Garantía de la Información y Seguridad

Código: 102757
Créditos ECTS: 6

2024/2025

Titulación	Tipo	Curso
2502441 Ingeniería Informática	OB	3
2502441 Ingeniería Informática	OT	4

Contacto

Nombre: Guillermo Navarro Arribas

Correo electrónico: guillermo.navarro@uab.cat

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 Tecnologias de la Información y Metodología de la Programación.

Objetivos y contextualización

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.

Competencias

Ingeniería Informática

- Adquirir hábitos de pensamiento.
- Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.
- Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
- Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes.
- 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.
- 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.
- Trabajar en equipo.

Resultados de aprendizaje

1. Colaborar en el diseño y seguimiento de las políticas de seguridad de sistemas informáticos.
2. Comprender y aplicar los principios de seguridad en la elaboración y ejecución de planes de actuación.
3. Conocer los principios de la informática forense y del tratamiento de los delitos informáticos.
4. Conocer y comprender las posibilidades técnicas de implantación de políticas de seguridad en sistemas distribuidos.
5. Desarrollar un pensamiento y un razonamiento crítico.
6. Determinar los requisitos de seguridad y confidencialidad, así como identificar los principales tipos de ataques y amenazas.
7. Determinar los requisitos de seguridad y cumplimiento de la normativa y la legislación vigente en los sistemas de información y comunicación de una organización.
8. Diseñar sistemas de protección de la información: control de acceso e integridad.
9. Trabajar cooperativamente.

Contenido

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

En esta asignatura se ven mecanismos concretos de seguridad para el diseño de sistemas de protección de la información, control de acceso e integridad. Se estudia también una visión global de la seguridad, gestión de amenazas, técnicas de modelado de amenazas, gestión de riesgos, y se introducen disciplinas como la informática forense y pericial. Cabe destacar que el orden en el que se tratarán los temas puede variar respecto a lo estipulado en esta guía por motivos de planificación docente.

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Sesiones de laboratorio	12	0,48	1, 2, 3, 4, 5, 7, 6, 8, 9
Sesiones de problemas	12	0,48	1, 2, 3, 4, 5, 7, 6, 8, 9
Sesiones de teoria	26	1,04	1, 2, 3, 4, 5, 7, 6, 8
Tipo: Supervisadas			

Trabajo tutorizado	18	0,72	1, 2, 3, 4, 5, 7, 6, 8
Tipo: Autónomas			
Preparación y estudio de las pruebas de evaluación	30	1,2	1, 2, 3, 4, 5, 7, 6, 8
Preparación y estudio del trabajo autónomo de prácticas y problemas	45	1,8	1, 2, 3, 4, 5, 7, 6, 8, 9

La asignatura se desarrolla en 50 horas de actividades dirigidas repartidas en sesiones de teoría, de problemas y de 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 (de teoría, problemas y laboratorio), y una parte no supervisada que el alumnado realizará de manera autónoma.

De forma más concreta las actividades dirigidas son:

- Sesiones de teoría: clases realizadas en las sesiones de teoría donde el profesorado suministrará información sobre los conocimientos de la asignatura y sobre estrategias para adquirir, ampliar y organizar estos conocimientos. Estas sessiones pueden incluir sessiones impartidas por profesionales del ámbito de la seguridad informática en forma de seminarios.
- Sesiones de problemas: donde se plantean unos problemas o actividades que el alumnado deberá desarrollar en grupo o individualmente (depent de la actividad concreta). Este trabajo puede constar de una parte de trabajo supervisado y una parte de trabajo autónomo.
- 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. Esto incluye la publicación de materiales, publicación de notas parciales, foro de discusión, entrega de trabajos, ...

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
Problemas, ejercicios, y actividades	15%	2	0,08	1, 2, 3, 4, 5, 7, 6, 8, 9
Pruebas individuales	45%	3	0,12	1, 2, 3, 4, 5, 7, 6, 8
Prácticas laboratorio	40%	2	0,08	1, 2, 3, 4, 5, 7, 6, 8, 9

Las actividades de evaluación se dividen en actividades individuales y colectivas tanto de carácter práctico como teórico. Estas actividades se llevarán a cabo a lo largo del curso de forma continua.

Evaluación final y calificaciones:

Sobre la evaluación continua 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 será de 4.5 sobre 10.
- Evaluación de prácticas en el laboratorio. La nota mínima exigida de cada una de las prácticas será de 4.5 sobre 10.
- Evaluación de problemas/actividades (trabajo realizado fuera del aula o en las sesiones de clase correspondientes). 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 debido a que alguna de las actividades de evaluación no llega a la nota mínima requerida, la nota numérica del expediente será el menor valor 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.

Otorgar una calificación de matrícula de honor es decisión del profesorado responsable de la asignatura. La normativa de la UAB indica que las MH solo podrán concederse a estudiantes que hayan obtenido una calificación final igual o superior a 9.00. Puede otorgarse hasta un 5% de MH del total de estudiantes matriculados.

Recuperaciónde notas de la evaluación continua:

Se realizará un examen final de recuperación que permitirá recuperar los exámenes parciales. Asimismo, se permitirá una entrega final para recuperar aquellas prácticas suspendidas (esta entrega adicional comportará una penalización en la nota final de la práctica). La parte de problemas y actividades que no requiere nota mínima no podrá recuperarse.

El estudiante puede presentarse a la recuperación siempre que se haya presentado a un conjunto de actividades que representen un mínimo de dos terceras partes de la calificación total de la asignatura.

Convalidaciones parciales al alumnado repetidor:

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

Fechas de actividades de evaluación:

Las fechas de evaluación continua 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, puesto que se entiende que es el mecanismo habitual de intercambio de información entre el profesorado y el alumnado.

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

Procedimiento de revisión de las calificaciones

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 realizar 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 esta actividad.

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., Copiloto, 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 por lo general trabajos con elementos no originales y exclusivos del estudiante;
- tener dispositivos de comunicación (como teléfonos móviles, smart watches, bolígrafos con cámara, etc.) accesibles durante las pruebas de evaluación teórico-prácticas individuales (exámenes);
- hablar con compañeros durante las pruebas de evaluación teórico-prácticas individuales (exámenes);
- copiar o intentar copiar de otros alumnos durante las pruebas de evaluación teórico-prácticas (exámenes);
- usar o intentar utilizar escritos relacionados con la materia durante la realización de las pruebas de evaluación teórico-prácticas (exámenes), 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 o la estudiante haya cometido irregularidades en un acto de evaluación (y, por tanto, no será posible el aprobado por compensación). En futuras ediciones 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.

Evaluación única

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

- Examen individual: examen individual específico para alumnado de evaluación única sobre el contenido de la asignatura, 50% sobre la calificación final.
- Prácticas: entrega y validación de las prácticas que se propondrán de forma específica para alumnado deevaluación única, 50% sobre la calificación final.

Se aplicará el mismo sistema de recuperación que en el caso de la evaluación continua pero respecto a las actividades de evaluación única. La revisión de la calificación final sigue el mismo procedimiento que por la evaluación continua.

Bibliografía

Bibliografia 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

Bibliografia 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
- Vicenç 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 multidiciplinaridad 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.

Lista de idiomas

Nombre	Grupo	Idioma	Semestre	Turno
(PAUL) Prácticas de aula	451	Catalán/Español	segundo cuatrimestre	manaña-mixto
(PAUL) Prácticas de aula	452	Catalán/Español	segundo cuatrimestre	manaña-mixto
(PLAB) Prácticas de laboratorio	451	Catalán	segundo cuatrimestre	manaña-mixto
(PLAB) Prácticas de laboratorio	452	Catalán	segundo cuatrimestre	manaña-mixto
(PLAB) Prácticas de laboratorio	453	Catalán	segundo cuatrimestre	manaña-mixto
(PLAB) Prácticas de laboratorio	454	Catalán	segundo cuatrimestre	manaña-mixto
(PLAB) Prácticas de laboratorio	455	Catalán	segundo cuatrimestre	manaña-mixto
(TE) Teoría	450	Catalán/Español	segundo cuatrimestre	manaña-mixto