19-20

MÁSTER UNIVERSITARIO EN
CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD

CÓDIGO 31109097

UNED

19-20

INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD

CÓDIGO 31109097

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

EQUIPO DOCENTE

HORARIO DE ATENCIÓN AL ESTUDIANTE

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

RESULTADOS DE APRENDIZAJE

CONTENIDOS

METODOLOGÍA

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

BIBLIOGRAFÍA COMPLEMENTARIA

RECURSOS DE APOYO Y WEBGRAFÍA

ADENDA AL SISTEMA DE EVALUACIÓN CON MOTIVO DE LA PANDEMIA COVID 19

Nombre de la asignatura	INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD
Código	31109097
Curso académico	2019/2020
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

En esta asignatura se realiza una introducción a las técnicas, modelos y algoritmos de aprendizaje automático de la inteligencia artificial que se pueden aplicar como herramientas para predecir, detectar y analizar las vulnerabilidades de seguridad y los ataques a los servicios de los sistemas de comunicaciones y de computación.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

No hay requisitos previos diferentes de los generales de acceso a este máster. Sin embargo, es conveniente tener un nivel de lectura en inglés suficiente como para entender contenidos técnicos en dicha lengua, ya que la bibliografía y algunos de los recursos proporcionados al estudiante en el curso virtual pueden estar únicamente en inglés, debido a la novedad de algunos de los contenidos propuestos para la asignatura.

EQUIPO DOCENTE

Nombre y Apellidos	JOSE RAMON ALVAREZ SANCHEZ (Coordinador de asignatura)
Correo Electrónico	jras@dia.uned.es
Teléfono	91398-7199
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	INTELIGENCIA ARTIFICIAL

Nombre y Apellidos	ENRIQUE JAVIER CARMONA SUAREZ
Correo Electrónico	ecarmona@dia.uned.es
Teléfono	91398-7301
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	INTELIGENCIA ARTIFICIAL

HORARIO DE ATENCIÓN AL ESTUDIANTE

La tutorización de los estudiantes se llevará a cabo principalmente a través del curso virtual correspondiente en la plataforma de e-Learning de la UNED, que proporciona foros para comunicación, almacenes de material y mecanismos para la recogida de las actividades de evaluación. Por supuesto, adicionalmente el equipo docente también atenderá, durante los periodos lectivos, por correo electrónico (y mensajes directos desde el curso virtual) todas las dudas o consultas específicas de los estudiantes sobre la asignatura. También se atenderán dudas específicas por teléfono los lunes de 15 a 19 h.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS BÁSICAS

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.

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.

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.

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

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 GENERALES

CG1 - Analizar métodos y técnicas de ciberataques.

CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.

COMPETENCIAS TRANSVERSALES

CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

COMPETENCIAS ESPECÍFICAS

CE6 - Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.

RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

- Conocer y saber aplicar los algoritmos básicos de agrupamiento para analizar patrones en ataques y posibles vulnerabilidades de seguridad.
- Conocer y aplicar las técnicas de aprendizaje automático para clasificación de patrones y su aplicación en ciberseguridad.
- Utilizar modelos probabilísticos para clasificación y agrupamiento en problemas de ciberseguridad.
- Conocer las arquitecturas básicas de aprendizaje profundo para su aplicación en ciberseguridad.

CONTENIDOS

Tema 1: La Inteligencia Artificial en ciberseguridad.

Introducción sobre la aplicación de los métodos de aprendizaje automático de la Inteligencia Artificial en los problemas de ciberseguridad.

Tema 2: Algoritmos de agrupamiento.

Los algoritmos de agrupamiento utilizan funciones de similaridad para agrupar trozos de información. Estos algoritmos son de gran utilidad para identificar tipos de comportamientos y detectar anomalías en ciberseguridad.

Tema 3: Clasificación.

Los algoritmos de clasificación son de los más importantes en aprendizaje automático y muy útiles para ayudar a decidir si un conjunto de datos indica un posible ataque, etc.

Tema 4: Modelos probabilísticos.

Se pueden utilizar modelos probabilísticos básicos también para agrupamiento y clasificación en el aprendizaje automático.

Tema 5: Arquitecturas de aprendizaje profundo (Deep Learning).

Las herramientas de redes neuronales (convolucionales y long sort-term memory) pueden utilizan capacidades de computación muy elevadas para obtener buenos resultados en ciberseguridad.

METODOLOGÍA

La metodología es la general del máster adaptada a las directrices del EEES, de acuerdo con las recomendaciones del Instituto Universitario de Educación a Distancia de la UNED. Se utilizarán la metodología y los medios propios de la enseñanza a distancia que la UNED pone a disposición de sus estudiantes.
El estudio de esta asignatura se debe realizar siguiendo las indicaciones del **manual didáctico que se encontrará en el curso virtual de la asignatura**.
De forma orientativa, la dedicación estimada a las actividades formativas se puede distribuir en 60 h. para el estudio de contenidos teórico-prácticos con bibliografía y materiales complementarios, 15 h. de tutorías, 15 h. de actividades en la plataforma virtual, 30 h. de prácticas informáticas y 30 h. para otros trabajos/prácticas.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen de desarrollo
Preguntas desarrollo	3
Duración del examen	120 (minutos)

Material permitido en el examen

Cualquier material impreso y calculadoras.

Criterios de evaluación

Las preguntas pueden ser carácter teórico-práctico y la valoración de cada pregunta se indicará en el enunciado.
Se valorará la explicación correcta y adecuada de los procedimientos o forma de solución utilizada además de los resultados parciales correctos. Los errores graves conceptuales pueden restar puntuación.

% del examen sobre la nota final	60
Nota del examen para aprobar sin PEC	8,5
Nota máxima que aporta el examen a la calificación final sin PEC	6
Nota mínima en el examen para sumar la PEC	5

Comentarios y observaciones

La solicitud de revisión de examen, dentro del plazo de 7 días después de la publicación de las notas, se debe hacer por correo electrónico al coordinador de la asignatura incluyendo los datos del estudiante (nombre, apellidos y número de DNI o documento usado en la matrícula). La solicitud de revisión deberá ser motivada. El estudiante deberá argumentar, a la vista de su examen digitalizado, las razones que fundamenten la oposición a la calificación otorgada. Las solicitudes carentes de motivación no seran admisibles.

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad: No

Descripción

Al final del semestre se debe enviar un trabajo individual de tipo práctico según el enunciado que se proporcionará en el curso virtual de la asignatura. La forma de entrega será el envío de los ficheros requeridos a través de la tarea correspondiente en el curso virtual de la asignatura.

Criterios de evaluación

Los requisitos que debe cumplir la práctica y su valoración se indicarán en el enunciado.

Ponderación de la prueba presencial y/o los trabajos en la nota final: Hasta un 20% de la nota final.

Fecha aproximada de entrega: Antes del final de las pruebas presenciales de cada convocatoria.

Comentarios y observaciones

El trabajo final **no** es obligatorio, pero en caso de no entregarlo, la calificación del mismo será 0.

Si se suspende el trabajo práctico final (o no se entrega) en la convocatoria ordinaria (junio), se podrá volver a entregar para la convocatoria extraordinaria (septiembre).

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?: Si,PEC no presencial

Descripción

En el manual didáctico específico de la asignatura se indicarán el enunciado y los medios de elaboración de las pruebas de evaluación continua. La forma de entrega será el envío de los ficheros requeridos a través de las tareas correspondientes en el curso virtual de la asignatura.

Criterios de evaluación

Los requisitos que debe cumplir cada PEC y su valoración se indicarán en el enunciado correspondiente.

Ponderación de la PEC en la nota final: Hasta un 20% de la nota final.

Fecha aproximada de entrega: Las actividades entregables tienen un plazo, a lo largo del curso, indicado en el manual didáctico.

Comentarios y observaciones

Las PEC **no** son obligatorias, pero al ser de evaluación continua, solo podrán presentarse antes del plazo indicado para cada una. La nota obtenida se conserva para las convocatorias del curso actual.

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s? No

Descripción

Criterios de evaluación

Ponderación en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

En caso de que la calificación (de 0 a 10) de la prueba presencial sea mayor o igual a 5, la nota final será la suma ponderada de las calificaciones (de 0 a 10) de la prueba presencial [PP], del trabajo práctico final [TF] y de las PEC, según la siguiente fórmula: *Nota_final = 0,6*[PP] + 0,2*[TF] + 0,2*[PEC]*.

En caso de que la calificación de la prueba presencial sea menor de 5, no se sumará la nota de las PEC, y la nota final se calculará con la fórmula: *Nota_final = 0,6*[PP] + 0,2*[TF]*.

BIBLIOGRAFÍA BÁSICA

ISBN(13):9780998016900
Título:INTRODUCTION TO ARTIFICIAL INTELLIGENCE FOR SECURITY PROFESSIONALS
Autor/es:The Cylance Data Science Team ;
Editorial:THE CYLANCE PRESS

El libro base se puede obtener en **formato electrónico (PDF) de forma gratuita para uso personal**, solicitándolo a través del formulario en la página web:
https://pages.cylance.com/en-us-introduction-to-ai-book.html
También está disponible para compra en versión electrónica para Kindle en la tienda online de Amazon, y para Nook en la tienda online de Barnes&Noble.

BIBLIOGRAFÍA COMPLEMENTARIA

En el Manual Didáctico específico elaborado por el equipo docente se incluyen para cada tema referencias bibliográficas para consultar y ampliar conocimientos, así como también recomendaciones de software.

RECURSOS DE APOYO Y WEBGRAFÍA

La plataforma de cursos virtuales y e-Learning de la UNED, proporcionará la adecuada interfaz de interacción entre estudiante y equipo docente. Se utilizará principalmente para gestionar y compartir documentos y también para la comunicación a través de sus foros. En esta plataforma se incluirá como documento específico el Manual Didáctico elaborado por el equipo docente y otros posibles materiales necesarios.

ADENDA AL SISTEMA DE EVALUACIÓN CON MOTIVO DE LA PANDEMIA COVID 19

https://app.uned.es/evacaldos/asignatura/adendasig/31109097

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.