Universidad Zaragoza

Curso Académico: 2022/23

30390 - Seguridad en redes y servicios

Información del Plan Docente

Año académico: 2022/23
Asignatura: 30390 - Seguridad en redes y servicios
Centro académico: 110 - Escuela de Ingeniería y Arquitectura
Titulación: 581 - Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación
Créditos: 6.0
Curso: 4
Periodo de impartición: Primer semestre
Clase de asignatura: Optativa
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 una perspectiva general del mundo de la ciberseguridad tanto en redes de comunicaciones como en aplicaciones y servicios informáticos. La ciberseguridad es uno de los pilares fundamentales para el funcionamiento de los sistemas TIC y es un área en pleno auge donde se está demandado una gran cantidad de profesionales cualificados. El enfoque es generalista, tocando las áreas más relevantes de la ciberseguridad actual y profundizando en alguno de ellos para que el alumno pueda experimentar este apasionante tema. 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. Continuamos con las características de las redes, servicios y aplicaciones ciberseguros y las herramientas que tenemos a nuestra disposición para conseguirlos. En un tercer paso, se exponen los peligros más relevantes a los que se enfrentan los servicios y sistemas de comunicaciones y cómo se pueden afrontar, para acabar, en un cuarto paso, juntando todas estas piezas en un marco común y poder así securizar y controlar un sistema con un alto grado de seguridad (como veremos en la asignatura, la seguridad absoluta no existe).

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 8: Promover el crecimiento económico sostenido, inclusivo y sostenible, el empleo pleno y productivo y el trabajo decente para todo.

> Meta 8.2: Lograr niveles más elevados de productividad económica mediante la diversificación, la modernización tecnológica y la innovación, entre otras cosas centrándose en los sectores con gran valor añadido y un uso intensivo de la mano de obra.

Objetivo 9: Industria, innovación e infraestructuras.

> Meta 9.1 Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, incluidas infraestructuras regionales y transfronterizas, para apoyar el desarrollo económico y el bienestar humano, haciendo especial hincapié en el acceso asequible y equitativo para todos.
>
> Meta 9.5 Aumentar la investigación científica y mejorar la capacidad tecnológica de los sectores industriales de todos los países, en particular los países en desarrollo, entre otras cosas fomentando la innovación y aumentando considerablemente, de aquí a 2030, el número de personas que trabajan en investigación y desarrollo por millón de habitantes y los gastos de los sectores público y privado en investigación y desarrollo
>
> Meta 9.c Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020.

1.2. Contexto y sentido de la asignatura en la titulación

La asignatura de *Seguridad en Redes y Servicios* se imparte en el cuarto curso de la titulación, más concretamente en el semestre de otoño 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 especifica de Telemática.

Los resultados de aprendizaje de esta asignatura servirán de complemento a las asignaturas de Transporte de Servicios Multimedia y Diseño y Evaluación de Redes que forman parte de la materia Arquitectura de redes y servicios, así como

Gestión de Red y Comercio electrónico, que forman parte de la materia Diseño de Servicios Telemáticos, 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 y sistema.

1.3. Recomendaciones para cursar la asignatura

Para seguir con normalidad esta asignatura es recomendable que el alumno que quiera cursarla haya cursado previamente las asignaturas básicas comunes: de *Fundamentos de Redes*, *Interconexión de redes* y *Programación de redes y servicios*.

Para el óptimo aprovechamiento de la asignatura se recomienda al alumno la asistencia activa a clase. 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 esta.

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)

Capacidad para 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.

R2. Conoce la complejidad de los problemas computacionales que sustentan a dichos operadores criptográficos.

R3. Sabe caracterizar los protocolos criptográficos básicos: confidencialidad, autenticidad e integridad. Es capaz de aplicarlos a diferentes aplicaciones distribuidas.

R4. Conoce los fundamentos básicos de la seguridad informática.

R5. Conoce las herramientas básicas para el análisis de las vulnerabilidades en redes de comunicaciones así como las técnicas y/o herramientas para paliarlas.

R6. Conoce los protocolos para securizar los diferentes niveles de la arquitectura TCP/IP.

2.3. Importancia de los resultados de aprendizaje

La asignatura podemos calificarla como útil para cualquier itinerario de la titulación. Además, 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.

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, problemas, prácticas y la realización de una prueba de evaluación.

A. Los problemas representan el 40% de la nota final.
B. Las prácticas representarán el 20% de la nota final.
C. Los trabajos representarán un 20% de la nota final.
D. La prueba de evaluación representará el 20% de la nota final.

Para superar la asignatura por evaluación continua es necesario que la calificación de cada una de las partes (A, B, C, D) s sea superior a 3 puntos sobre 10, y que la media de todas las partes sea superior a 5.

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, pruebas prácticas en el laboratorio así como preguntas teóricas y prácticas formuladas en modo test u otro modo. 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 (30 horas). Exposición por parte del profesor de los principales contenidos de la asignatura, combinada con la participación 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.

Prácticas de laboratorio (30 horas). Los alumnos realizarán sesiones de prácticas de 2 horas de duración durante 15 sesiones.

Realización de trabajos prácticos tutelados (15 horas). Esta actividad no presencial permitirá avanzar en todos los resultados de aprendizaje propuestos. La evolución del trabajo será presentada periódicamente al profesor.

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 (30 horas) y prácticas de laboratorio (30 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. Además, se realizan trabajos prácticos tutelados (15 horas) donde se abordará tenas actuales de ciberseguridad.

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 ciberseguridad
2. Criptografía práctica
3. Seguridad en Aplicaciones, Sistemas Operativos y Endpoints
4. Sistemas Redundantes
5. Botnets: SPAM + Fraude + DDoS
6. Malware
7. Seguridad en la arquitectura TCP/IP

8. Protocolos de seguridad y VPNs

9. Anonimato en Internet: TOR + Proxy

10. Ciberinteligencia: Shodan + Foca

Prácticas de Laboratorio:

Comprenderá 15 sesiones de 2 horas de duración cada una de ellas. Al principio de cada práctica se hará una exposición de los fundamentos teóricos necesarios para llevarla a cabo. Los alumnos presentarán posteriormente los resultados exigidos para cada una de las prácticas.

1. Auditoría de Seguridad Externa

2. Montando una VPN: Túnel openVPN

3. Implementando Seguridad perimetral: Firewalls

4. Detectando amenazas: Intrusion Detection Systems

5. Implementando un SIEM: Elasticsearch

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

El calendario de la asignatura 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, problemas, trabajos, etc. 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 se harán públicas atendiendo a los horarios fijados por la Escuela.

4.5. Bibliografía y recursos recomendados

http://psfunizar10.unizar.es/br13/egAsignaturas.php?codigo=30390