Universidad de Alcalá

GUÍA DOCENTE

Seguridad en Sistemas Distribuidos

Grado en
Ingeniería en Sistemas de Información (GISI)
Ingeniería de Computadores (GIC)
Ingeniería Informática (GII)

Universidad de Alcalá

Curso Académico 2022/2023

4º Curso - 1er Cuatrimestre (GISI+GIC+GII)

Aprobada en Junta de Escuela el día 3 de junio de 2022

GUÍA DOCENTE

Nombre de la asignatura:	**Seguridad en Sistemas Distribuidos**
Código:	**580015 (GISI+GIC+GII)**
Titulación en la que se imparte:	**Grado en** **Ingeniería en Sistemas de Información (GISI)** **Ingeniería de Computadores (GIC)** **Ingeniería Informática (GII)**
Departamento y Área de Conocimiento:	**Ciencias de la Computación** **Ciencias de la Computación**
Carácter:	**Optativa (Genérica) (GISI+GIC+GII)**
Créditos ECTS:	**6.0**
Curso y cuatrimestre:	**4º Curso - 1er Cuatrimestre (GISI+GIC+GII)**
Profesorado:	Manuel Sánchez Rubio José Javier Martínez Herráiz
Horario de Tutoría:	Consultar al comienzo de la asignatura
Idioma en el que se imparte:	Español

1a. PRESENTACIÓN

Los planes de estudios de los Grados en Ingeniería Informática, Ingeniería de Computadores e Ingeniería de 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 Informática y de Computadores y de 45 ECTS para el grado en Sistemas de Información. En los tres grados, para obtener 45 créditos se podrán obtener con una combinación de módulos y materias optativas, un mínimo de 30 ECTS; prácticas externas, un máximo de 15 ECTS; créditos obtenidos mediante el programa de bonocréditos, un máximo de 9 ECTS. Y para el grado en Ingeniería de Computadores los 12 grados restantes se obtendrán a través de materias transversales definidas para toda la universidad. 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. COURSE SUMMARY

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 45 ECTS for the degree Information Systems. In the two degrees, to obtain 45 credits may be obtained with a combination of modules and electives, a minimum of 30 ECTS; external practices, a maximum of 15 ECTS; Credits earned through the program bonocréditos, a maximum of 9 ECTS. And for Degree in Computer Engineering remaining 12 degrees were obtained through cross materials defined for the whole university. 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 básicas, generales y transversales.

Esta asignatura contribuye a adquirir las siguientes competencias básicas, generales y transversales:

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

Esta asignatura proporciona la(s) siguiente(s) competencia(s) específica(s):

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.

Resultados de aprendizaje

Al terminar con éxito esta asignatura/enseñanza, 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. Ser capaz de 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

Bloques de contenido	Total de clases, créditos u horas
Bloque I: Seguridad: Introducción a la seguridad Sistemas de cifrado clásicos Sistemas de clave secreta Sistemas de clave asimétrica	9 horas
Bloque II: Tecnología de seguridad: implementación Redes anónimas: TOR Hacking en Redes Sociales OSINT: Inteligencia en Fuentes Abiertas Ataques a infraestructuras críticas Criptomonedas y ciberdelitos: BITCOIN Fraudes en medios de pago Redes DMZ IDS / IPS Hacking en Fuentes abiertas Ataques de suplantación de identidad	38 horas
Bloque III: Estandarización para la seguridad en los sistemas informáticos y su aplicación a sistemas distribuidos ISO27000 Sistema de gestión de la seguridad de la información Auditorías y certificación Puntos de control	3 horas

Bloque IV: Normativa y legislación Legislación sobre Protección de Datos: aplicabilidad y requisitos Legislación sobre seguridad: Esquema nacional de seguridad Esquema nacional de interoperabilidad Plan de infraestructuras críticas Legislación sobre comercio electrónico	6 horas

4. METODOLOGÍAS DE ENSEÑANZA APRENDIZAJE. ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	58 horas (56 horas de clase presencial +2 horas de evaluación)
Número de horas del trabajo propio del estudiante:	92 (Incluye horas de estudio, elaboración de actividades, preparación de exámenes)
Total horas	150

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases magistrales y expositivas, en combinación con prácticas en el laboratorio y conferencias magistrales	**Clases Teóricas presenciales**. Exposición y discusión de los conocimientos de la asignatura. Planteamiento y resolución teórica de ejercicios y supuestos relacionados. Orientadas a la enseñanza de las competencias específicas de la asignatura, especialmente las relacionadas con los conocimientos básicos **Clases Prácticas**: . Análisis y asimilación de los contenidos de la materia, resolución de problemas, consulta bibliográfica, preparación de trabajos individuales y grupales. Orientadas especialmente al desarrollo de métodos para la autoorganización y planificación del trabajo individual y en equipo. **Prácticas en 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. Servirán como base para la adquisición de las competencias genéricas descritas. Con capacidad de hacerlas donde estime oportuno el alumno. **Conferencias magistrales.** Se organizaran clases magistrales de grandes referencias en la materia de Fuerzas y Cuerpos de Seguridad del Estado y organizaciones afines, como aporte adicional para el alumno **Tutorías**: individuales y/o grupales. Asesoramiento individual y/o en grupos durante el proceso de enseñanza-aprendizaje, bien en forma presencial o a distancia.
Trabajos en grupo y cooperativo	La asignatura dispone de dos trabajos a realizar, en el primero de ellos, sobre búsqueda en fuentes abiertas (OSINT) será de índole individual, el segundo, sobre vectores de ataque, se propone al alumno la capacidad de poder trabajar en grupo de forma cooperativa.
Trabajo y estudio personal	Análisis y asimilación de los contenidos de la materia, resolución de casos, consulta bibliográfica, preparación de trabajos individuales y grupales, realización de pruebas de evaluación presenciales y autoevaluaciones.

5. EVALUACIÓN: Procedimientos, criterios de evaluación y calificación

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.

5.1. PROCEDIMIENTOS

La evaluación debe estar inspirada en los criterios de evaluación continua (Normativa de Evaluación de

los Aprendizajes, NEA, art 3). No obstante, respetando la normativa de la Universidad de Alcalá se pone a disposición del alumno un proceso alternativo de evaluación final de acuerdo a la Normativa de Evaluación de los Aprendizajes según lo indicado en su Artículo 10, los alumnos tendrán un plazo de quince días desde el inicio del curso para solicitar por escrito al Director de la Escuela Politécnica Superior su intención de acogerse al modelo de evaluación no continua aduciendo las razones que estimen convenientes. La evaluación del proceso de aprendizaje de todos los alumnos que no cursen solicitud al respecto o vean denegada la misma se realizará, por defecto, de acuerdo al modelo de evaluación continua. El estudiante dispone de dos convocatorias para superar la asignatura, una ordinaria y otra extraordinaria.

Convocatoria ordinaria

Evaluación continua:

Puesto que la materia de la asignatura tiene, principalmente, una utilidad práctica en los entornos de seguridad y en ambientes de delitos informáticos, la evaluación se centrará en el desarrollo y verificación de los aspectos prácticos incluyendo la aplicación de los conceptos estudiados, su verificación práctica y el uso de distintos patrones de uso relacionado con la materia.

Siguiendo esa línea, las principales herramientas de evaluación serán:

1. **Entregables de Problemas (EP).** Resolución de problemas prácticos de forma individual o en grupos reducidos. Resolución de problemas prácticos de forma individual o en grupos reducidos.

2. **Entregables de Laboratorio (EL).** Realización de dos prácticas, una de carácter individual (OSINT) y una grupal (Vectores de ataque(con un valor de de laboratorio y entrega de las correspondientes memorias. La evaluación considerará la observación sistemática, donde el profesor registrará las principales dificultades y habilidades observadas en cada alumno, y la realización de una memoria única por práctica, por parte de cada uno de los grupos de alumnos que la hayan realizado.

3. **Pruebas de Evaluación (PE).** Realización de pruebas escritas centradas en los aspectos tanto prácticos como teóricos de la asignatura.
4. **Asistencia a conferencias magistrales (CM).** Se realizarán conferencias magistrales a través de expertos en la materia ya sea de Fuerzas y Cuerpos de Seguridad del Estado empresa privada y/o pública.

Los alumnos, en grupo, entregarán los informes de las prácticas de laboratorio siguiendo el calendario establecido. Estas prácticas serán evaluadas por el profesor responsable del grupo de laboratorio, para valorar si se han cumplido los objetivos indicados en el guion de la misma.

Evaluación mediante examen final:

En el caso de evaluación mediante examen final, los elementos de evaluación a emplear serán los siguientes:

1. **Prueba de laboratorio (PL).** Entrega de la práctica individual y la práctica grupal

2. **Prueba Evaluación Final (PEF).** Pregunta de desarrollo.
3. **Asistencia a conferencias magistrales (CM).**

Se recomienda a los alumnos que realicen las prácticas de laboratorio durante el desarrollo del cuatrimestre, sustituyendo de esta forma el examen práctico de laboratorio por la evaluación de las memorias correspondientes a las diferentes prácticas.

Convocatoria extraordinaria

El procedimiento será el mismo que el descrito para la evaluación mediante examen final en la convocatoria ordinaria.

5.2. EVALUACIÓN

CRITERIOS DE EVALUACIÓN

Se utilizarán los siguientes criterios para la evaluación de la asignatura, relacionados con los resultados del aprendizaje:

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 paraexplicar los métodos técnicos para asegurar un entorno distribuido.

CE4: El alumno muestra capacidad de describir y conocerlos 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 resume los instrumentos de calificación que serán aplicados a cada uno de los criterios de Evaluación.

- **Entregables de Problemas (EP):** Entregas de desarrollos y resolución de problemas tanto prácticos como teóricos.
- **Entregables de Laboratorio (EL):** Entregas de resultados y conclusiones de las prácticas propuestas a lo largo de la asignatura.
- **Prueba de Laboratorio (PL):** A realizar únicamente por los alumnos que opten por la evaluación final.
- **Prueba Evaluación (PE):** Prueba con una pregunta de desarrollo que coincidirá con la terminación de los bloques de temario en los que se divide la misma.
- **Prueba de Evaluación Final:** Una única prueba con las mismas características que las PE, pero que sólo deberán realizar aquellos alumnos que opten por la evaluación final.
- **Clases magistrales (CM).** Clases magistrales a cargo de expertos en ciberdelitos en Fuerzas y Cuerpos de Seguridad del Estado.

CRITERIOS DE CALIFICACIÓN

En la convocatoria **ordinaria–evaluación continua** la relación entre las competencias, resultados del aprendizaje, criterios e instrumentos de evaluación, 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%

Se otorgará la calificación de "No presentado" al alumno que habiendo optado por el procedimiento de evaluación continua, cumpla alguno de los siguientes requisitos:

- Cuando el alumno haya incumplido al menos la asistencia al 60% de las clases en grupos reducidos.
- Cuando el alumno no haya entregado, al menos el 60% de los trabajos solicitados.

En la convocatoria **ordinaria–evaluación final** la relación entre las competencias, resultados del aprendizaje, criterios e instrumentos de evaluación, 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-CE5	PPEF	70%
		CE1-CE5	PEF	30%

Convocatoria extraordinaria

En el caso de la convocatoria extraordinaria se mantendrán los mismos porcentajes que se han establecido en el caso de la evaluación mediante examen final, dando la opción de realizar la PL o de mantener la nota obtenida en las EL (evaluación continua) o en la PEF (evaluación final), según decisión del alumno. En cualquier caso, la PL la realizarán aquellos alumnos que no la hayan realizado en la opción de examen final en la convocatoria ordinaria.

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

6.1. Bibliografía básica

- Sanchez, M. , Barchino, R, Martínez, J, "Redes de Computadores", Ed. UAH
- Schneier. Applied cryptography. Protocols, Algoritms and Source code in C.J.Wiley & Sons,Inc. EEUU 1994. ISBN:0-471-59756-

- Gómez Vieites. Enciclopedia de la seguridad informática. Ra-Ma 2006 ISBN: 84-7897-731-7
- Fuster. Técnicas criptográficas de protección de datos. Ra-Ma.

6.2. Bibliografía complementaria

- Estándares ISO27000 (Biblioteca)
- Legislación actualizada (Biblioteca/BOE/

NOTA INFORMATIVA

La Universidad de Alcalá garantiza a sus estudiantes que, si por exigencias sanitarias las autoridades competentes impidieran la presencialidad total o parcial de la actividad docente, los planes docentes alcanzarían sus objetivos a través de una metodología de enseñanza-aprendizaje y evaluación en formato online, que retornaría a la modalidad presencial en cuanto cesaran dichos impedimentos.