FICHA IDENTIFICATIVA

DATOS DE LA ASIGNATURA

Código: 34681
Nombre: Seguridad informática
Ciclo: Grado
Créditos ECTS: 6
Curso académico: 2026-27

TITULACIONES

Titulación	Centro	Curso	Periodo
1400 - Grado en Ingeniería Informática	Escola Tècnica Superior d'Enginyeria	3	Segundo cuatrimeste
1407 - Grado en Ingeniería Multimedia	Escola Tècnica Superior d'Enginyeria	4	Segundo cuatrimeste
1936 - Doble Grado en Matemáticas e Ingeniería Informática	Facultat de Ciències Matemàtiques	4	Segundo cuatrimeste

MATERIAS

Titulación	Materia	Carácter
1400 - Grado en Ingeniería Informática	Sistemas Operativos, Sistemas Distribuidos y Redes	OBLIGATORIA
1407 - Grado en Ingeniería Multimedia	Optatividad	OPTATIVA
1936 - Doble Grado en Matemáticas e Ingeniería Informática	Cuarto curso	OBLIGATORIA

COORDINACIÓN

SORIANO GARCIA FRANCISCO R

PEREZ CONDE CARLOS

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 alumnado 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 "Sistemas operativos, sistemas distribuidos y redes"

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: Programación, Estructuras de datos y algoritmos, 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

1400 - Grado en Ingeniería Informática

G3 - Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

G4 - Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según las competencias específicas establecidas.

G6 - Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos según las competencias específicas establecidas.

R1 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

R5 - Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas.

SI2 - Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.

TI2 - Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.

TI7 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

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
   Seguridad de los programas
   Seguridad de servidores y clientes
   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.- 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).- 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.- 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.Se utilizará la plataforma de e-learning (Aula Virtual) de la Universitat de València como soporte de comunicación con el alumnado. A través de ella se tendrá acceso al material didáctico utilizado en clase, así como los problemas y ejercicios a resolver.

EVALUACIÓN

La evaluación de la asignatura se llevará a cabo en la **primera convocatoria** de la siguiente forma:- 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, no tiene nota mínima y tiene un peso sobre la nota final del 10 %.- Pruebas objetivas individuales (EX), 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). Cada una de estas pruebas abordará todos los contenidos de la asignatura. Como el T3 incluye toda la asignatura, EX se calcula de dos formas y se utiliza automáticamente la más favorable: EX = Máximo(T3; 0,2*T1+0,3*T2+0,5*T3) Esta parte tiene un peso sobre la nota final del 60 % y es necesario llegar a un 4,5 sobre 10 para promediar. Los exámenes T1 y T2 no son recuperables.- Evaluación de las actividades prácticas y de laboratorio (PL) a partir de la consecución de objetivos en las sesiones de laboratorio, la elaboración de trabajos/memorias y exposiciones orales. 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 o la estudiante podrá entregar el trabajo correspondiente a su profesor o profesora de laboratorio. La entrega deberá ser en persona, en horario de tutorías y el o la estudiante deberá estar preparado o preparada 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 final de la asignatura se calculará de la siguiente forma: Si EX < 4,5 o PL < 4,5: Nota_final = Mínimo(EX; PL) En otro caso: Nota_final = 0,1*EC + 0,6*EX + 0,3*PLEn la **segunda convocatoria** la asignatura se evaluará de la misma forma que en la primera convocatoria, con las siguientes salvedades:- 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.- El examen de la segunda convocatoria sustituirá a la prueba T3.- En la parte EC se mantendrá la nota del estudiante.Para poder solicitar **adelanto de convocatoria**, los estudiantes deberán haber cursado previamente la asignatura y haber obtenido la nota mínima exigida en la evaluación de las actividades prácticas y de laboratorio (PL). De esta forma se trata de conciliar el derecho del alumnado a dicho adelanto con la metodología docente y el mecanismo de evaluación de la asignatura.En cualquier caso, la evaluación de la asignatura se hará de acuerdo con el Reglamento de evaluación y calificación de la Universitat de València para los títulos de grado y master aprobado por Consejo de Gobierno de 30 de mayo de 2017 (ACGUV 108/2017). Asimismo, 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

- Referencias básicas

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.

- Referencias complementarias

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.

Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 20th anniversary edition., Wiley, 2015.

Tanenbaum, Andrew S., and David J. Wetherall. Computer Networks. 5th ed., Pearson, 2014.

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.

Oettinger, W. (2022). Learn computer forensics: your one-stop guide to searching, analyzing, acquiring, and securing digital evidence (2nd ed.). Packt Publishing. https://doi.org/10.0000/9781803239071

Johansen, G. (2025). Digital forensics and incident response: incident response tools and techniques for effective cyber threat response (Fourth edition.). Packt Publishing.

Toolan. (2025). File System Forensics. (1st ed.). John Wiley & Sons, Ltd.

Parasram, S. V. N. (2023). Digital forensics with Kali linux: enhance your investigation skills by performing network and memory forensics with Kali Linux 2022. x (Third edition.). Packt Publishing Ltd. https://doi.org/10.0000/9781837639656

Singh, G. D. (2024). The Ultimate Kali Linux Book: Harness Nmap, Metasploit, Aircrack-Ng, and Empire for Cutting-edge Pentesting (Third edition.). Packt Publishing Ltd.

Messier, R. (2024). Learning Kali Linux: security testing, penetration testing & ethical hacking (2nd ed.). O'Reilly Media, Incorporated.

Doshi, H. (2024). CISA: Certified Information Systems Auditor study guide (Third edition.). Packt Publishing Ltd.

Gregory, P. H., & Chapple, M. (2025). CISA Certified Information Systems Auditor Study Guide: Covers 2024 - 2029 Exam Objectives. (1st ed.). John Wiley & Sons, Incorporated.

Panek, W. (2026). CEH Certified Ethical Hacker V13 Study Guide. (1st ed.). John Wiley & Sons, Incorporated.