ASIGNATURA DE GRADO:
TEORÍA DE LA INFORMACIÓN Y CRIPTOGRAFÍA BÁSICA

Curso 2017/2018

(Código de asignatura : 71024091)

NOMBRE DE LA ASIGNATURA	TEORÍA DE LA INFORMACIÓN Y CRIPTOGRAFÍA BÁSICA
CÓDIGO	71024091
CURSO ACADÉMICO	2017/2018
DEPARTAMENTO	SISTEMAS DE COMUNICACIÓN Y CONTROL
TÍTULO EN QUE SE IMPARTE	**GRADO EN INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN**
CURSO	CUARTO CURSO
PERIODO	SEMESTRE 1
TIPO	OPTATIVAS
	GRADO EN INGENIERÍA INFORMÁTICA
CURSO	CUARTO CURSO
PERIODO	SEMESTRE 1
TIPO	OPTATIVAS
Nº ECTS	6
HORAS	150.0
IDIOMAS EN QUE SE IMPARTE	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Esta guía presenta las orientaciones básicas que se requieren para el estudio de la asignatura de *Teoría de la información y criptografía básica*. Por esta razón se recomienda leer detenidamente esta guía antes de iniciar el estudio, con el objetivo de hacerse una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

Teoría de la información y criptografía básicaes una asignatura de seis créditos ECTS de carácter optativo que se imparte en el primer semestre del cuarto curso de carrera en la titulación de Grado en Ingeniería en Tecnologías de la Información dentro de la materia de *Seguridad y Auditoría de la Información*.

El objetivo esencial de la asignatura es adquirir los conocimientos fundamentales asociados a la teoría de la información y la criptografía, orientándolos a la comprensión de las técnicas y su implantación en proyectos tecnológicos. En este sentido, se analizan las propiedades de la información, los procedimientos de cifrado y sus aplicaciones prácticas.

La asignatura de *Teoría de la información y criptografía* básica se encuadra en la materia de *Seguridad y Auditoría de la Información*. Esta misma materia se compone además de otras dos asignaturas estrechamente relacionadas:

- *Procesamiento y herramientas de gestión de la seguridad de redes*, asignatura obligatoria del primer semestre de tercer curso.
- *Consultoría y auditoría*, que se cursa de forma optativa en el segundo semestre del tercer curso.

Esta asignatura es asimismo una extensión de la asignatura de *Seguridad*, que se imparte en tercer curso de la Ingeniería en Informática.

Las competencias educativas atribuidas a la asignatura de Teoría de la información y criptografía básica participan del conjunto de competencias de la materia en Seguridad y Auditoría. Específicamente la asignatura contribuye al desarrollo de las siguientes competencias generales y específicas, que son comunes a los dos grados en que se imparten.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR LA ASIGNATURA

Esta asignatura requiere de un conocimiento básico y las competencias adquiridas en materias cursadas previamente, como las relacionadas con redes, así como con lenguajes de programación. Asimismo requiere de los conocimientos de la asignatura obligatoria de la materia de Seguridad de tercer curso.

EQUIPO DOCENTE

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES **(Coordinador de Asignatura)**
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
DEPARTAMENTO	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	MARIA CAROLINA MAÑOSO HIERRO
Correo Electrónico	carolina@scc.uned.es
Teléfono	91398-7168
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
DEPARTAMENTO	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	ANGEL PEREZ DE MADRID Y PABLO
Correo Electrónico	angel@scc.uned.es
Teléfono	91398-7160
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
DEPARTAMENTO	SISTEMAS DE COMUNICACIÓN Y CONTROL

HORARIO DE ATENCIÓN AL ESTUDIANTE

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al alumnado disponer de los siguientes recursos:

- Tutores en los centros asociados. Los tutores serán los encargados del seguimiento y control de las pruebas que constituyen la evaluación continua del alumno.
- Tutorías presenciales o virtuales en el centro asociado correspondiente.
- Entorno Virtual. A través del curso virtual el equipo docente de la asignatura pondrá a disposición de los alumnos diverso material de apoyo al estudio, así como el enunciado del trabajo practico-teórico a distancia.
- Foros de discusión donde los estudiantes podrán plantear sus dudas para que sean respondidas por el profesorado de tutoría o por el propio equipo docente. Este recurso es el SOPORTE FUNDAMENTAL de la asignatura, y supone la principal herramienta de comunicación entre equipo docente y estudiante, así como éstos entre sí.
- Tutorías con el equipo docente: los lunes de 15:00 a 19:00 h para el periodo durante el que se desarrolla la asignatura.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

Las **competencias genéricas** se articulan en cuatro áreas competenciales y recogen los tres niveles especificados en los Descriptores de Dublín. En cuanto a la asignatura de *Teoría de información y criptografía básica* se concreta en:

- *Competencias cognitivas superiores*(G.2): selección y manejo adecuado de conocimientos, recursos y estrategias cognitivas de nivel superior apropiados para el afrontamiento y resolución de diversos tipos de tareas/problemas con distinto nivel de complejidad y novedad: Análisis y Síntesis. Aplicación de los conocimientos a la práctica Resolución de problemas en entornos nuevos o poco conocidos. Pensamiento creativo. Razonamiento crítico. Toma de decisiones.
- *Competencias en el uso de las herramientas y recursos de la Sociedad del Conocimiento*(G.5): Manejo de las TIC. Competencia en la búsqueda de información relevante. Competencia en la gestión y organización de la información. Competencia en la recolección de datos, el manejo de bases de datos y su presentación
- *Trabajo en equipo*(G.6). Trabajo en equipo desarrollando distinto tipo de funciones o roles. En la Sociedad del Conocimiento se presta especial atención a las potencialidades del trabajo en equipo y a la construcción conjunta de conocimiento, por lo que las competencias relacionadas con el trabajo colaborativo son particularmente relevantes.

En cuanto a las **competencias específicas**, se concreta para la asignatura de *Teoría de la información y criptografía básica*, las propias del bloque Común a la Rama de Informática y las del bloque específico de las Tecnologías de la Información.

- Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos. (BC.6)
- Capacidad de comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos. (BTEti.7)

Asimismo la asignatura concreta otras **competencias recomendadas** para títulos en la rama informática:

- Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.
- Capacidad para comprender y poder aplicar conocimientos avanzados de computación de altas prestaciones y métodos numéricos o computacionales a problemas de ingeniería.

La intensificación en la materia requiere un nivel medio, en algunas competencias medio-alto, para alcanzar un nivel considerado suficiente para poder participar con éxito en el ámbito de la seguridad, como elemento importante en los proyectos de ingeniería informática.

RESULTADOS DE APRENDIZAJE

El objetivo básico de la asignatura es dar una visión completa de los fundamentos básicos de la teoría de la información y la criptografía. Como resultado del estudio y aprendizaje de los contenidos de esta asignatura el alumnado será capaz de:

- Comprender las técnicas básicas sobre los procedimientos de difuminación de la información mediante cifrado mediante una revisión histórica de los diferentes métodos empleados hasta nuestro tiempo (RA4). Está relacionado con las competencias genéricas G.2 y específicas BC.6 mencionadas anteriormente.
- Analizar el funcionamiento de los algoritmos de secreto compartido (clave privada) y cifrado público, y las implicaciones más importantes de su utilización como por ejemplo la distribución segura de la clave compartida (RA5). Está relacionado con las competencias genéricas G.2, G.5, y específicas BC.6, BC.6, BTEti.7.
- Desarrollar proyectos de uso de las técnicas criptográficas mediante la arquitectura de seguridad criptográfica de Java e implementar procedimientos de seguridad basadas en los algoritmos criptográficos más comunes (RA7). Relacionado con las competencias generales G.5, G.6 y específicas BC.6, BTEti.7.

CONTENIDOS

1. Introducción a la Criptología

2. Conceptos Básicos.

3. Conceptos fundamentales de Teoría de la Información

4. Complejidad Algorítmica

5. Aritmética Modular

6. Curvas Elípticas en Criptografía

7. Aritmética Entera de Múltiple Precisión

8. Criptografía y Números Aleatorios

9. Criptografía Clásica

10. Cifrados por Bloques

10. Cifrados por Bloques

12. Cifrados Asimétricos

13. Funciones Resumen

14. Esteganografía

15. Pruebas de Conocimiento Cero

16. Protocolos de Comunicación Segura

17. Autenti¿cación, Certi¿cados y Firmas Digitales

18. PGP

19. Seguridad en Computadores

METODOLOGÍA

La metodología de estudio utiliza la tecnología de formación a distancia en cursos virtuales. En este entorno se trabajaran los contenidos teórico- prácticos cuya herramienta fundamental de comunicación será el curso virtual, utilizando la bibliografía básica y el material complementario. Esta actividad del alumno en el aula virtual corresponde aproximadamente a un 30% del tiempo total asignado al estudio de la asignatura.

El trabajo autónomo de estudio, junto con las actividades de ejercicios y pruebas de autoevaluación disponibles, bajo la supervisión del tutor, con las herramientas y directrices preparadas por el equipo docente, completará aproximadamente un 60% del tiempo de preparación de la asignatura. Por último esta asignatura tiene además programadas unas actividades de evaluación a distancia. Esta actividad formativa representa aproximadamente el 10% del tiempo dedicado a la asignatura.

En la siguiente tabla se muestra su relación con los resultados de aprendizaje y el porcentaje de forma esquemática.

Actividades formativas:	RA relacionados	Número de horas
Preparación estudio contenido teórico	RA4, RA5	30%
Desarrollo de actividades con carácter presencial o en línea (curso virtual)	RA7	10%
Trabajo autónomo	RA7	60%
	TOTAL:	100%

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen mixto
Preguntas test	10
Preguntas desarrollo	1
Duración del examen	120 (minutos)
Material permitido en el examen	Técnicas Criptográficas de Protección de Datos. FÚSTER, A. y Otros, Editorial RA-MA, 2004
Criterios de evaluación	La calificación del examen constituye la nota final
% del examen sobre la nota final	100
Nota mínima del examen para aprobar sin PEC	5
Nota máxima que aporta el examen a la calificación final sin PEC	10
Nota mínima en el examen para sumar la PEC	0
Comentarios y observaciones	

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	No hay.
Descripción	
Criterios de evaluación	
Ponderación de la PEC en la nota final	0
Fecha aproximada de entrega	
Comentarios y observaciones	

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?	
Descripción	La evaluación continua se realiza mediante la participación de los estudiantes en la asignatura y sus aportaciones en el transcurso de la misma.
Criterios de evaluación	
Ponderación en la nota final	10
Fecha aproximada de entrega	
Comentarios y observaciones	

¿Cómo se obtiene la nota final?

La calificación del examen constituye la nota final. Seguidaente se considerará la evaluación continua para matizarla-

BIBLIOGRAFÍA BÁSICA

CRIPTOGRAFIA Y SEGURIDAD EN COMPUTADORES
Versión 4-0.9.0
27 de mayo de 2011
MANUEL JOSE LUCENA LOPEZ

BIBLIOGRAFÍA COMPLEMENTARIA

LIBRO ACTUALMENTE NO PUBLICADO
ISBN(13):
Título: TÉCNICAS CRIPTOGRÁFICAS DE PROTECCIÓN DE DATOS (3ª)
Autor/es: Fuster, José María ;
Editorial: : RAMA

ISBN(13): 9788436249750
Título: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es: Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial: U.N.E.D.

RECURSOS DE APOYO Y WEBGRAFÍA

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:

- Esta guía y la guía didáctica de estudio de la asignatura.
- Distintos libros electrónicos gratuitos, algunos interactivos.
- Material desarrollado exprofeso para el curso por el equipo docente
- Pruebas prácticas de evaluación a distancia.

TUTORIZACIÓN EN CENTROS ASOCIADOS