Universidad de Alcalá

GUÍA DOCENTE

Sistemas de Gestión de la Seguridad de la Información

Master Universitario en Ciberseguridad
Universidad de Alcalá

Curso Académico 2019/20
Segundo Cuatrimestre

DESCRIPCIÓN DE LA ASIGNATURA

Nombre de la asignatura:	**Sistemas de Gestión de la seguridad de la información**
Código:	202559
Titulación en la que se imparte:	**Máster Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	Departamento de Automática, Área de Ingeniería Telemática.
Carácter:	**Obligatorio**
Créditos ECTS:	4.5
Curso y cuatrimestre:	**Curso 1º - Cuatrimestre 2º**
Coordinador y Tutor Académico:	Bernardo Alarcos Alcázar
Horario de Tutoría:	Por determinar
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

La asignatura de sistemas de gestión de la seguridad de la información tiene como objetivo permitir al estudiante profundizar en materias relacionadas con la gestión de la seguridad de la información desde la visión de las metodologías y procedimientos aplicables. Se abordarán las normativas relacionadas con la gestión de la seguridad (ISO27000 – COBIT o el Plan Nacional de Seguridad) así como las diferentes metodologías que incorpora un proyecto de gestión de la seguridad como son la aplicación de controles de seguridad, análisis de riesgos, establecimiento de políticas de seguridad, establecimientos de un plan de contingencias o gestión de incidentes. Se tendrá en cuenta las normativas nacionales sobre la seguridad de la información y los aspectos psicológicos relacionados con la ciberseguridad.

2. COMPETENCIAS

Competencias Generales (CG)

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

CB8	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
CB10	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Esta asignatura contribuye a reforzar las siguientes transversales:

CT3	Toma de decisiones
CT4	Orientación a la calidad

Competencias específicas (CESP)

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.
CE4	Capacidad para aplicar, escoger y valorar diferentes controles de seguridad, ya sean basados en hardware, software y/o procedimentales.

Resultados del aprendizaje

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

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

Gestión de Riesgos: Evaluación del riesgo. Métodos de cálculo de riesgo. Tratamiento del riesgo. Evaluación y tiempos de recuperación. Integración en los ciclos de vida de los procesos. Monitorización y Comunicación.
Programas de Gestión de la Seguridad de la Información. Introducción. Arquitectura. Gestión y actividades administrativas. Servicios y actividades operacionales. Controles y contramedidas. Métricas y Monitorización. *Frameworks*: ISO 27000, COBIT, Esquema Nacional de Seguridad.
Gestión de incidentes de seguridad de la información. Introducción. Procedimientos. Organización. Recursos. Objetivos. Métricas y monitorización. Plan de respuesta. Continuidad de negocio y recuperación de desastres. Actividades posincidente.

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

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.

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
CB8, CB10, CT3, 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%
CB8, CB10, CT3, 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
CB8, CB10, CT3, CT4, CE1, CE2, CE3	RA1-RA4	E	40%
CE1, CE2, CE3	RA1-RA4	PEE	60%
CB8, CB10, CT3, CT4, CE1, CE2, CE3, CT1, CT3, CT4	RA1-RA4	TA	40%

6. BIBLIOGRAFÍA

Libros.

- Gómez, Vieites, Álvaro. Gestión de incidentes de seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibalcala/detail.action?docID=3229340

- Chicano, Tejada, Ester. Gestión de incidentes de seguridad informática (MF0488_3), IC Editorial, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibalcala/detail.action?docID=4184054

- MAGERIT – VERSION 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

- Gómez, Fernández, Luis, and Rivero, Pedro Pablo Fernández. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2018. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibalcala/detail.action?docID=5486388

- 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:

- http://www.iso27000.es/
- http://www.27000.org/
- https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XGyd5pNKgWo
- https://www.incibe-cert.es/guias-y-estudios
- https://www.ccn-cert.cni.es/
- http://www.iso27000.es/herramientas.html
- https://thepsychologist.bps.org.uk/volume-29/september/social-psychology-cybersecurity
- https://www.cloudindustryforum.org/content/why-real-key-cybersecurity-psychology

- Advanced social engineering attacks. https://www.sciencedirect.com/science/article/pii/S2214212614001343