Universidad de Alcalá

GUÍA DOCENTE

Análisis de datos para la ciberseguridad

Máster Universitario en Ciberseguridad

Universidad de Alcalá

Curso Académico 2019/20

GUÍA DOCENTE

Nombre de la asignatura:	**Análisis de datos para la ciberseguridad**
Código:	**202560**
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

Las técnicas de análisis de datos permiten extraer conocimiento de datos heterogéneos. Esos datos pueden provenir de múltiples fuentes (IDS, firewall, listas negras, bases de datos de vulnerabilidades, de ataques, sistemas SIEM, etc.), y requieren un tratamiento previo a la tarea analítica. Además de lo anterior, la detección de intrusiones puede beneficiarse del análisis de datos para crear modelos automatizados o para descubrir patrones o estructura en los mismos, utilizando técnicas de aprendizaje automático.

La presente asignatura tiene como objetivo el conocer los aspectos fundamentales de las diferentes técnicas de analítica de datos sobre grandes bases de datos de eventos, hechos y artefactos relacionados con la ciberseguridad. Concretamente, se introducen las técnicas de aprendizaje automático como una forma de construir modelos que mejoran las capacidades de detección, así como las técnicas de procesamiento del lenguaje natural y de grafos de relaciones que tienen un papel crucial en la ciberinteligencia.

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 aplicar técnicas de inteligencia computacional y aprendizaje automático a los datos recogidos por sistemas como los mencionados.

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. CE1: Capacidad para aplicar técnicas, combinar y analizar datos y seleccionar fuentes de datos para los diferentes aspectos de la ciberinteligencia.

2. CE2: Capacidad para aplicar técnicas de inteligencia computacional al análisis de datos y al conocimiento situacional en 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. Introducción a las técnicas de análisis de datos: uso de entornos y bibliotecas de data science.	1 ECTS
Parte II. Fundamentos de técnicas de análisis de datos para ciberseguridad. Introducción a las técnicas analíticas, introducción al aprendizaje automático, introducción al análisis de grafos y redes sociales, técnicas básicas de procesamiento del lenguaje natural.	2 ECTS
Parte III. Casos de análisis de datos. Casos específicos de análisis.	1 ECTS
Parte IV. Tratamiento escalable para el análisis de datos. Entornos para el procesamiento escalable de grandes volúmenes de datos.	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
Número de horas del trabajo propio del estudiante:	Trabajo del estudiante: 67,5 horas
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 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
CE1, CB7	RA1	Prueba presencial	30%
CE1, CE2, CG3, CG4, CB7, CB10	RA1/RA2	Prueba presencial	30%
CE1, CE2, CG3, CG4, CB6, CB7, CB10	RA1/RA2	Trabajo en equipo	40%

[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.*

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

VanderPlas, J. (2016**). Python data science handbook: essential tools for working with data**. O'Reilly Media, Inc.

Chio, C., & Freeman, D. (2018). **Machine Learning and Security: Protecting Systems with Data and Algorithms**. O'Reilly Media, Inc.

Bibliografía Complementaria

Collins, M., & Collins, M. S. (2014). **Network security through data analysis: building situational awareness**. O'Reilly Media, Inc.

Stamp, M. (2017). **Introduction to machine learning with applications in information security**. Chapman and Hall/CRC.