Universidad de Alcalá

GUÍA DOCENTE

FUNDAMENTOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Máster Universitario en Ciberseguridad (M179)
Universidad de Alcalá

Curso Académico 2019/20
Primer Cuatrimestre

GUÍA DOCENTE

Nombre de la asignatura:	**FUNDAMENTOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
Código:	**202555**
Titulación en la que se imparte:	**Máster Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	**Dpto. Ciencias de la Computación / Ciencia de la Computación e Inteligencia Artificial**
Carácter:	**Obligatorio**
Créditos ECTS:	**4,5**
Curso y cuatrimestre:	**Curso 1º - Cuatrimestre 1º**
Profesorado:	José Javier Martínez Herráiz
Horario de Tutoría:	**Por determinar**
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

La asignatura “Fundamentos de la Gestión de la Seguridad de la Información” aborda aspectos previos a la gestión de la seguridad de la información, como es conocer la legislación sobre ciberseguridad a nivel nacional y las normativas internacionales sobre metodologías de auditorías de seguridad y, en general, buenas prácticas de seguridad.

Tiene como objetivo derivado el análisis y diseño de políticas de seguridad en el desarrollo de un proyecto informático en una organización. Centrándose en los procedimientos y guías de seguridad tanto lógica como física y la creación de cuadros de mando de seguridad.

Los conocimientos que se adquieren son los relacionados con asegurar la continuidad de la función de informática mediante la incorporación a la organización de procedimientos de seguridad.

Especial relevancia tienen los conocimientos relacionados con la verificación y comprobación del buen funcionamiento de las tecnologías de la información incorporadas en una organización, a través de técnicas de auditoría de seguridad informática.

Es la asignatura precedente de “Sistemas de Gestión de la seguridad de la Información” (2º Cuatrimestre) junto con la que, de manera complementaria, configura la materia “Gestión y organización de la seguridad de la información”

2. COMPETENCIAS

Competencias Generales (CG) y Básicas (CB)

Esta asignatura contribuye a reforzar las siguientes competencias generales y básicas:

CG1	Capacidad para aplicar conocimientos y técnicas de seguridad de la información a la gestión, evaluación, cumplimiento de normativas y diseño de departamentos, programas y proyectos.
CB7	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

Competencias específicas (CE)

Esta asignatura contribuye a reforzar las siguientes competencias específicas:

CE1	Capacidad para aplicar conocimientos a la gestión de equipos, centros y departamentos responsables de la seguridad informática, incluyendo la auditoría de esos sistemas basada en un análisis de riesgos y el establecimiento de políticas.
CE2	Capacidad para razonar y tomar decisiones relativas a la seguridad y la privacidad acordes con el conocimiento de la regulación relevante, nacional e internacional.
CE3	Capacidad para aplicar conocimientos de economía y psicología de la seguridad, incluyendo la ingeniería social y los factores humanos en la ciberseguridad.

Competencias transversales (CT)

Esta asignatura contribuye a reforzar las siguientes transversales:

CT1	Gestión del tiempo
CT2	Trabajo en equipo
CT4	Orientación a la calidad

Resultados del aprendizaje

Los resultados de aprendizaje esperados con esta asignatura, en su orientación al desarrollo profesional, son los siguientes:

RA1	Aplicar conocimientos y técnicas de la seguridad de la información a la gestión de diferentes áreas de negocio, sectores o aplicaciones concretas.
RA2	Dirigir y planificar la puesta en marcha de un proyecto de gestión de la seguridad en una empresa u organización, aplicando controles de seguridad conforme a una metodología.

RA3	Conocer los diferentes procedimientos asociados a la gestión de la seguridad, como son análisis de riesgos, políticas de seguridad y los planes de contingencia, así como las leyes y regulaciones asociadas.
RA4	Conocer los aspectos psicológicos y humanos relacionados con la seguridad de la información y los equipos informáticos.

3. CONTENIDOS

Introducción a la gestión de la seguridad: necesidad de la gestión de la seguridad, ámbito de aplicación, amenazas de seguridad de la información, aspectos sociales y psicológicos de la ciberseguridad, auditorías de seguridad.
Normativa y buenas prácticas en seguridad: Planes, políticas de seguridad, estándares, procedimientos, guías, legislación relacionados con la seguridad en las TIC.
Auditoría de Seguridad y Análisis de Riesgos: La función de auditoría de seguridad y su marco jurídico. La estructura y metodología de trabajo: técnicas de la auditoría de seguridad informática. Informe de auditoría de seguridad informática. Análisis de Riesgos

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE.-ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases presenciales teórico prácticas, incluyendo trabajo en ordenador: 31,5 horas Tutorías: 9 horas Seminarios temáticos y conferencias: 4,5 horas Total: 45 horas presenciales
Número de horas del trabajo propio del estudiante:	Trabajo personal del estudiante: 45 horas Trabajo en grupos de estudiantes: 22,5 horas
Total horas	112,5 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases Presenciales	• Exposiciones en clase, de carácter teórico 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	• Lectura crítica de recursos docentes. • Resolución de ejercicios, prácticas o casos, de manera individual o colaborativa • Elaboración de trabajos e informes

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación[1]

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 master en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del master comunicará la resolución en un máximo de 15 días. En caso de no haber recibido respuesta, se considera estimada esta solicitud.

[1] *Es importante señalar los procedimientos de evaluación: por ejemplo evaluación continua, final, autoevaluación, co-evaluación. Instrumentos y evidencias: trabajos, actividades. Criterios o indicadores que se van a valorar en relación a las competencias: dominio de conocimientos conceptuales, aplicación, transferencia conocimientos. Para el sistema de calificación hay que recordar la* ***Normativa del Consejo de Gobierno del 16 de Julio de 2009****: la calificación de la evaluación continua representará****, al menos, el 60%.*** *Se puede elevar este % en la guía.*

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

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. Las actividades de seguimiento podrán plantearse para hacer en clase, o como trabajo personal para el alumno, y podrán temer carácter individual o grupal. Las actividades de seguimiento suponen un 40% 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 30% 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 20% 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	Instrumento de Evaluación	Peso en la calificación
CG1, CB7, CT1, CT2, CT4, CE1, CE2, CE3	RA1-RA4	E	40%
CE1, CE2, CE3	RA1-RA3	PEI	30%
CE1, CE2, CE3	RA1-RA3	PEF	30%

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 60% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 40% de la calificación final.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CE1, CE2, CE3	RA1-RA4	PEF	60%
CG1, CB7, CT1, CT2, CT4, CE1, CE2, CE3	RA1-RA4	TA	40%

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 60% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 40% de la calificación final. Para los estudiantes que hayan seguido el proceso de evaluación continua y hayan obtenido al menos un 20% en las actividades de seguimiento, la PEE tendrá un peso del 60%, tomándose el 40% restante de calificación de las actividades de seguimiento.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CB7, CT1, CT2, CT4, CE1, CE2, CE3	RA1-RA4	E	40%
CE1, CE2, CE3	RA1-RA4	PEE	60%
CG1, CB7, CT1, CT2, CT4, CE1, CE2, CE3,	RA1-RA4	TA	40%

6. BIBLIOGRAFÍA

Libros.

- Barman, S. (2001). Writing information security policies. New Riders Publishing.
- Krutz, R. L. And Dean Vines, R. (2004). The CISSP Prep Guide: Mastering the CISSP and ISSEP Exams (2nd edition). Wiley.
- Talabis, M. y Martin, J. (2012). *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis.* Massachusetts: Syngress.
- Taleb, N. N. (2016). *El Cisne Negro: El impacto de lo altamente improbable.* Paidós Ibérica Editorial. Nueva edición ampliada y revisada.

- Tipton, H.F. and Micki, K. (2004). *Information Security Management Handbook.* Florida: Auerbach Publications
- Pintos, Fernández, Joaquín. Auditorías y continuidad de negocio (UF1895), IC Editorial, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibalcala/detail.action?docID=4310536

Referencias en Internet:

- https://www.incibe-cert.es/guias-y-estudios
- https://www.ccn-cert.cni.es/
- https://thepsychologist.bps.org.uk/volume-29/september/social-psychology-cybersecurity