FICHA IDENTIFICATIVA

DATOS DE LA ASIGNATURA

Código: 34896
Nombre: Seguridad informática
Ciclo: Grado
Créditos ECTS: 6
Curso académico: 2025-26

TITULACIONES

Titulación	Centro	Curso	Periodo
1403 - Grado en Ingeniería Telemática	Escola Tècnica Superior d'Enginyeria	3	Sin determinar, Segundo cuatrimeste

MATERIAS

Titulación	Materia	Carácter
1403 - Grado en Ingeniería Telemática	Administración de Sistemas	OBLIGATORIA

COORDINACIÓN

SORIANO GARCIA FRANCISCO R

RESUMEN

La seguridad es un atributo esencial de los sistemas informáticos. Incluso en una disciplina como la informática, en la que los cambios son continuos, los requisitos de seguridad cambian a un ritmo especialmente rápido. Este ritmo se debe sobre todo a dos razones. La primera es la dependencia de sistemas informáticos es cada vez mayor, por lo que el nivel de exigencia aumenta. La segunda es la continua aparición de nuevas tecnologías. Estas nuevas capacidades permiten implantar mecanismos de seguridad más refinados, pero al mismo tiempo también posibilitan la realización de ataques más sofisticados, lo que provoca un cambio continuo.

En este contexto, la asignatura está planteada para dar una visión de conjunto de los elementos esenciales de la seguridad de los sistemas informáticos, buscando que el alumno aprenda a seguir este proceso de cambio continuo y sea capaz de mantenerse al día y de utilizar, en cada momento, las técnicas más apropiadas. En este sentido, la asignatura se apoya sustancialmente en los conceptos específicos introducidos en las asignaturas de redes, sistemas operativos, bases de datos y programación, al mismo tiempo que los complementa con contenidos propios del ejercicio profesional de la seguridad, como el establecimiento de políticas de seguridad, el análisis de vulnerabilidades, la detección de intrusos o el análisis forense.

La asignatura Seguridad informática se imparte en el segundo cuatrimestre de tercer curso como parte de la materia Administración de sistemas.

CONOCIMIENTOS PREVIOS

RELACIÓN CON OTRAS ASIGNATURAS DE LA MISMA TITULACIÓN

No se han especificado restricciones de matrícula con otras asignaturas del plan de estudios.

OTROS TIPOS DE REQUISITOS

Se recomienda haber cursado las siguientes asignaturas: Informática, Ampliación de Informática, Sistemas operativos y Arquitectura de redes de computadores. De entre ellas, son especialmente relevantes las dos últimas, por tratar algunos conceptos relacionados con la seguridad que complementan los contenidos estudiados en esta asignatura.

COMPETENCIAS / RESULTADOS DE APRENDIZAJE

-

E1 - Capacidad de 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.

E2 - Capacidad para 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.

E3 - Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis.

G4 - Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico de Telecomunicación.

R1 - Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación.

DESCRIPCIÓN DE CONTENIDOS

1. Introducción

Concepto de seguridad
¿Qué queremos proteger y por qué? Política de seguridad
¿Frente a qué? Riesgos y vulnerabilidades
El proceso de la seguridad
Normativas (ética, legislación y estándares, ISACA, ISO 27000, IS2)

2. Criptografía

Criptografía simétrica
Criptografía asimétrica
Funciones de dispersión (hashes)
Comunicación y almacenamiento seguros
Integridad
Firma digital
Gestión de claves públicas
Autenticación e intercambio de claves de sesión
Privacidad
Laboratorio

3. Seguridad del nodo

Validación y autenticación
Control de acceso
Programación segura
Seguridad del servidor y seguridad del cliente
Laboratorio

4. Seguridad perimétrica

Concepto de cortafuegos
Filtrado de paquetes
Proxies
Diseño de cortafuegos
Integración de VPNs
Laboratorio

5. Detección y tratamiento de intrusiones

Detección de intrusos basada en el host (HIDS)
Detección de intrusos basada en la red (NIDS)
Honeypots y honeynets
Análisis forense

Laboratorio

6. Auditoria y Hacking Ético

Introducción al proceso de auditoría
El test de intrusión y sus tipos
Fases de un ataque/test de intrusión
Herramientas para el hacking ético

VOLUMEN DE TRABAJO (HORAS)

ACTIVIDADES PRESENCIALES

Actividad	Horas
Teoría	30,00
Prácticas en aula	10,00
Laboratorio	20,00
Total horas	**60,00**

ACTIVIDADES NO PRESENCIALES

Actividad	Horas
Asistencia a otras actividades	0,00
Elaboración de trabajos individuales o en grupo	10,00
Estudio y trabajo autónomo	30,00
Preparación de clases	30,00
Preparación de actividades de evaluación	20,00
Resolución de casos prácticos	0,00
Total horas	**90,00**

METODOLOGÍA DOCENTE

Las actividades formativas se desarrollarán de acuerdo con la siguiente distribución:

- Actividades teóricas. En las clases teóricas se desarrollarán los temas proporcionando una visión global e integradora, analizando con mayor detalle los aspectos clave y de mayor complejidad, fomentando, en todo momento, la participación del alumnado (E-2).

- Actividades prácticas. Complementan las actividades teóricas con el objetivo de aplicar los conceptos básicos y ampliarlos con el conocimiento y la experiencia que vayan adquiriendo durante la realización de los trabajos propuestos. Comprenden los siguientes tipos de actividades presenciales: clases de problemas y cuestiones en aula, sesiones de discusión y resolución de problemas y ejercicios previamente trabajados por el alumnado, prácticas de laboratorio , presentaciones orales, conferencias, tutorías programadas (individualizadas o en grupo) (G-4, E-2)

- Trabajo personal del alumnado. Realización (fuera del aula) de trabajos monográficos, búsqueda bibliográfica dirigida, cuestiones y problemas, así como la preparación de clases y exámenes (estudio). Esta tarea se realizará de manera individual e intenta potenciar el trabajo autónomo. (G-4, R-1, E-2)

- Trabajo en pequeños grupos. Realización, por parte de pequeños grupos de estudiantes (2-4) de trabajos, cuestiones, problemas fuera del aula. Esta tarea complementa el trabajo individual y fomenta la capacidad de integración en grupos de trabajo. (G-4, R-1, E-2).

EVALUACIÓN

Primera Convocatoria

La asignatura podrá ser evaluada de dos formas distintas, una dando mayor peso a las actividades presenciales y otra con mayor peso para el examen final. Todo el alumnado tendrá como nota final la más alta de las dos.

La evaluación de la asignatura se llevará a cabo en la primera convocatoria mediante:

Evaluación de la teoría y los problemas (TP).

Esta parte tendrá un peso del 70 % de la nota final y será necesario llegar a un 4,5 sobre 10 para promediar.

Evaluación continua (EC), basada en la participación y grado de implicación en el proceso de enseñanza-aprendizaje, teniendo en cuenta la asistencia regular a las actividades presenciales previstas y la resolución de cuestiones y problemas propuestos. Esta parte no es recuperable (G-4, R-1, E-2).

Pruebas objetivas individuales, consistentes en varios exámenes o pruebas de conocimiento, que constarán tanto de cuestiones teórico-prácticas como de problemas. Las pruebas se realizarán hacia la primera mitad del cuatrimestre (denominada T1), durante la segunda mitad del cuatrimestre (T2) y fuera del horario lectivo en el periodo de exámenes (denominada T3). (G-4, E-2).

Cada una de estas pruebas abordará todos los contenidos de la asignatura impartidos hasta el momento de su realización.

La nota de TP se calculará de la siguiente forma:

TP = 0,15 * EC + 0,15* T1 + 0,25 * T2 + 0,45 * T3.

Evaluación de las actividades prácticas de laboratorio (L) a partir de la consecución de objetivos en las sesiones de laboratorio. (G-4, E-2)

Estas actividades se realizarán por parejas, su peso será del 30 % sobre la nota final y será necesario llegar a un 4,5 sobre 10 para promediar. Todas las sesiones de laboratorio tendrán el mismo peso sobre la nota final.

En caso de no poder asistir a una sesión, el alumnado podrá entregar el trabajo correspondiente a su profesorado de laboratorio. La entrega deberá ser en persona, en horario de tutorías y el alumnado deberá estar preparado para responder cuestiones sobre la realización de la práctica y para realizar partes de la misma en el momento (con pequeños cambios). Este tipo de entrega tiene que ser realizada antes de que ningún grupo de laboratorio haya realizado la práctica y tendrá una penalización del 20 %.

La nota de la asignatura se conformará en el caso de seguir la evaluación continua como la suma de las

partes anteriores del siguiente modo:

Si TP es menor 4,5 o L es menor que 4,5

Nota_Final = Mínimo (TP, L)

En otro caso:

Nota_final = 0,70 * TP + 0,30 * L

En caso de no haber superado la asignatura siguiendo la evaluación continua (o en caso de que la nota calculada de esta segunda forma resultara más favorable para el alumno), la prueba de evaluación T3 será el examen final de la asignatura y TP se calculará de la siguiente forma:

TP = 0,15 * EC + 0,85 * T3

La nota final se calculará de la misma forma que con la evaluación continua.

Segunda convocatoria

En la segunda convocatoria la asignatura se evaluará de la misma forma que en la primera convocatoria, con las siguientes salvedades:

a.- Se abrirá un plazo de entrega de prácticas con las mismas condiciones que en la primera convocatoria (lógicamente no se realizarán en el laboratorio), salvo que la penalización será del 30 % y que la entrega deberá realizarse antes del examen de la segunda convocatoria.

b.- El examen de la segunda convocatoria sustituirá a la prueba T3.

c.- En la parte EC se mantendrá la nota del alumno.

Adelanto de convocatoria

Para poder solicitar adelanto de convocatoria, el estudiantado deberá haber cursado previamente la asignatura y haber obtenido la nota mínima exigida en la evaluación de las actividades prácticas de laboratorio (L). De esta forma se trata de conciliar el derecho del estudiantado a dicho adelanto con la metodología docente y el mecanismo de evaluación de la asignatura.

En cualquier caso, el sistema de evaluación se regirà por lo establecido en el Reglamento de Evaluación y Calificación de la Universitat de València para grados y masters (**ACGUV 108/2017**).

La copia o plagio manifiesto de cualquier actividad que forma parte de la evaluación supondrá la imposibilidad de superar la asignatura, sometiéndose seguidamente a los procedimientos disciplinarios oportunos indicados en el *PROTOCOLO DE ACTUACIÓN ANTE PRÁCTICAS FRAUDULENTAS EN LA UNIVERSITAT DE VALÈNCIA* (ACGUV 123/2020).

BIBLIOGRAFÍA

Básica:

- Pfleeger, Charles P., et al. Security in Computing. Sixth edition., Addison Wesley Professional, 2024
- Kizza, Joseph Migga. Guide to Computer Network Security. 6th ed. 2024., Springer International Publishing, 2024, https://doi.org/10.1007/978-3-031-47549-8

Complementaria:

- Vacca, John R., editor. Computer and Information Security Handbook. Volume 1. Fourth edition., Morgan Kaufmann, 2025
- Pfleeger, Charles P., and Shari Lawrence Pfleeger. Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach. 1st edition, Prentice Hall, 2012
- Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. 5th ed., Pearson, 2014.
- Schneier, Bruce. Applied Cryptography¿: Protocols, Algorithms, and Source Code in C. 20th anniversary edition., Wiley, 2015.
- Zwicky, Elizabeth D., et al. Building Internet Firewalls. 2nd ed., O¿Reilly, 2000.
- Northcutt, Stephen. Inside Network Perimeter Security. 2nd ed., Sams, 2005.
- Khan, Umer. Cisco PIX Firewalls: Configure / Manage / Troubleshoot. 1st ed., Elsevier Science & Technology Books, 2005, https://doi.org/10.1016/B978-1-59749-004-7.X5000-6.
- Sammons, John. The Basics of Digital Forensics¿: The Primer for Getting Started in Digital Forensics. Second edition., Syngress, 2015.
- Nikkel, Bruce. Practical Linux Forensics. No Starch Press, 2021
- Carrier, Brian. File System Forensic Analysis. Addison-Wesley, 2005
- Farmer, Dan, and Wietse Venema. Forensic Discovery. Addison-Wesley, 2004.
- Shiva V. N. Parasram. Digital Forensics with Kali Linux - Second Edition. Packt Publishing, 2020.
- Cannon, David, et al. CISA¿: Certified Information Systems Auditor Study Guide. 4th ed., Sybex, a Wiley brand, 2016.
- Engebretson, Patrick. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Second edition, Elsevier Science, 2013.
- Graham, Daniel. Ethical Hacking. No Starch Press, 2021.
- Sheikh, Ahmed. Certified Ethical Hacker (CEH) Preparation Guide¿: Lesson-Based Review of Ethical Hacking and Penetration Testing. 1st ed., Apress, 2021, https://doi.org/10.1007/978-1-4842-7258-9.
- Velu, Vijay Kumar. Mastering Kali Linux for Advanced Penetration Testing¿: Become a Cybersecurity Ethical Hacking Expert Using Metasploit, Nmap, Wireshark, and Burp Suite. Fourth edition., Packt Publishing, Limited, 2022.