Universitat Autònoma de Barcelona

2020/2021

Garantía de la Información y Seguridad

Código: 102757
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2502441 Ingeniería Informática	OB	3	2
2502441 Ingeniería Informática	OT	4	2

La metodología docente y la evaluación propuestas en la guía pueden experimentar alguna modificación en función de las restricciones a la presencialidad que impongan las autoridades sanitarias.

Contacto

Nombre: Guillermo Navarro Arribas
Correo electrónico: Guillermo.Navarro@uab.cat

Uso de idiomas

Lengua vehicular mayoritaria: catalán (cat)
Algún grupo íntegramente en inglés: No
Algún grupo íntegramente en catalán: Sí
Algún grupo íntegramente en español: No

Equipo docente

Jordi Casas Roma

Prerequisitos

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
- Informática forense y pericial
- Ingeniería social

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.

Metodología

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, ...

Actividades

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

Evaluación

La evaluación se hará en base al seguimiento del alumnado durante la asignatura. Se divide principalmente en dos bloques:

- Evaluación individual: evidencias concretas sobre el contenido de la asignatura y evaluación del trabajo supervisado de forma individual. Aunque puede haber una parte de evaluación de carácter práctico, se trata mayoritariamente de trabajo teórico.
- Evaluación colectiva: consta mayoritariamente de la evaluación del trabajo supervisado tanto a nivel teórico como práctico.

Como se puede ver, las actividades de evaluación se dividen en pruebas individuales y colectivas tanto de carácter práctico como de carácter teórico. Las pruebas individuales se llevarán a cabo a lo largo del curso de forma continuada. Aún así se prevé la realización de una prueba final que permita recuperar las pruebas parciales de evaluación individual.

Evaluación final:

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 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 del trabajo supervisado (trabajo realizado fuera del aula) y problemas o actividades en las sesiones de problemas. 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 sobre 10.

En caso de no superar la asignatura debidoa que alguna de las actividades de evaluación no alcanza 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.

La calificación de "matrícula de honor" se otorgará al alumnado con nota igual o superior a 9 por orden de mejor nota final.

Recuperación de notas de la evaluación continua:

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

Convalidaciones parciales al alumnado repetidor:

Inicialmente no se plantea la posibilidad de convalidar partes de la asignatura, ni la realización de pruebas de síntesis especiales al alumnado repetidor. Sin embargo este hecho se puede reconsiderar a comienzo 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 possibles incidencias. Siempre se informará en el campus virtual sobre estos cambios ya que se entiende es el mecanismo habitual de intercambio deinformación entre el profesorado y el alumnado.

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

Para cada actividad de evaluación, se indicará un lugar, fecha y hora de revisión en la que el estudiante podrá revisar la actividad con el profesor. En este contexto, se podrán hacer 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 el alumnado que puedan conducir a una variación de la calificación, 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 otros:

- la copia total o parcial de una práctica, informe, o cualquier otra actividad de evaluación;
- dejar copiar;
- presentar un trabajo de grupo no hecho íntegramente por los miembros del grupo;
- 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, etc.) accesibles durante las pruebas de evaluación teórico-prácticas individuales (exámenes).

La nota numérica del expediente será el valor menor entre 3.0 y la media ponderada de las notas en caso de que el estudiante haya cometido irregularidades en un acto de evaluación (y por tanto no será posible aprobar la asignatura por compensación).

Actividades de evaluación

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

Bibliografía

De manera orientativa se da la siguinete bibliografia para la asignatura:

- Mark Stamp (2011) Information Security: principles and practice, 2n Edition. John Wiley & Sons.
- Adam Shostack (2014) Threat Modeling. Designing for security. John Wiley & Sons.
- Xabiel García Pañeda, David Melendi Palacio (2008) La peritación informática, un enfoque práctico, Colegio Oficial de Ingenieros en Informática Principado de Asturias.
- Vicenç Torra (2017) Data Privacy: Foundations, New Developments and the Big Data Challenge. Springer.
- Peter Szor (2005) The Art of Computer Virus Research and Defense. Adisson-Wesley.
- Wenliang Du (2017) Computer Security. A Hands-on Approach
- Matt Bishop (2002) Computer Security: Art and Science, Addison-Wesley.
- Dieter Gollmann (2011) Computer Security, 3rd Edition. John Wiley & Sons