Universidad de Alcalá

GUÍA DOCENTE

Seguridad

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

Universidad de Alcalá

Curso Académico 2019/2020

4º Curso – 2º Cuatrimestre

GUÍA DOCENTE

Nombre de la asignatura:	**Seguridad**
Código:	**780036**
Titulación en la que se imparte:	**Grado en Ingeniería en Sistemas de Información** **Grado en Ingeniería de Computadores** **Grado en Ingeniería Informática**
Departamento y Área de Conocimiento:	**Automática. Área de Ingeniería Telemática**
Carácter:	**Optativo**
Créditos ECTS:	**6**
Curso y cuatrimestre:	**4º, C2**
Profesorado:	Iván Marsá Maestre Susel Fernández Melián
Horario de Tutoría:	
Idioma en el que se imparte:	Español/English Friendly

1. PRESENTACIÓN

La información que se almacena en los equipos informáticos y que se intercambia entre estos a través de redes de comunicaciones, puede llegar a tener un gran valor para las personas, organizaciones y empresas. Por el hecho de estar disponible a través de una red de comunicaciones como Internet, puede estar accesible a una gran cantidad de personas, entre las que habrá un porcentaje de personas con malas intenciones. Esto hace que la información se vea sometida a una gran cantidad de amenazas y por lo tanto aumente el riesgo de ser perdida, modificada, falsificada u observada sin autorización, en actos que hoy conocemos como ciberdelincuencia o bien por fallos humanos, averías de equipos o accidentes. Por estos motivos, la seguridad de la información es un aspecto fundamental en la sociedad actual, y las capacidades necesarias para analizar el nivel de seguridad de la información y tomar las medidas de protección adecuadas, tienen un valor en fuerte demanda en el mundo empresarial.

Esta asignatura profundiza en los aspectos técnicos relacionados con la seguridad de la información, una vez que se han adquirido los conocimientos básicos que sustentan la tecnología que permite generar, intercambiar y almacenar dicha información, en las asignaturas de Arquitectura de redes I y Arquitectura de redes II.

La asignatura se estructura en cuatro grandes bloques en los que se tratarán tanto los aspectos teóricos como prácticos relacionados:

1. Seguridad de la Información, en donde se analizan los procedimientos criptográficos que permiten procesar la propia información para ocultarla o bien tener garantías de que no ha sido generada o modificada sin autorización.
2. Control de acceso, en donde se estudian los principales mecanismos que existen para prevenir el acceso a la información por personas o entidades no autorizadas y medidas para detectar intentos de acceso no autorizado.
3. Protocolos de seguridad: en donde se analizan las principales soluciones globales de seguridad que se usan para proteger la información en diferentes entornos clásicos, y que normalmente son una composición de mecanismos vistos en los bloques 1 y 2.

Seguridad de sistemas, en donde se analizan los principales ataques que se pueden producir contra los sistemas que almacenan y procesan la información, como pueden ser los ordenadores personales, smartphones o servidores y las diferentes aplicaciones que corren sobre estos, incidiendo en este aspecto en las metodologías para medir el nivel de seguridad de estos sistemas mediante un proceso de auditoría y análisis de riesgos.

1.b PRESENTATION

Information stored in computers and exchanged between them through communication networks may have great value for people, organizations and companies. Since it is available through a communications network such as the Internet, it can be accessible to a large number of people, among which there will be some with malicious intent. This means that the information is subject to a large number of threats and therefore increases the risk of being lost, modified or eavesdropped without authorization, in acts that we know today as cybercrime or human failures, equipment breakdowns or accidents. For these reasons, information security is a fundamental aspect of today's society, and the necessary capabilities to analyze the level of information security and take appropriate protection measures have a high demand in the business world.

This course delves into the technical aspects related to information security, once students have acquired the basic knowledge that supports the technology that allows generating, exchanging and storing information, in the Network Architecture I and Network Architecture II courses.

The course is structured in four parts:

1. Information Security, where the cryptographic procedures that allow processing the information itself to hide it or have guarantees that it has not been generated or modified without authorization are analyzed.
2. Access control, where the main mechanisms that exist to prevent access to information by unauthorized parties and mechanisms to detect attempts of unauthorized access are studied.
3. Security protocols: where the main global security solutions that are used to protect information in different classic environments are analyzed, usually a composition of mechanisms seen in parts 1 and 2.
4. System Security, where the main attacks that can occur against the systems that have and process information are analyzed, such as personal computers, smartphones or servers and the different applications that run on them, focusing in the methodologies to assess the level of security of these systems through an audit process.

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.

CG9 Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

CG10 Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática, de acuerdo con los conocimientos adquiridos según lo establecido en el apartado 5 de la resolución BOE-A-2009-12977.

CG11 Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática.

Competencias específicas;

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

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.

CIS5 Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.

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

Resultados del aprendizaje

Al término de la asignatura, el alumno habrá alcanzado los siguientes resultados de aprendizaje:

RA1	Utilizar mecanismos criptográficos para gestionar riesgos de seguridad de la información, evaluando las implicaciones de uso de los diferentes mecanismos disponibles.
RA2	Escoger y desplegar mecanismos de seguridad (controles) preventivos, de detección y reactivos sobre dispositivos y servicios de red, incluyendo cortafuegos, sistemas de detección de intrusiones y políticas de seguridad.

RA3	Valorar los riesgos de seguridad en un determinado sistema de información, de acuerdo con el inventario de activos del sistema y las amenazas y vulnerabilidades que le afectan.
RA4	Construir soluciones de seguridad aceptables en escenarios concretos, utilizando diferentes mecanismos criptográficos y aplicaciones de seguridad.
RA5	Recabar evidencias en incidentes de seguridad de sistemas, buscar información sobre las mismas y realizar el análisis y posterior comunicación de conclusiones como parte de un equipo de investigación.
RA6	Trabajar en equipo de forma colaborativa para la resolución de problemas relacionados con la seguridad en redes y sistemas y comunicar de manera eficaz sus conocimientos, procedimientos, resultados e ideas al respecto, tanto por escrito como de forma oral.

3. CONTENIDOS

Bloques de contenido (se pueden especificar los temas si se considera necesario)	Total de clases, créditos u horas
Seguridad de la Información: introducción; criptografía simétrica: DES, 3DES, AES; criptografía asimétrica: RSA, ECC; funciones hash, hmac.	16 horas (4 semanas)
Control de acceso: autenticación: passwords, inicio de sesión único (SSO), biometría, Autorización: listas de control de acceso (ACLs), modelos multinivel. Mecanismos: cortafuegos, sistemas de detección de Intrusiones (IDS).	12 horas (3 semanas)
Protocolos de Seguridad: protocolos de autenticación, autenticación mutua, ataques de hombre en el medio. Seguridad en los protocolos de Internet.	8 horas (2 semanas)
Seguridad de Sistemas: Vulnerabilidades y amenazas, análisis de vulnerabilidades. Software seguro: Escalada de privilegios, malware. Seguridad en Aplicaciones Web. Auditoría. Seguridad en Sistemas Operativos. Informática forense.	12 horas (3 semanas)

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE.-ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases en grupo reducido: 56 horas (4 horas x 14 semanas) Evaluación final: 4 horas. Total: 60 horas presenciales
Número de horas del trabajo propio del estudiante:	Preparación de las clases, aprendizaje autónomo, preparación de ejercicios, pruebas y prácticas, preparación de la prueba final: Total: 90 horas
Total horas	150 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases Presenciales	• Presentación y/o revisión de conceptos de carácter eminentemente práctico. • Resolución de problemas. • Sesiones prácticas de laboratorio: orientadas a consolidar los conceptos presentados previamente, así como a familiarizar al estudiante con las herramientas y metodologías de apoyo al estudio de la materia y futuro desempeño profesional (mejorar la comprensión de los conceptos de seguridad, detección de intrusiones, análisis de vulnerabilidades y puesta en marcha de medidas de seguridad). • Presentaciones orales y otras actividades. • Actividades de trabajo en grupo.
Tutorías individuales, grupales y vía web (foro, correo, etc.)	• Resolución de dudas. • Apoyo al aprendizaje autónomo.
Trabajo autónomo	• Lecturas. • Realización de actividades: ejercicios, búsqueda de información, análisis de datos.

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación

Procedimientos

El alumno dispone de dos convocatorias, una ordinaria y otra extraordinaria para la superación de la asignatura.

Convocatoria Ordinaria (Evaluación Continua y Evaluación Final)

En la convocatoria ordinaria, se distingues dos posibles vías para la evaluación: Evaluación Continua (EC) y Examen Final (EF). El alumno será evaluado preferentemente mediante el proceso descrito de evaluación continua. Para acogerse al proceso de examen final, el alumno debe solicitarlo por escrito al Director del centro en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del centro comunicará la resolución en un máximo de 15 días. En caso de no haber recibido respuesta, se considera estimada esta solicitud.

Convocatoria Extraordinaria

La convocatoria extraordinaria consistirá en una prueba similar al examen final.

Criterios de Evaluación

El alumno será evaluado de acuerdo con los siguientes criterios:

CE1	Conoce los diferentes mecanismos criptográficos explicados en la asignatura.
CE2	Es capaz de seleccionar, dado un escenario concreto de riesgos de seguridad de la información, el mecanismo criptográfico más adecuado conforme a unos requisitos de confidencialidad, integridad y disponibilidad dados.
CE3	Es capaz de evaluar, dado un escenario concreto de criptografía, las posibles vulnerabilidades que pueden aparecer.

CE4	Conoce las vulnerabilidades y amenazas más usuales en cuanto a seguridad de redes y sistemas.
CE5	Es capaz de realizar un inventario de activos de un sistema de información.
CE6	Es capaz de evaluar los riesgos de seguridad de un sistema de información, de acuerdo con el inventario de activos del sistema y la valoración de las amenazas y vulnerabilidades que le afectan.
CE7	Conoce los diferentes mecanismos de seguridad que pueden utilizarse para proteger un sistema de información, incluyendo cortafuegos, sistemas de detección de intrusiones y políticas de seguridad.
CE8	Es capaz de aplicar los diferentes mecanismos de seguridad (controles) preventivos, de detección y reactivos sobre dispositivos y servicios de red,
CE9	Es capaz de trabajar en equipo para el análisis de sistemas de información y el diseño de soluciones de seguridad, y la investigación de incidentes de seguridad.
CE10	Es capaz de tomar decisiones de forma autónoma y con iniciativa, y de argumentar de forma adecuada dichas decisiones.
CE11	Es capaz de generar, dado un escenario concreto de riesgos de seguridad de sistemas de información, una solución de seguridad aceptable utilizando diferentes mecanismos criptográficos y aplicaciones de seguridad.
CE12	Es capaz de trabajar en equipo de forma colaborativa para la resolución de problemas relacionados con la seguridad de redes y sistemas.
CE13	Es capaz de comunicar de manera eficaz sus conocimientos, procedimientos, resultados e ideas en el contexto de la asignatura, tanto por escrito como de forma oral.

Instrumentos de evaluación y Criterios de Calificación

Se plantea una evaluación continua del rendimiento del estudiante mediante el seguimiento del trabajo programado y la realización de una prueba parcial a mitad de cuatrimestre, más una prueba de conjunto a realizar al final del semestre.

- Actividades de seguimiento entregables (E): El seguimiento del trabajo del estudiante permite que el profesor conozca el grado de dedicación del estudiante respecto a las distintas actividades propuestas. A su vez, a los estudiantes les sirve para conocer si van alcanzando los objetivos marcados a lo largo del curso. Entre las actividades de seguimiento se incluirán: resolución de problemas, pequeños tests y pequeños trabajos. Las actividades de seguimiento podrán plantearse para hacer en clase, para hacer en el laboratorio, o como trabajo personal para el alumno. Las actividades de seguimiento suponen un 30% de la calificación final.
- Prueba de evaluación Intermedia (PEI): La prueba de Evaluación Intermedia tiene un peso del 30% sobre la calificación final.
- Prueba de Evaluación Final (PEF): La Prueba de Evaluación Final tiene un peso del 40% de la calificación final, y persigue un doble objetivo: evaluar la capacidad de relación de los conceptos aprendidos y revisar los conceptos evaluados en la prueba parcial. Por ello, si se ha obtenido al menos un 15% de calificación en las actividades de seguimiento, la prueba de conjunto permitirá además mejorar la calificación final si se obtiene un resultado superior al obtenido al aplicar la media de todas las calificaciones.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CG9, CG10, CG11, CIC6, CSI2,	RA1-RA6	CE1-CE13	E	30%

CSI5, CIS5, CTI7				
CIC6, CSI2	RA1,RA2	CE1-CE3, CE7	PEI	30%
CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE8,CE10,CE11	PEF	40%

Aquellos estudiantes que tengan reconocido el derecho a evaluación final, según fija la normativa de la UAH, deben realizar una prueba de evaluación final (PEF) que incluye cuestiones teóricas y la realización de uno o más ejercicios, con un peso del 70% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 30% de la calificación final.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE8,CE10,CE11	PEF	70%
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA3-RA6	CE4-CE13	TA	30%

La convocatoria extraordinaria plantea una única prueba de evaluación extraordinaria (PEE), que incorpora cuestiones teóricas y la resolución de uno o más ejercicios, con un peso del 70% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 30% de la calificación final. Para los estudiantes que hayan seguido el proceso de evaluación continua y hayan obtenido al menos un 15% en las actividades de seguimiento, la PEE tendrá un peso del 70%, tomándose el 30% restante de calificación de las actividades de seguimiento.

Competencia	Resultado Aprendizaje	Criterio de Evaluación	Instrumento de Evaluación	Peso en la calificación
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE11	E	30%
CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE8,CE10,CE11	PEE	70%

CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA3-RA6	CE4-CE13	TA	30%

6. BIBLIOGRAFÍA

Bibliografía Básica

- Information Security: Principles and Practice (2ª Ed.) M. Stamp Wiley, 2011
- Hacking Exposed 7: Network security secrets & solutions. Mc Graw-Hill, 2012

Bibliografía Complementaria

- Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017.
- Threat Modeling: Designing for Security. Wiley. 2014.

Universidad de Alcalá

TEACHING GUIDE

Security

Bachelor's Degree in
Information Systems
Computer Engineering
Informatics Engineering

University of Alcala

Academic year 2019/2020

4th Year – 1st Semester

TEACHING GUIDE

Course Name:	Security
Code:	780036
Degree in:	Degree in Information Systems Engineering Degree in Computer Engineering Degree in Computer Science
Department and area:	Automática Telematics Engineering
Type:	Optional
ECTS Credits:	6
Year and semester:	4th Year - 1st Semester
Teachers:	Iván Marsá Maestre Susel Fernández Melián
Tutoring schedule:	To be defined
Language:	Spanish/English friendly

COURSE SUMMARY

Information stored in computers and exchanged between them through communication networks may have great value for people, organizations and companies. Since it is available through a communications network such as the Internet, it can be accessible to a large number of people, among which there will be some with malicious intent. This means that the information is subject to a large number of threats and therefore increases the risk of being lost, modified or eavesdropped without authorization, in acts that we know today as cybercrime or human failures, equipment breakdowns or accidents. For these reasons, information security is a fundamental aspect of today's society, and the necessary capabilities to analyze the level of information security and take appropriate protection measures have a high demand in the business world.

This course delves into the technical aspects related to information security, once students have acquired the basic knowledge that supports the technology that allows generating, exchanging and storing information, in the Network Architecture I and Network Architecture II courses.

The course is structured in four parts:

1. Information Security, where the cryptographic procedures that allow processing the information itself to hide it or have guarantees that it has not been generated or modified without authorization are analyzed.
2. Access control, where the main mechanisms that exist to prevent access to information by unauthorized parties and mechanisms to detect attempts of unauthorized access are studied.
3. Security protocols: where the main global security solutions that are used to protect information in different classic environments are analyzed, usually a composition of mechanisms seen in parts 1 and 2.
4. System Security, where the main attacks that can occur against the systems that have and process information are analyzed, such as personal computers, smartphones or

servers and the different applications that run on them, focusing in the methodologies to assess the level of security of these systems through an audit process.

2. SKILLS

General skills:

CG3 Ability to design, develop, evaluate and ensure the accessibility, ergonomics, usability and safety systems, services and applications, as well as the information they manage.

CG9 Ability to solve problems with initiative, decision making, autonomy and creativity. Ability to communicate and transmit knowledge and skills of the profession of Technical Engineer.

CG10 Knowledge to perform measurements, calculations, assessments, appraisals, surveys, studies, reports, scheduling and similar work computer, according to the knowledge acquired as provided in paragraph 5 of resolution BOE-A-2009 -12,977.

CG11 Ability to analyze and assess the social and environmental impact of technical solutions, understanding the ethical and professional responsibility of the activity of the Technical Engineer.

Specific skills:

CIC6 Ability to understand, implement and manage the guarantee and security of computer systems.

CSI2 Ability to determine the requirements of information and communication systems of an organization considering aspects of security and compliance with regulations and legislation.

CSI5 Ability to understand and apply the principles of risk assessment and apply them correctly in the development and implementation of action plans.

CIS5 Ability to identify, evaluate and manage potential associated risks that may arise.

CTI7 Ability to understand, apply and manage the guarantee and security of computer systems.

Learning Outcomes

After succeeding in this course the students will be able to:

RA1	Use cryptographic mechanisms to manage information security risks, evaluating the implications of using the different available mechanisms
RA2	Choose and deploy security mechanisms (controls) for prevention, detection and reaction over network devices and services, including firewalls, intrusion detection systems and security policies.
RA3	Assess the security risks in a given information system, according to the inventory of system assets and the threats and vulnerabilities that affect them.

RA4	Build security solutions feasible for specific scenarios, using different cryptography mechanisms and security applications
RA5	Collect evidence on security incidents of systems, search for information about them and perform the analysis and subsequent communication of conclusions as part of a research team.
RA6	Work as a team in a collaborative way to solve problems related to network and system security and effectively communicate their knowledge, procedures, results and ideas, in both oral and written form.

3. CONTENT

Content Blocks	Total number of hours
Information security: introduction; symmetric cryptography: DES, 3DES, AES. Asymmetric cryptography: RSA, ECC, hash functions, hmac.	16 hours (4 weeks)
Access control: authentication: passwords, Single Sing On (SSO), biometry. Authorization: access control lists (ACLs), multilevel models. Mechanisms: firewalls, intrusion detection systems (IDS).	12 hours (3 weeks)
Security protocols: authentication, mutual authentication, man-in-the-middle attacks. Security in the Internet protocols.	8 hours (2 weeks)
Systems security: vulnerabilities and threats, vulnerability analysis. Software security: privilege escalation, malware. Security in Web applications. Systems audit. Security in operating systems. Information forensics.	12 hours (3 weeks)

4. TEACHING - LEARNING METHODOLOGIES. FORMATIVE ACTIVITIES.

4.1. Credit distribution

Number of on-site hours:	60 hours (56 hours on-site +4 exams hours)
Number of hours of student work:	90 hours
Total hours	150 hours.

4.2. Methodological strategies, teaching materials and resources

Classroom sessions	• Presentation and/or review of practical concepts. • Problem resolution. • Laboratory practices: aimed at consolidating the previously presented concepts, as well as to familiarize the student with the tools and methodologies to support the study of the subject and future professional performance (to improve the understanding of security concepts, intrusion detection, analysis of vulnerabilities, and implementation of security measures). • Oral presentations and other activities. • Group activities.
Tutoring (individual, for groups and via Web)	• Question discussion. • Support for autonomous learning
Autonomous work	• Reading. • Learning Activities: exercises, information search, data analysis.

5. ASSESSMENT: procedures, evaluation and grading criteria

Preferably, students will be offered a continuous assessment model that has characteristics of formative assessment in a way that serves as feedback in the teaching-learning process.

Procedures

The evaluation must be inspired by the criteria of continuous evaluation (Regulations for the Regulation of Teaching Learning Processes, NRPEA, art 3). However, in compliance with the regulations of the University of Alcala, an alternative process of final evaluation is made available to the student in accordance with the Regulations for the Evaluation of Apprenticeships (approved by the Governing Council on March 24, 2011 and modified in the Board of Directors). Government of May 5, 2016) as indicated in Article 10, students will have a period of fifteen days from the start of the course to request in writing to the Director of the Polytechnic School their intention to take the non-continuous evaluation model adducing the reasons that they deem convenient. The evaluation of the learning process of all students who do not apply for it or are denied it will be done, by default, according to the continuous assessment model. The student has two calls to pass the subject, one ordinary and one extraordinary.

Ordinary call
In the ordinary call, students will undertake a continuous assessment process. This process includes lab assignments, activities in class, self-assessment quizzes, and two intermediate exams. In exceptional circumstances, adequately documented, a student might be assessed by a Single Final Exam. The student should request this in written form to the Dean, during the first two weeks after his enrolment, specifying the circumstances preventing him to follow the continuous assessment procedure.

Extraordinary call
The Extraordinary Call will have a similar exam format to the one used for the Final Exam assessment in the Ordinary Call.

Evaluation criteria

The assessment criteria measure the level in which the skills have been acquired by the student. For
that purpose, the following are defined:

CE1. The student knows the different cryptographic mechanisms seen in the course.
CE2. The student is able to select, given a specific scenario with its information security risks, the most suitable cryptographic mechanism to fulfil a set of confidentiality, integrity and availability requirements.
CE3. The student is able to assess, given a specific cryptography scenario, the potential vulnerabilities that might appear.
CE4. The student knows the most common vulnerabilities and threats regarding network and system security.
CE5. The student is able to perform an asset inventory on an information system.
CE6. The student is able to assess the security risks of an information system, according to the system asset inventory and the vulnerabilities and threats affecting it.
CE7. The student knows the different security mechanisms that may be used to protect an information system, including firewalls, intrusion detection systems and security policies.
CE8. The student is able to apply the different security mechanisms for prevention, detection and reaction on network services and devices.

CE9. The student is able to work in a team to analyze information systems, to design security solutions, and to investigate security incidents.
CE10. The student is able to make decisions in an autonomous and proactive way, and to justify those decisions.
CE11. The student is able to generate, given a specific scenario regarding information system security risks, an acceptable security solution using different cryptographic mechanisms and security applications.
CE12. The student is able to work collaboratively in a team to solve problems regarding system and network security.
CE13. The student is able to communicate effectively knowledge, procedures, results and ideas within the context of the course, both in oral and written form.

Grading tools and criteria

The default grading tools correspond to continuous assessment via a series of follow-up assignments
and a midterm exam, along with an overall exam at the end of the semester.

- **Follow-up assignments (E)**: Following up student's work allows the professor to know the performance of the student regarding the different assignments. In addition, it helps students to know whether they are reaching the goals established throughout the course. Among the follow-up activities there will be: problem solving activities, quizzes and small assignments. These activities may be designed to do in class, in the lab, or at home. Follow-up activities make up to a 30% of the student grade.
- **Intermediate Assessment Exams (PEI)**: The intermediate assessment exam will make up to a 30% of the student grade.
- **Overall Assessment Exam (PEF)**: The overall assessment exam has a 40% weight in the student grade, and has a double purpose: assess the ability of the student to integrate the course contents and review the learning of these concepts. Taking this into account, if students have attained at least 15% of their final grade in the follow-up activities, the overall assessment exam will allow to improve the grade if the result obtained is higher than the average grade of the continuous assessment.

Skill	Learning outcome	Grading criteria	Grading tool	Contribution to the final mark
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA6	CE1-CE13	E	30%
CIC6, CSI2	RA1,RA2	CE1-CE3, CE7	PEI	30%
CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE8,CE10,CE11	PEF	40%

Students to which the Dean has granted final assessment, according to the UAH regulations, will have
to do a final assessment exam (PEF) including theoretical questions and exercises, with a contribution of 70% to the final mark. In addition, they will have to deliver a Course Assignment (TA), which will preferably be made in teams, with a contribution of 30% to the final mark.

Skill	Learning outcome	Grading criteria	Grading tool	Contribution to the final mark
CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE8,CE10,CE11	PEF	70%
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA3-RA6	CE4-CE13	TA	30%

The extraordinary call will have an extraordinary assessment exam (PEE) including theorical questions and exercises, with a contribution of 70% to the final mark. In addition, students will have to deliver a Course Assignment (TA), which will preferably be made in teams, with a contribution of 30% to the final mark. Students who have followed the continuous assessment in the ordinary call and have attained at least 15% of their final grade in the follow-up activities will not have to do the TA, getting the corresponding part of the grade from the follow-up activities.

Skill	Learning outcome	Grading criteria	Grading tool	Contribution to the final mark
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE11	E	30%
CIC6, CSI2, CSI5, CIS5, CTI7	RA1-RA4	CE1-CE8,CE10,CE11	PEE	70%
CG3, CG9, CG10, CG11, CIC6, CSI2, CSI5, CIS5, CTI7	RA3-RA6	CE4-CE13	TA	30%

6. BIBLIOGRAPHY

Basic Bibliography

- Information Security: Principles and Practice (2ª Ed.) M. Stamp Wiley, 2011
- Hacking Exposed 7: Network security secrets & solutions. Mc Graw-Hill, 2012

Additional Bibliography

- Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017.
- Threat Modeling: Designing for Security. Wiley. 2014.