG12 Poseer habilidades para el aprendizaje continuado, autodirigido y autónomo.

CE4 Capacidad para diseñar y dimensionar redes de transporte, difusión y distribución de señales multimedia.

CE6 Capacidad para modelar, diseñar, implantar, gestionar, operar, administrar y mantener redes, servicios y contenidos.

CE7 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.

CE8 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.

CE9 Capacidad para resolver la convergencia, interoperabilidad y diseño de redes heterogéneas con redes locales, de acceso y troncales, así como la integración de servicios de telefonía, datos, televisión e interactivos.

2.2. Resultados de aprendizaje

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

Conoce una amplia gama de operadores criptográficos y sus características de eficiencia y costos computacionales.

Sabe valorar adecuadamente los diferentes operadores criptográficos que se deben aplicar para las exigencias que un escenario de comunicaciones puede ofrecer.

Sabe distinguir entre la seguridad de un operador y la seguridad de un protocolo.

Extrae, a partir de las finalidades de un servicio, cuáles van a ser las necesidades de seguridad en su implementación.

A partir de diferentes requisitos de los servicios, es capaz de identificar los diferentes roles de seguridad que aparecerán en su modelado.

Reconoce la corrección en el diseño de servicios seguros.

Conoce diferentes herramientas de modelado que le servirán para establecer una métrica de seguridad.

Sabe analizar el nivel de seguridad de un servicio.

Conoce los protocolos criptográficos que se aplican a la mayor parte de los servicios de seguridad y es capaz de adaptarlos a las necesidades de una implementación particular.

Es capaz de analizar un problema de seguridad en las comunicaciones, para después poder ofrecer alternativas de diseño con los operadores correspondientes y obtener una solución óptima al problema planteado.

2.3. Importancia de los resultados de aprendizaje

La asignatura la podemos calificar como fundamental dentro de la materia en la que se ubica, ya que no se puede entender el diseño, análisis e implementación de un proyecto de telecomunicaciones sin una metodología de evaluación de la seguridad y de las posibilidades y alcance de los servicios. La asignatura permite al alumno conocer y ser capaz de diseñar y evaluar el alcance y la seguridad de un sistema de comunicaciones y/o modificar un sistema previo para dotarlo de nuevas capacidades de gestión y seguridad.

3. Evaluación

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

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

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:

E1A: Examen de contenidos teórico/prácticos (50%). Puntuación de 0 a 10 puntos. Se trata de un examen escrito. Mediante esta prueba se evalúan los resultados de aprendizaje. 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 puntos sobre 10 en el Examen de Contenidos Teórico/Prácticos.

E1B: Evaluación de prácticas de laboratorio y trabajo práctico (50%). Puntuación de 0 a 10 puntos. Se realizará una práctica cuya entrega y posterior defensa frente al profesor supondrán la nota de la misma.

Para superar la asignatura es necesaria una puntuación mínima de 4 puntos sobre 10 en la Evaluación de prácticas de laboratorio.

4. Metodología, actividades de aprendizaje, programa y recursos

4.1. Presentación metodológica general

El proceso de aprendizaje se desarrollará en varios niveles: clases magistrales en las que se fomentará la participación del alumno, clases prácticas en el laboratorio. La metodología que se propone trata de fomentar el trabajo continuado del estudiante.

4.2. Actividades de aprendizaje

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:

A01: Clase magistral (30 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 está diseñada para proporcionar a los alumnos los fundamentos teóricos del contenido de la asignatura.

A02: Resolución de problemas y casos (10 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 puede exigir trabajo de preparación por parte de los alumnos.

A03: Prácticas de laboratorio (20 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración cada semana.

A08: Evaluación (3 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

4.3. Programa

Introducción a los servicios seguros de comunicaciones: motivación y definición.

Principios de diseño de servicios seguros.

Operadores criptográficos: Criptografía simétrica y asimétrica.

Funciones pseudoaleatorias.

Cifrado en bloque.

Funciones Hash.

Cifrado autenticado.

Criptografía de clave pública.

Herramientas de análisis y gestión de servicios seguros.

Servicios seguros: Confidencialidad, autenticidad, integridad, distribución de claves, compartición de secretos, blockchains, etc.

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

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.

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.

4.5. Bibliografía y recursos recomendados

http://biblos.unizar.es/br/br_citas.php?codigo=60962&year=2020