Protección de datos y ciberseguridad

Curso Académico: (2022 / 2023) **Fecha de revisión: 26-05-2022**

Departamento asignado a la asignatura: Departamento de Informática, Departamento de Ingeniería Telemática

Coordinador/a: CALLEJO PINARDO, PATRICIA

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 2 Cuatrimestre : 2

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción a la Ciberseguridad
2. Principios de Protección de Datos
3. Privacidad en Big Data
4. Gestión y Administración de la Seguridad
5. Aspectos Legales de la Protección de Datos

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

AF1. CLASES TEÓRICO-PRÁCTICAS. En ellas se presentarán los conocimientos que deben adquirir los alumnos. Estos recibirán las notas de clase y tendrán textos básicos de referencia para facilitar el seguimiento de las clases y el desarrollo del trabajo posterior. Se resolverán ejercicios, prácticas problemas por parte del alumno y se realizarán talleres y pruebas de evaluación para adquirir las capacidades necesarias.
AF2. TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.
AF3. TRABAJO INDIVIDUAL O EN GRUPO DEL ESTUDIANTE
AF8: TALLERES Y LABORATORIOS.
AF9: EXAMEN FINAL. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.
MD1: THEORETICAL CLASS. The professor will give in-class presentations, including computer and audiovisual aids in which the course¿s main concepts are developed. Additional materials and literature will also be provided in order to supplement the student¿s learning.
MD2: PRACTICAL CASES. Students will be required to resolve case studies, problems, etc. posed by the professor both individually and in groups.
MD3: TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.
MD6: PRÁCTICAS DE LABORATORIO. Docencia aplicada/experimental a talleres y laboratorios bajo la supervisión de un tutor.

SISTEMA DE EVALUACIÓN

E2: EXAMEN FINAL. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.
E1: EXAMEN PARCIAL.
CE: EVALUACIÓN CONTINUA. En ella se valorarán los trabajos, presentaciones, actuación en debates, exposiciones en clase, ejercicios, prácticas y trabajo en los talleres a lo largo del curso.
CE= Lab ABE+Lab Pilar+Presentaciones de MAGERIT+Extra
Extra= ejercicio de SDC + participación en DoS y continuidad de negocio + participación en clases normales y en el foro con preguntas, respuestas y comentarios
E1, E2, Lab ABE, Lab Pilar, MAGERIT Presentations y Extra se evalúan sobre 10 puntos.
Es preciso obtener un mínimo de 4 en E2 para aprobar la asignatura.

FM: Nota Final= 0.4*E2+0.6*(E1+CE+Extra)/4

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

BIBLIOGRAFÍA BÁSICA

- Alfred J. Menezes , Jonathan Katz , Paul C. van Oorschot , Scott A. Vanstone Handbook of Applied Cryptography (Discrete Mathematics and Its Applications), CRC Press, 1996
- Josep Domingo-Ferrer, David Sánchez, Jordi Soria-Comas Database Anonymization: Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections, Morgan & Claypool Publishers , 2017

RECURSOS ELECTRÓNICOS BÁSICOS

- Miguel A. Amutio, Javier Candau, Pepe Mañas . MAGERIT ¿ version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method: https://administracionelectronica.gob.es/pae_Home/dam/jcr:80b16a91-75b1-432d-ab23-844a12aab5fc/MAGERIT_v_3_book_1_method_PDF_NIPO_630-14-162-0.pdf