Universidad de Alcalá

GUÍA DOCENTE

Sistemas de información para la ciberseguridad

Máster Universitario en Ciberseguridad

Universidad de Alcalá

Curso Académico 2019/20

GUÍA DOCENTE

Nombre de la asignatura:	**Sistemas de información para la ciberseguridad**
Código:	**202557**
Titulación en la que se imparte:	**Máster Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	**Ciencias de la Computación. Áreas de Lenguajes y Sistemas Informáticos/ Ciencias de la Computación e Inteligencia Artificial**
Carácter:	**Obligatorio**
Créditos ECTS:	**4.5**
Curso y cuatrimestre:	**Anual**
Profesorado:	**Miguel-Angel Sicilia Salvador Sánchez Alonso Marçal Mora Cantallops**
Horario de Tutoría:	
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

La asignatura aborda la ciberseguridad como un conjunto de técnicas, métodos y tecnologías que utilizan datos de diversas fuentes como base para la monitorización, prevención e investigación. Dentro de esta concepción, se abordan dos tipos fundamentales de fuentes de datos:

- Internas: incluyendo los datos de las redes y comunicaciones, así como de los componentes que las monitorizan, como pueden ser los Sistemas de Detección de Intrusiones (Intrusion Detection Systems), sistemas de recogidas de logs, o software para la monitorización de configuración, así como sistemas integrados como los SIEM.
- Externas: incluyendo por un lado fuentes de eventos de ciberseguridad externas (incluyendo las de organizaciones que monitorizan eventos globales, listas ne- gras u otros) y por otro recogida de datos de inteligencia, proveniente de foros, redes sociales o darknets de diferente tipo.

La perspectiva de la asignatura es abordar en este bloque los métodos, técnicas y tecnologías para la monitorización, análisis y predicción de ataques, tan- to en entornos investigativos como las honeynets, como en sistemas de alerta que integran datos en SIEM. En lugar de analizar cada componente por separado, se aborda desde la perspectiva de un sistema de información para la seguridad. Además, se incluye en este bloque los sistemas destinados a aspectos investigativos de ciberinteligencia, incluyendo la recopilación de datos de múltiples

fuentes, su agregación y su corelación con técnicas avanzadas a partir de información heterogénea..

Por lo anterior, los resultados de aprendizaje esperados son los siguientes:

- RA1: Saber extraer, almacenar, integrar y procesar datos externos de la Web o de darknets, así como de diferentes fuentes de inteligencia especializadas, para su uso como información para la protección y la investigación de inteligencia.
- RA2: Conocer y saber comparar y seleccionar elementos tecnológicos de monitorización y alerta de seguridad en redes en el contexto de una estrategia integrada de protección.
- RA3: Saber diseñar sistemas de investigación de seguridad como fuente de datos para conocer el comportamiento del atacante.
- RA4: Saber seleccionar, configurar y explotar sistemas de agregación de eventos y correlación, adaptados a los requisitos de monitorización y detección adecuados.

2. COMPETENCIAS

Competencias básicas y generales:

1. CG3: Capacidad para aplicar herramientas a la protección, análisis y evaluación de componentes software asi como para emitir juicios sobre los atributos relacionados con la seguridad de sistemas.
2. CG4: Capacidad para seleccionar, implantar, desplegar y mantener soluciones de monitorización, defensa e inteligencia en ciberseguridad, combinando diferentes elementos hardware, software y humanos.
3. CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
4. 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.
5. 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.

Competencias específicas:

1. CE12: Capacidad para aplicar técnicas, combinar y analizar datos y seleccionar fuentes de datos para los diferentes aspectos de la ciberinteligencia.

2. CE11: Capacidad para la selección, configuración y despliegue de componentes y sistemas software de monitorización, agregación de datos, correlación y reacción para la ciberseguridad.

Competencias transversales:

1. Gestión del tiempo
2. Trabajo en equipo
3. Resolución de problemas
4. Toma de decisiones

3. CONTENIDOS

Bloques de contenido	Total de créditos
Parte I. Tipología y fuentes de datos	0,5 ECTS
Parte II. Sistemas de detección y protección de intrusiones	1 ECTS
Parte III. SIEM y sistemas de agregación y correlación y automatización de la ciberseguridad.	1,5 ECTS
Parte IV. Sistemas para la investigación de la ciberseguridad	0,5 ECTS

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 Trabajo del estudiante: 67,5 horas 112,5
Número de horas del trabajo propio del estudiante:	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
	Trabajo del estudiante: 67,5 horas
	112,5
Total horas	112,5

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases teórico-prácticas	Las clases presenciales será de carácter teórico-práctico.
Lectura crítica de recursos docentes	Se proporcionarán recursos para el trabajo personal.
Resolución de ejercicios y prácticas	El trabajo personal y grupal se centrará en la resolución de ejercicios y prácticas guiadas.
Elaboración de trabajos	La evaluación será de carácter práctico, mediante la elaboración de trabajos de análisis de datos.

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 máster en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del

[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.*

máster 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 Pruebas de evaluación Continua (PEC) de acuerdo a la siguiente Tabla.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CE11, CE12, CB7	RA2/RA4	Prueba presencial	40%
CE11, CE12, CE2, CG3, CG4, CB7, CB10	RA1/RA2/RA4	Prueba presencial	40%
CE11, CE12, CE2, CG3, CG4, CB6, CB7, CB10	RA1/RA3	Prueba presencial	20%

Aquellos estudiantes que tengan reconocido el derecho a evaluación final, según fija la normativa de la UAH, deben realizar un examen final presencial.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
Todas	Todos	Examen presencial	100%

La convocatoria extraordinaria plantea una única prueba de consistente igualmente en un examen final presencial.

.

6. BIBLIOGRAFÍA

Bibliografía Básica

Sanders, C., & Smith, J. (2013). Applied network security monitoring: collection, detection, and analysis. Elsevier.

Miller, D. (2011). Security information and event management (SIEM) implementation. McGraw-Hill.