Criptografía y seguridad informática

Curso Académico: (2023 / 2024) **Fecha de revisión: 19-05-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 3 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Programación (Curso 1 / Cuatrimestre 1)
Matemática Discreta (Curso 1 / Cuatrimestre 2)
Estadística (Curso 2 / Cuatrimestre 1)
Desarrollo de software (Curso 2 / Cuatrimestre 2)

COMPETENCIAS Y RESULTADOS DEL APRENDIZAJE

¿ Conocer los fundamentos científicos y tecnológicos de la criptografía y de la seguridad en computadores
¿ Conocer y aplicar mecanismos y protocolos criptográficos y de autenticación
¿ Conocer y adquirir conciencia de los fundamentos legales y la regulación existente sobre privacidad y seguridad informática

OBJETIVOS

Los objetivos de esta asignatura son que el estudiante reconozca la importancia actual de la criptografía y de las tecnologías que permiten su tratamiento, los puntos débiles de éstas y las amenazas que sufren. Así mismo, el alumno debe terminar conociendo los principios, métodos y medios de los sistemas de seguridad de la información.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Fundamentos de seguridad en computadores
2. Fundamentos matemáticos de la criptografía
3. Mecanismos y protocolos criptográficos
4. Autenticación e Infraestructuras de clave pública
5. Aspectos legales

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

CLASES TEÓRICO-PRÁCTICAS. 1,75 ECTS con 100% presencialidad. 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 prueba de evaluación para adquirirlas capacidades necesarias.
TUTORÍAS. 0,25 ECTS con 100% presencialidad. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.
TRABAJO INDIVIDUAL O EN GRUPO DEL ESTUDIANTE. 3,75 ECTS con 0% presencialidad.
TALLERES Y LABORATORIOS. 0,25 ECTS con 100% presencialidad.

Metodología:
CLASE MAGISTRAL. Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporcionan los materiales y la bibliografía para complementar el aprendizaje de los alumnos.
PRÁCTICAS. Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.
TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor. Para asignaturas de 6 créditos se dedicarán 4 horas con un 100% de presencialidad.
PRÁCTICAS DE LABORATORIO. Docencia aplicada/experimental a talleres y laboratorios bajo la

supervisión de un tutor.

SISTEMA DE EVALUACIÓN

EXAMEN FINAL. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. El porcentaje de valoración varía para cada asignatura en un rango entre el 30% y el 60%.

EVALUACIÓN CONTINUA. En ella se valorarán los trabajos/prácticas a lo largo del curso. El porcentaje de valoración varía para cada asignatura en un rango entre el 40 y el 70 % de la nota final. Se podrá requerir la obtención de un rendimiento mínimo en el examen final.

En particular:
1. CONVOCATORIA ORDINARIA
1.1. EVALUACIÓN CONTINUA
La evaluación se basará en los siguientes criterios:
- Resolución de un caso práctico a lo largo del curso (obligatorio): 50%
- Examen parcial (obligatorio): 10%
- Presentación de un trabajo teórico (obligatorio): 10%
- Examen final (obligatorio): 30%
Se podrá valorar la asistencia y participación activa en clase para obtener puntuación adicional.

Para aprobar la asignatura se deben satisfacer dos condiciones:
- Obtener en el examen final una calificación igual o superior a 4 puntos sobre 10.
- Lograr, como suma de todas las partes, al menos 5 puntos sobre 10.

1.2. EVALUACIÓN NO CONTINUA
Esta alternativa se aplica si no se entrega alguno de los trabajos o exámenes planteados.
La evaluación se basará en los siguientes criterios:
- Examen final: 60%
Dicho examen final incluirá pruebas específicas para comprobar el conocimiento que debe haberse adquirido mediante la realización de los trabajos planteados.
Para aprobar la asignatura se debe satisfacer:
- Lograr al menos 5.0 puntos sobre 10.

CONVOCATORIA EXTRAORDINARIA
2.1. SI EL ESTUDIANTE SIGUIÓ EVALUACIÓN CONTINUA EN LA CONV. ORDINARIA
La evaluación se basará en los siguientes criterios:
- Se mantiene la nota obtenida en la evaluación continua en relación a los trabajos (70%)
- Examen final (obligatorio): 30%

Para aprobar la asignatura se deben satisfacer dos condiciones:
- Obtener en el examen final una calificación igual o superior a 4 puntos sobre 10.
- Lograr, como suma de todas las partes, al menos 5 puntos sobre 10.

2.2. EVALUACIÓN NO CONTINUA
Esta alternativa se aplica si no se entregó alguno de los trabajos planteados.
La evaluación se basará en los siguientes criterios:
- Examen final: 100
Dicho examen final incluirá pruebas específicas para comprobar el conocimiento que debe haberse adquirido mediante la realización de los trabajos planteados.
Para aprobar la asignatura se debe satisfacer:
- Lograr al menos 5.0 puntos sobre 10.

Peso porcentual del Examen Final:	30
Peso porcentual del resto de la evaluación:	70

BIBLIOGRAFÍA BÁSICA

- A.I. González-Tablas Ferreres y P. Martín González Recopilación de problemas de examen 2010-2015. Criptografía y Seguridad Informática, CopyRed, 2016
- C. Paar Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag, 2014

- J. PASTOR; M.A. SARASA; J.L. SALAZAR CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES. (2ª EDICIÓN), PRENSAS UNIVERSITARIAS DE ZARAGOZA.
- Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption , Random House LCC US .

- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.