Universidad de Alcalá

GUÍA DOCENTE

SEGURIDAD EN SISTEMAS DISTRIBUIDOS

Grado en Ingeniería de Computadores
Grado en Sistemas de Información
Grado en Ingeniería Informática

Universidad de Alcalá

Curso Académico 2019/2020

4º curso/2º Cuatrimestre

GUÍA DOCENTE

Nombre de la asignatura:	**Seguridad en Sistemas Distribuidos**
Código:	**580015**
Titulación en la que se imparte:	**Grado en Ingeniería de Computadores** **Grado en Ingeniería en Sistemas de Información** **Grado en Ingeniería Informática**
Departamento y Área de Conocimiento:	**Ciencias de la Computación**
Carácter:	**Optativa**
Créditos ECTS:	**6**
Curso:	**Cuarto Curso – Segundo Cuatrimestre**
Profesorado:	**Manuel Sánchez Rubio** **José Javier Martínez Herráiz**
Horario de Tutoría:	El horario de Tutorías se indicará el primer día de clase.
Idioma en el que se imparte:	**Español**

1A. PRESENTACIÓN

Los planes de estudios de los Grados en Ingeniería de Computadores y Sistemas de Información están estructurados en tres bloques de formación: Básica, Obligatoria y Optativa. Los bloques de formación básica y obligatoria cubren el cuerpo de conocimiento principal propuesto por los informes o guías curriculares: Computing Curricula: Computer Science 2001[CC 2001], Computing Curricula Software Engineering 2004 [SE 2004], Computing Curricula 2005; de ACM-IEEE, Computer Engineering de 2004 [CE 2004]; y la guía IS 2002, de la AIS [AIS 2002]. La materia de Seguridad en Sistemas Distribuidos se encuadra dentro del bloque de Formación Optativa, que consta de 57 ECTS para el grado en Ingeniería de Computadores y el grado en Ingeniería Informática y de 45 ECTS para el grado en Sistemas de Información. Los módulos y materias optativas, todas de 6 ECTS, entre las que se encuentra Seguridad en Sistemas Distribuidos, están diseñadas para intensificar la formación del alumno en materias específicas que complementan la formación básica y obligatoria.

La proliferación de sistemas distribuidos y la computación ubicua ha conseguido altas cuotas de uso entre los sistemas informáticos, consiguiendo mayor rendimiento que los sistemas clientes servidor puro. Esta proliferación, y las características técnicas

propias de estos sistemas, dejan al descubierto una serie de necesidades para asegurar la privacidad de la información y la seguridad en su transmisión.

La asignatura Seguridad en Sistemas Distribuidos trata la seguridad en este tipo de sistemas desde el punto de vista matemático en cuanto a métodos de autenticación y cifrado, desde el punto de vista organizativo, a través de las normativas y estándares internacionales de ingeniería del software aplicado a seguridad, y desde el punto de vista legal para el ámbito nacional y supranacional, a través de la legislación vigente.

Prerrequisitos y Recomendaciones:

Para la asignatura de Seguridad en sistemas Distribuidos se recomienda haber superado la materia obligatoria: Redes.

1B. PRESENTATION

The curricula of Degrees in Computer Engineering and Information Systems are structured in three blocks of training: Basic, Mandatory and Optional. The blocks of basic and mandatory training covering the main body of knowledge propos ed by the reports or curriculum guides: Computing Curricula: Computer Science 2001 [CC 2001] Software Engineering Computing Curricula 2004 [SE 2004] Computing Curricula 2005; ACM-IEEE Computer Engineering 2004 [CE 2004]; and IS 2002, AIS [AIS 2002] guide. Matter Security in Distributed Systems falls within the block Optional Formation, consisting of 57 ECTS for degrees in Computer Engineering and Computer Science Engineering and 45 ECTS for the degree Information Systems. Modules and optional subjects, all of 6 ECTS, including Security in Distributed Systems, they are designed to enhance student´s training in specific areas that complement the basic and mandatory training.

The growth of distributed systems and ubiquitous computing has reached high use rates among computer systems, achieving higher performance than pure client-server systems. This growth, and these systems specific technical features, expose a series of needs to ensure information privacy and security in transmission.

The subject Security in Distributed Systems deals with security in this kind of systems from a mathematical point of view in terms of authentication and encryption methods, from an organizational point of view through regulations and international standards of software engineering applied to security, and from a legal point of view to the national and supranational scope throw actual legislation.

Prerequisites and Recommendations:

For Security in Distributed Systems subject it is recommended having passed the compulsory subject: Networks.

2. COMPETENCIAS

Competencias generales:

CG3 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.

Competencias específicas:

CSI5 Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.

CIC3 Capacidad de analizar y evaluar arquitecturas de computadores, incluyendo plataformas paralelas y distribuidas, así como desarrollar y optimizar software de para las mismas.

CIC4 Capacidad de diseñar e implementar software de sistema y de comunicaciones.

CIC6 Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

CC3 Capacidad para evaluar la complejidad computacional de un problema, conocer estrategias algorítmicas que puedan conducir a su resolución y recomendar, desarrollar e implementar aquella que garantice el mejor rendimiento de acuerdo con los requisitos establecidos.

CSI2 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.

CSI5 Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.

CTI7 Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Resultados del aprendizaje

. Al terminar con éxito la asignatura Seguridad en Sistemas Distribuidos, los estudiantes serán capaces de:

- RA1 Describir y conocer los fundamentos actuales de los criptosistemas de clave privada y pública así como su utilización para conseguir secreto, integridad, autenticidad, no repudio y disponibilidad.
- RA2 Evaluar la seguridad de un sistema de gestión de la información en un entorno distribuido.

- RA3 Explicar los métodos técnicos para asegurar un entorno distribuido.
- RA4 Saber aplicar los estándares de seguridad de la información y la privacidad en el diseño y uso de los sistemas distribuidos.
- RA5 Identificar las particularidades legales y éticas del tratamiento de la información.

3. CONTENIDOS

1. Bloque I: Seguridad:
    a. Introducción a la seguridad
    b. Sistemas de cifrado clásicos
    c. Sistemas de clave secreta
    d. Sistemas de clave asimétrica
2. Bloque II: Tecnología de seguridad: implementación
    a. Redes anónimas: TOR
    b. Redes DMZ
    c. IDS / IPS
    d. Hacking en Fuentes abiertas
    e. Ataques de suplantación de identidad
3. Bloque III: Estandarización para la seguridad en los sistemas informáticos y su aplicación a sistemas distribuidos
    a. ISO27000
        i. Sistema de gestión de la seguridad de la información
        ii. Auditorías y certificación
        iii. Puntos de control
4. Bloque IV: Normativa y legislación
    a. Legislación sobre Protección de Datos: aplicabilidad y requisitos
    b. Legislación sobre seguridad:
        i. Esquema nacional de seguridad
        ii. Esquema nacional de interoperabilidad
        iii. Plan de infraestructuras críticas
    c. Legislación sobre comercio electrónico

Programación de los contenidos

Unidades temáticas	Temas	Total horas, clases, créditos o tiempo de dedicación (*)
Seguridad con base matemática	• Sistemas de cifrado clásicos • Sistemas de clave secreta • Sistemas de clave asimétrica	12h
Tecnología de seguridad	• Redes anónimas: TOR • Redes DMZ • IDS / IPS • Hacking en Fuentes abiertas • Ataques de suplantación de identidad	27h
Estandarización	• CMM-SSE • ISO27000	6h
Normativa y legislación	• Legislación sobre Protección de Datos: aplicabilidad y requisitos • Legislación sobre seguridad: ENS, ENI, PNIC • Legislación sobre comercio electrónico	11h

(*) incluye PEC (pruebas de evaluación continua)

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE. ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

La asignación de horas a las distintas actividades formativas, incluyendo los exámenes es la siguiente:

Número de horas presenciales	56 horas + 4 horas de examen de evaluación
Número de horas del trabajo propio del estudiante:	90 horas
Total horas	150 horas

4.2. Estrategias metodológicas, materiales y recursos didácticos

La asignatura Seguridad en Sistemas Distribuidos se organiza como una asignatura cuatrimestral de 6 ECTS (150 horas).

En el proceso de enseñanza-aprendizaje de los contenidos anteriormente reseñados se emplearán las siguientes actividades formativas:

- Clases Teóricas presenciales.
- Clases Prácticas: resolución de problemas presenciales.
- Prácticas en Laboratorio presenciales.
- Tutorías: individuales y/o grupales.

Además, en función de la naturaleza de las distintas partes de la materia objeto de estudio, se podrán utilizar, entre otras, las siguientes actividades formativas:

- Elaboración de trabajos con responsabilidad individual pero con gestión de la información como equipo.
- Puesta en común de la información, problemas y dudas que aparezcan en la realización de los trabajos.
- Organización y realización de jornadas públicas con presentaciones orales y discusión de resultados.
- Utilización de Plataforma de Aula Virtual.

Actividades presenciales:

1. En el aula: exposición y discusión de los conocimientos básicos de la asignatura. Planteamiento y resolución teórica de ejercicios y supuestos relacionados.
2. En el laboratorio: planteamiento y desarrollo de ejercicios prácticos que permitan solventar problemas y analizar hipótesis y contribuyan al desarrollo de la capacidad de análisis de resultados, razonamiento crítico y comprensión de los métodos de resolución planteados, así como su implementación práctica.

Actividades no presenciales:

1. Análisis y asimilación de los contenidos de la materia, resolución de problemas, consulta bibliográfica, preparación de trabajos individuales y grupales, y autoevaluaciones. Orientadas especialmente al desarrollo de métodos para la auto-organización y planificación del trabajo individual y en equipo.
2. Tutorías: asesoramiento individual y en grupos durante el proceso de enseñanza-aprendizaje, bien en forma presencial o a distancia.

Materiales y recursos

- Software para el desarrollo de pruebas sobre los conceptos matemáticos
- Software de servidor web.
- Software para la gestión y generación de certificados.
- Herramientas de programación para la creación de programas de utilidad para la realización de prácticas sobre los sistemas utilizados

- Bibliografía de referencia
- Ordenadores personales
- Conexión a Internet y Plataforma de Aula Virtual
- Proyectores

5. EVALUACIÓN

El sistema de evaluación de la asignatura se ajustará al RD 1125/2003 por el cual se regula el sistema de créditos ECTS. Los estudiantes se acogerán a los procedimientos de evaluación según lo articulado en el título 2 (art. 9 y 10) de la Normativa de Evaluación de los Aprendizajes de la UAH aprobada en su Consejo de Gobierno de 24 de marzo de 2011.

La evaluación de la adquisición de competencias tendrá en cuenta la actitud y el interés del alumno. Preferentemente se ofrecerá a los alumnos un sistema de evaluación continua que tenga características de evaluación formativa, de manera que sirva de realimentación en el proceso de enseñanza-aprendizaje por parte del alumno. Para ello se establecen los siguientes:

Procedimientos

1. Convocatoria ordinaria La evaluación en la convocatoria ordinaria debe estar inspirada en los criterios de Evaluación continua (Normativa de Regulación de los Procesos de Enseñanza Aprendizaje, NRPEA, art 3), atendiendo siempre a la adquisición de las competencias especificadas en la asignatura.

> *Evaluación Continua*: Consistente en la realización y superación de las prácticas de laboratorio, la realización y superación de los trabajos y actividades de la asignatura, y la realización y superación de exámenes. La superación de las prácticas, de los trabajos de la asignatura y de los exámenes se realizará a lo largo del cuatrimestre.

Para poder aprobar la Evaluación Continua el alumno debe entregar las actividades de aprendizaje propuestas y presentarse a las evaluaciones en las fechas establecidas.

2. Evaluación Final. Aquellos alumnos que presenten solicitud por escrito al Director de la Escuela y tengan una causa justificada, podrán ser evaluados mediante evaluación final. Esta evaluación constará de un examen final para acreditar que han adquirido la totalidad de las competencias descritas en esta guía docente y entregaran un trabajo práctico final. Esta evaluación constituirá el 100% de la nota de la asignatura. Para acogerse al proceso de evaluación final, el alumno debe solicitarlo por escrito al director del centro en las dos primeras semanas de su incorporación, indicando las razones que impiden seguir el sistema de evaluación continua.

3. Evaluación Extraordinaria. En la convocatoria extraordinaria, los alumnos que no hayan superado la convocatoria ordinaria realizarán un examen final para acreditar que han adquirido la totalidad de las competencias descritas en esta guía docente y entregaran un trabajo práctico final, con una distribución de la puntuación y estructura similar a las pruebas de evaluación final de la convocatoria ordinaria. Estas pruebas constituirán el 100% de la nota de la asignatura.

La dimensión y cuestiones que serán valoradas en el aprendizaje se corresponden a la adquisición de competencias presentadas en la guía. En todos los procedimientos de evaluación los problemas servirán para evaluar la adquisición de las competencias relativas a la capacidad para la resolver problemas y casos de la asignatura. Las cuestiones teóricas permiten evaluar la adquisición de competencias en la comprensión y dominio de los conceptos básicos, y del conocimiento aplicado. Con los trabajos y problemas de laboratorio se evalúa la adquisición de la competencia sobre el uso de software específico. Se evaluará la capacidad del alumno para resolver problemas con iniciativa, toma de decisiones, creatividad, razonamiento crítico. Además, la evaluación de la adquisición de competencias tendrá en cuenta los siguientes criterios de evaluación:

- Utilizar terminología especifica.
- Capacidad para gestionar problemas en entornos determinados.
- Responsabilidad en la realización de las tareas.
- Desarrollo de actitudes para el trabajo colaborativo.
- Capacidad para desarrollar soluciones eficientes con los modelos disponibles.
- Adaptación a los cambios de requisitos en la administración y planificación de un sistema de seguridad.

Criterios de Evaluación

Los Criterios de Evaluación deben atender al grado de adquisición de las competencias por parte del estudiante. Para ello se definen los siguientes:

CE1: El alumno muestra capacidad de describir y conocer los fundamentos actuales de los criptosistemas de clave privada y pública así como su utilización para conseguir secreto, integridad, autenticidad, no repudio y disponibilidad.

CE2: El alumno demuestra que es capaz de de evaluar la seguridad de un sistema de gestión de la información en un entorno distribuido.

CE3: El alumno ha adquirido los conocimientos técnicos para explicar los métodos técnicos para asegurar un entorno distribuido.

CE4: El alumno muestra capacidad de describir y conocer los estándares de seguridad de la información y la privacidad en el diseño y uso de los sistemas distribuidos.

CE5: El alumno puede identificar las particularidades legales y éticas del tratamiento de la información.

Instrumentos de evaluación.

Esta sección indica los instrumentos de evaluación que serán aplicados a cada uno de los criterios de Evaluación.

1. Pruebas de Evaluación Continua (PEC1): Bloque I y Bloque II.
2. Pruebas de Evaluación Continua (PEC2): Participación en conferencias programadas.
3. Trabajos prácticos de la asignatura (TPA): Uno para los bloques I y II. TPA 1 y uno para los bloques III y IV. TPA 2
4. Prueba Práctica de Evaluación Final (PPEF)
5. Prueba de Evaluación Final (PEF)

Criterios de Calificación

Convocatoria Ordinaria: Evaluación Continua

En la convocatoria ordinaria – evaluación continua la relación entre los criterios, instrumentos y calificación es la siguiente.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CIS5, CIC3, CIC4, CIC6, CC3, CSI2, CSI5, CTI7	RA1, RA2, RA3, RA4, RA5	CE1, CE2, CE3	PEC 1	30%
		CE1-CE5	PEC 2	30%
		CE1, CE2, CE3	TPA1	20%
		CE2, CE4, CE5	TPA2	20%

Convocatoria Ordinaria: Evaluación Final

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CIS5, CIC3, CIC4, CIC6, CC3, CSI2, CSI5, CTI7	RA1, RA2, RA3, RA4, RA5	CE1-CE5	PPEF	70%
		CE1-CE5	PEF	30%

Convocatoria Extraordinaria

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CIS5, CIC3, CIC4, CIC6, CC3, CSI2, CSI5, CTI7	RA1, RA2, RA3, RA4, RA5	CE1-CE5	PPEF	70%
		CE1-CE5	PEF	30%

6. BIBLIOGRAFÍA

Bibliografía Básica

- B.Schneier. Applied cryptography. Protocols, Algoritms and Source code in C.J.Wiley & Sons,Inc. EEUU 1994. ISBN:0-471-59756-2
- A. Gómez Vieites. Enciclopedia de la seguridad informática. Ra-Ma 2006 ISBN: 84-7897-731-7
- A. Fuster. Técnicas criptográficas de protección de datos. Ra-Ma.

Bibliografía Complementaria

- Estándares ISO27000 (Biblioteca)
- Legislación actualizada (Biblioteca/BOE/ http://administracionelectronica.gob.es)