Universidad de Alcalá

GUÍA DOCENTE

Seguridad

Grado en
Ingeniería en Tecnologías de Telecomunicación (GITT)
Ingeniería Telemática (GIT)

Universidad de Alcalá

Curso Académico 2022/2023

4º Curso - 1er Cuatrimestre (GITT)

3er Curso - 2º Cuatrimestre (GIT)

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

GUÍA DOCENTE

Nombre de la asignatura:	**Seguridad**
Código:	**350039 (GITT)** **380002 (GIT)**
Titulación en la que se imparte:	**Grado en** **Ingeniería en Tecnologías de Telecomunicación (GITT)** **Ingeniería Telemática (GIT)**
Departamento y Área de Conocimiento:	**Automática** **Ingeniería Telemática**
Carácter:	**Optativa (Especialidad) (GITT)** **Obligatoria (GIT)**
Créditos ECTS:	**6.0**
Curso y cuatrimestre:	**4º Curso - 1er Cuatrimestre (GITT)** **3er Curso - 2º Cuatrimestre (GIT)**
Profesorado:	Susel Fernández Melián
Horario de Tutoría:	Consultar al comienzo de la asignatura
Idioma en el que se imparte:	Español/English friendly

1a. 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.
4. 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.

1b. 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. COMPETENCIAS

Competencias básicas, generales y transversales.

Esta asignatura contribuye a adquirir las siguientes competencias básicas, generales y transversales definidas en el apartado 3 del Anexo de la Orden CIN/352/2009:

TR3 - Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico de Telecomunicación.

TR6 - Capacidad de analizar y valorar el impacto social y medioambiental de las soluciones técnicas.

TR8 - Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.

TRU4 - Capacidad de aprendizaje autónomo.

Competencias de Carácter Profesional

Esta asignatura proporciona la(s) siguiente(s) competencia(s) de carácter profesional definida(s) en el apartado 5 del Anexo de la Orden CIN/352/2009:

CTE2 - Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos.

CTE6 - Capacidad de diseñar arquitecturas de redes y servicios telemáticos.

Resultados de aprendizaje

Al terminar con éxito esta asignatura/enseñanza, los estudiantes serán capaces de:

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	Total de clases, créditos u horas
Seguridad de la Información: introducción; criptografía simétrica: DES, 3DES, AES; criptografía asimétrica: RSA, ECC; funciones hash, hmac.	20 horas (5 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).	20 horas (5 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.	8 horas (2 semanas)

4. METODOLOGÍAS DE ENSEÑANZA APRENDIZAJE. ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases en grupo grande: 28 horas (2 horas x 14 semanas) Clases en grupo reducido: 28 horas (2 horas x 14 semanas) Evaluación final: 2 horas. Total: 58 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: 92 horas
Total horas	150

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 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 Aprendizaje (aprobada en Consejo de Gobierno de 24 de marzo de 2011 y modificada en Consejo de Gobierno de 5 de mayo de 2016) 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

En la convocatoria ordinaria, se distinguen dos posibles vías para la evaluación: Evaluación Continua (EC) y Examen Final (EF).

Convocatoria extraordinaria

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

5.2. EVALUACIÓN

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 mas 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 tiene aprobada la media de la calificación en las actividades de seguimiento, la prueba de evaluación final permitirá además mejorar la calificación final si se obtiene un resultado superior al obtenido al aplicar la media de todas las calificaciones.

Competencia	Resultado de Aprendizaje	Criterio de Evaluación	Instrumento de evaluación	Peso en la calificación
CTE2, CTE6, TR3, TR6, TR8, TRU4	RA1-RA6	CE1-CE13	E	30%
CTE2, CTE6	RA1,RA2	CE1-CE3, CE7	PEI	30%
CTE2, CTE6	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), 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 de Aprendizaje	Criterio de Evaluación	Instrumento de evaluación	Peso en la calificación
CTE2, CTE6	RA1-RA4	CE1-CE8, CE10, CE11	PEF	70%
CTE2, CTE6, TR3, TR6, TR8, TRU4	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 tengan aprobada la media de las actividades de seguimiento, la PEE tendrá un peso del 70%, tomándose el 30% restante de calificación de las actividades de seguimiento.

Competencia	Resultado de Aprendizaje	Criterio de Evaluación	Instrumento de evaluación	Peso en la calificación
CTE2, CTE6	RA1-RA4	CE1-CE8, CE10, CE11	PEE	70%
CTE2, CTE6, TR3, TR8, TRU4	RA1-RA6	CE1-CE13	E/TA	30%

6. BIBLIOGRAFÍA

6.1. Bibliografía básica

- Information Security: Principles and Practice (3ª Ed.) M. Stamp Wiley, 2011
- Hacking Exposed 7: Network security secrets & solutions. Mc Graw-Hill, 2012

6.2. Bibliografía complementaria

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

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.