Universidad Zaragoza

Curso Académico: 2023/24

30390 - Seguridad en redes y servicios

Información del Plan Docente

Año académico: 2023/24
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 de la asignatura

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 al logro de las metas 8.2 del objetivo 8, y de las metas 9.1, 9.5 del Objetivo 9.

2. Resultados de aprendizaje

- 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.
- Sabe caracterizar los protocolos criptográficos básicos: confidencialidad, autenticidad e integridad. Es capaz de aplicarlos a diferentes aplicaciones distribuidas.
- Conoce los fundamentos básicos de la seguridad informática.
- Conoce las herramientas básicas para el análisis de las vulnerabilidades en redes de comunicaciones así como las técnicas y/o herramientas para paliarlas.
- Conoce los protocolos para securizar los diferentes niveles de la arquitectura TCP/IP.

3. Programa de la asignatura

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:

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. Actividades académicas

Clase magistral participativa (30 horas). Exposición por parte del profesor de los principales contenidos de la asignatura, combinada con la participación del alumnado.

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.

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.

5. Sistema de evaluación

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/ejercicios 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.