

Titulación	Tipo	Curso
Ingeniería Informática	OB	3
Ingeniería Informática	OP	4

Profesor/a de contacto

Nombre : Guillermo Navarro Arribas

Correo electrónico : guillermo.navarro@uab.cat

Equipo docente

Carlos Garrigues Olivella

Idiomas de los grupos

Puede consultar esta información al [final](#) del documento.

Prerrequisitos

No hay requisitos oficiales, pero sí se recomienda tener conocimientos básicos sobre criptografía, redes y programación. Estos conocimientos son alcanzables con asignaturas previas del grado: Redes, Información y Seguridad, Fundamentos de Tecnologías de la Información y Metodología de la Programación.

Objetivos

El objetivo de esta asignatura es que el alumnado alcance unos conocimientos básicos sobre la problemática de la seguridad de la información y los mecanismos existentes para la protección de sistemas informáticos. De esta manera, el alumnado puede desarrollar una visión crítica hacia la seguridad informática. Por otra parte, el alumnado deberá ser capaz de poner en práctica algunos aspectos de la asignatura. Conocer cómo se realizan ciertos ataques es un paso importante para entender las necesidades de seguridad de los sistemas, y poder luego aplicar técnicas de protección adecuadas en cada caso.

Resultados de aprendizaje

1. Desarrollar un pensamiento y un razonamiento crítico.
2. Diseñar sistemas de protección de la información: control de acceso e integridad.
3. Conocer y comprender las posibilidades técnicas de implantación de políticas de seguridad en sistemas distribuidos.
4. Determinar los requisitos de seguridad y confidencialidad, así como identificar los principales tipos de ataques y amenazas.
5. Determinar los requisitos de seguridad y cumplimiento de la normativa y la legislación vigente en los sistemas de información y comunicación de una organización.

6. Conocer los principios de la informática forense y del tratamiento de los delitos informáticos.
7. Comprender y aplicar los principios de seguridad en la elaboración y ejecución de planes de actuación.
8. Colaborar en el diseño y seguimiento de las políticas de seguridad de sistemas informáticos.
9. Trabajar cooperativamente.

Contenidos

Mecanismos de seguridad

- Autenticación
- Autorización y control de acceso
- Infraestructura de clave pública
- Seguridad del software
- Detección de malware y detección de intrusiones
- Privacidad de datos

Gestión de la seguridad y otros aspectos

- Gestión de vulnerabilidades
- Modelado de amenazas y ataques, pentesting
- Gestión de riesgos

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Sesiones de teoría	26	1,04	1, 2, 3, 4, 5, 6, 7, 8
Preparación y estudio del trabajo autónomo de prácticas y problemas	45	1,8	1, 2, 3, 4, 5, 6, 7, 8, 9
Preparación y estudio de las pruebas de evaluación	30	1,2	1, 2, 3, 4, 5, 6, 7, 8
Sesiones de laboratorio	12	0,48	1, 2, 3, 4, 5, 6, 7, 8, 9
Trabajo tutorizado	18	0,72	1, 2, 3, 4, 5, 6, 7, 8
Sesiones de problemas	12	0,48	1, 2, 3, 4, 5, 6, 7, 8, 9

La asignatura se desarrolla en 50 horas de actividades dirigidas repartidas en sesiones de teoría, problemas y laboratorio. En el planteamiento de la asignatura se potenciará el trabajo tutorizado sobre aspectos concretos de la asignatura. Este trabajo se divide en una parte supervisada que se realizará en las sesiones de clase, y una parte no supervisada que el alumnado realizará de manera autónoma.

De forma más concreta las actividades dirigidas son:

- Sesiones de teoría y problemas: el profesorado suministrará información sobre los conocimientos de la asignatura y sobre estrategias para adquirir, ampliar y organizar estos conocimientos. Se fomentará una participación activa del alumnado, y se realizará un seguimiento del aprendizaje mediante actividades individuales o en grupo.
- Sesiones de prácticas en el laboratorio: donde se tratarán con profundidad y a nivel práctico temas relacionados con los expuestos en las sesiones de teoría.

Durante todo el curso se utilizará el aula Moodle del Campus Virtual de la UAB como medio principal de comunicación entre el profesorado y el alumnado.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Evaluación

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Prácticas laboratorio	40%	2	0,08	1, 2, 3, 4, 5, 6, 7, 8, 9
Problemas, ejercicios, y actividades	15%	2	0,08	1, 2, 3, 4, 5, 6, 7, 8, 9
Pruebas individuales	45%	3	0,12	1, 2, 3, 4, 5, 6, 7, 8

Evaluación final y calificaciones:

Sobre la evaluación continuada que se llevará a cabo durante el curso se prevé la realización de:

- 2 pruebas parciales de evaluación individual. La nota mínima exigida de cada una de las pruebas es de 4,5 sobre 10.
- Evaluación de prácticas de laboratorio. La nota mínima exigida de cada una de las prácticas es de 4,5 sobre 10.
- Evaluación de problemas/actividades. Esta parte no requiere nota mínima.

Para poder aprobar la asignatura es necesario que la evaluación de cada una de las partes supere el mínimo exigido y que la evaluación total supere los 5 puntos. En caso de no superar la asignatura porque alguna de las actividades de evaluación no alcance la nota mínima requerida, la nota numérica del expediente será el valor menor entre 4,5 y la media ponderada de las notas.

La calificación de "no evaluable" se otorgará al alumnado que no participe en ninguna de las actividades de evaluación.

Para cada actividad de evaluación se indicará un lugar, fecha y hora de revisión en la que el alumnado podrá revisar la actividad con el profesorado. En este contexto, se podrán presentar reclamaciones sobre la nota de la actividad, que serán evaluadas por el profesorado responsable de la asignatura. Si el estudiante no se presenta a esta revisión, no se revisará posteriormente dicha actividad.

Concesión de matrículas de honor: las MH solo se podrán conceder a estudiantes que hayan obtenido una calificación final igual o superior a 9,00. Se puede otorgar hasta un 5% de MH del total de estudiantes matriculados.

Recuperación de notas de la evaluación continuada:

- Se realizará un examen final de recuperación que permitirá recuperar los exámenes parciales de forma separada.
- Asimismo, se permitirá recuperar aquellas prácticas suspendidas (esta entrega adicional comportará una penalización en la nota final de la práctica).
- La evaluación de problemas/actividades no es recuperable, pero el alumnado puede optar (a principio de curso) por ser evaluado en esta parte mediante una prueba adicional de actividades que se realizará el mismo día que la prueba de recuperación de validación de conocimientos.

Convalidaciones parciales al alumnado repetidor: Inicialmente, no se plantea la posibilidad de convalidar partes de la asignatura, ni la realización de pruebas especiales para el alumnado repetidor. Aun así, este hecho se puede reconsiderar a principio de curso en función de los contenidos de cada parte.

Calendario de actividades: Las fechas de evaluación continuada y entrega de trabajos y prácticas se publicarán en el campus virtual y pueden estar sujetas a cambios de programación por motivos de adaptación a posibles incidencias. Siempre se informará en el campus virtual sobre estos cambios, ya que se entiende que es el mecanismo habitual de intercambio de información entre el profesorado y el alumnado. Asimismo,

se detallarán con suficiente antelación los mecanismos de evaluación, metodología o funcionamiento general de la asignatura que no se hayan concretado en esta guía.

Compromiso ético: Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, las irregularidades cometidas por un/a estudiante que puedan conducir a una variación de la calificación en una actividad evaluable se calificarán con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para aprobar la asignatura, esta asignatura quedará suspendida directamente, sin oportunidad de recuperarla en el mismo curso. Estas irregularidades incluyen, entre otras:

- la copia total o parcial de una práctica, informe, o cualquier otra actividad de evaluación;
- dejar copiar;
- presentar un trabajo de grupo no realizado íntegramente por los miembros del grupo (aplicado a todos los miembros, no solo a los que no han trabajado);
- uso no autorizado de la IA (p. ej., Copilot, ChatGPT o equivalentes) para resolver ejercicios, prácticas y/o cualquier otra actividad evaluable;
- presentar como propios materiales elaborados por un tercero, aunque sean traducciones o adaptaciones, y en general trabajos con elementos no originales y exclusivos del estudiante;
- tener dispositivos de comunicación (como teléfonos móviles, smartwatches, bolígrafos con cámara, etc.) accesibles durante las pruebas de evaluación;
- hablar con compañeros durante las pruebas de evaluación;
- copiar o intentar copiar de otros alumnos durante las pruebas de evaluación;
- usar o intentar usar escritos relacionados con la materia durante la realización de las pruebas de evaluación, cuando estos no hayan sido explícitamente permitidos.

La nota numérica del expediente será el valor menor entre 3,0 y la media ponderada de las notas en caso de que el alumnado haya cometido irregularidades en un acto de evaluación (y, por tanto, no será posible el aprobado por compensación). En ediciones futuras de esta asignatura, al alumnado que haya cometido irregularidades en un acto de evaluación no se le convalidará ninguna de las actividades de evaluación realizadas. En resumen: copiar, dejar copiar o plagiar (o el intento de) en cualquiera de las actividades de evaluación equivale a un SUSPENSO, no compensable y sin convalidaciones de partes de la asignatura en cursos posteriores.

Para esta asignatura, se permite el uso de tecnologías de inteligencia artificial (IA) exclusivamente en tareas de apoyo, como la búsqueda bibliográfica o de información, la corrección de textos o las traducciones. El estudiante deberá identificar claramente qué partes han sido generadas con esta tecnología, especificar las herramientas empleadas e incluir una reflexión crítica sobre cómo estas han influido en el proceso y el resultado final de la actividad. La falta de transparencia en el uso de la IA en actividades evaluables se considerará falta de honestidad académica y puede comportar una penalización parcial o total en la nota de la actividad, o sanciones mayores en casos de gravedad.

Evaluación única: La evaluación única de la asignatura constará de las siguientes actividades de evaluación:

- Examen individual: examen individual sobre el contenido de la asignatura, 75% sobre la calificación final.
- Prácticas: entrega y validación de las prácticas que se propondrán de forma específica para el alumnado de evaluación única, 50% sobre la calificación final.
- Se aplicará el mismo sistema de recuperación que para la evaluación continuada, pero respecto a las actividades de evaluación única. La revisión de la calificación final sigue el mismo procedimiento que para la evaluación continuada.

Bibliografía

Bibliografía principal:

- Paul C. van Oorschot (2021) Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, Second Edition. <https://people.scs.carleton.ca/~paulv/toolsjewels.html>

Bibliografía complementaria:

- Mark Stamp (2022) Information Security: principles and practice, Third Edition. Wiley.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991010618636406709
- Adam Shostack (2014) Threat Modeling. Designing for security. John Wiley & Sons.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010486872806709
- Xabiel García Pañeda, David Melendi Palacio (2008) La peritación informática, un enfoque práctico, Colegio Oficial de Ingenieros en Informática Principado de Asturias.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991007440409706709
- Vicens Torra (2022) Guide to data privacy : models, technologies, solutions. Springer.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010721333006709
- Wenliang Du (2021) Computer Security. A Hands-on Approach. Third Edition.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010604568906709
- Matt Bishop (2019) Computer Security: Art and Science, Second Edition. Addison-Wesley.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991010604569006709
- Dieter Gollmann (2011) Computer Security, 3rd Edition. John Wiley & Sons.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991004205279706709
- Michael Sikorski, Andrew Honig (2012) Practical Malware Analysis. The hands-on guide to dissecting malicious software. No Starch Press.
https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010489658406709

Software

Dada la multidisciplinaridad de esta asignatura se utilizarán diferentes herramientas y lenguajes de programación dependiendo de la actividad concreta a realizar, tanto para las prácticas como por las actividades y ejercicios. Se utilizan lenguajes de programación como Python, o C, y diferente software y herramientas de sistemas.

Grupos e idiomas de la asignatura

La información proporcionada es provisional hasta el 30 de noviembre. A partir de esta fecha, podrá consultar el idioma de cada grupo a través de este [enlace](#). Para acceder a la información, será necesario introducir el CÓDIGO de la asignatura

Tipo de docencia	Grupo	Idioma	Semestre	Turno
(TE) Teoría	450	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PAUL) Prácticas de aula	451	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	451	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PAUL) Prácticas de aula	452	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	452	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PAUL) Prácticas de aula	453	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	453	Catalán/Español	segundo cuatrimestre	mañana-mixto

(PLAB) Prácticas de laboratorio	454	Catalán/Español	segundo cuatrimestre	mañana-mixto
(PLAB) Prácticas de laboratorio	455	Catalán/Español	segundo cuatrimestre	mañana-mixto