23-24

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA

INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD

CÓDIGO 31109097

UNED

23-24

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

Nombre de la asignatura	INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD
Código	31109097
Curso académico	2023/2024
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

El objetivo de esta asignatura es proporcionar al estudiante una introducción práctica a las técnicas, modelos y algoritmos básicos 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.
Esta asignatura puede proporcionar al estudiante una perspectiva de las técnicas más modernas usadas en los ataques a los sistemas de comunicaciones y de computación y, por tanto, también para prevenir o defender y proteger dichos sistemas frente a estos ataques. Al mismo tiempo, las técnicas de aprendizaje automático también pueden ser aplicadas al análisis de los ataques tanto en tiempo real como posteriormente. Por lo tanto esta asignatura puede ser un complemento a asignaturas del máster como "Auditoría y Monitorización de la Seguridad", "Análisis Forense" o "Seguridad en Infraestructuras Críticas".
Adicionalmente, las técnicas de aprendizaje automático de la inteligencia artificial se están usando actualmente en otras áreas de la informática y la computación, especialmente en todas las profesiones en las que se realiza algún tratamiento de datos masivos (*data analytics*, *data mining*, etc.).

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Para el estudio y comprensión de esta asignatura se requieren conocimientos básicos previos de programación en lenguaje Python.
Adicionalmente, 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.
También se atenderán dudas o consultas específicas durante el periodo lectivo, preferentemente por email, dirigidas directamente al coordinador del equipo docente:
Email: jras@dia.uned.es
José Ramón Álvarez Sánchez
Dpto. de Inteligencia Artificial
E.T.S.I. Informática - UNED
cl. Juan del Rosal, 16
E-28040 - Madrid
Teléfono: +34-91-398-7199 (lunes de 15:00 a 19:00 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 de los recursos disponibles dentro del **curso virtual de la plataforma online de la UNED correspondiente a la asignatura**, que también incluye un Manual Didáctico específico elaborado por el equipo docente, en el que proporcionará información adicional sobre el libro base y otros materiales necesarios para estudiar 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

Ninguno.

Criterios de evaluación

Las preguntas pueden ser ejercicios de carácter teórico-práctico con longitud libre para la respuesta.

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. La valoración de cada pregunta se indicará en el propio enunciado.

% del examen sobre la nota final	50
Nota del examen para aprobar sin PEC	
Nota máxima que aporta el examen a la calificación final sin PEC	5
Nota mínima en el examen para sumar la PEC	4

Comentarios y observaciones

En caso de no alcanzar la nota mínima de 4 (de 0 a 10) en el examen presencial, no se sumará la nota de la PEC, aunque sí la del trabajo final.

La calificación final máxima si únicamente se realiza la prueba presencial (sin PEC, ni Trabajo Final) solo puede ser de hasta 5 puntos.

Las fechas y lugares de examenes presenciales se publicarán por la UNED en el Calendario de exámenes personalizado en el acceso al CAMPUS virtual de cada estudiante.

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	No

Descripción

Además de la prueba presencial indicada arriba, al final del semestre se debe enviar un trabajo individual personal 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

La calificación del trabajo final (de 0 a 10), ponderada por un 30%, contribuirá en cualquier caso a la nota final. No se requiere ninguna nota mínima en el trabajo final (ni haberlo entregado) para considerar la puntuación del examen, ni viceversa.

Ponderación de la prueba presencial y/o los trabajos en la nota final	El trabajo final aporta hasta un 30% de la nota final.
Fecha aproximada de entrega	Antes del final de las pruebas presenciales de cada convocatoria.

Comentarios y observaciones

La calificación del trabajo final en la convocatoria de junio se mantiene para la convocatoria de septiembre. Si la nota del trabajo final obtenida en junio es inferior a 5, o no se había entregado, entonces se podrá volver a entregar para la convocatoria extraordinaria (septiembre).

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC? Si,PEC no presencial

Descripción

Las Pruebas de Evaluación Continua (PEC) se realizan a distancia. Los enunciados y los plazos de entrega se detallan como tareas **dentro del curso virtual** en el apartado "Actividades Evaluables".

Estas pruebas serán de naturaleza teórico/práctica para realizar en el transcurso del semestre. La entrega de cada PEC será únicamente por vía telemática dentro del curso virtual en el plazo indicado en el mismo y a lo largo del semestre.

Criterios de evaluación

La media de calificaciones de las PEC (de 0 a 10 cada una) ponderada por un 20% se sumará a la nota final solo en caso de que la nota de la prueba presencial sea un 4 o más.

No es necesaria ninguna nota mínima en las PECs (ni haberlas entregado) para aprobar la asignatura.

Ponderación de la PEC en la nota final: La PEC puede aportar hasta un 20% de la nota final en caso de obtener al menos un 4 en el examen presencial.

Fecha aproximada de entrega: Las actividades entregables tienen un plazo, a lo largo del segundo semestre, indicado en el Manual Didáctico en el curso virtual.

Comentarios y observaciones

Al ser pruebas de evaluación continua, las PEC entregadas fuera de plazo no se evaluarán. La nota total de las PEC se mantiene para la convocatoria de septiembre.

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?

Si la calificación (de 0 a 10) de la prueba presencial es mayor o igual a 4, entonces la nota final se calcula con la fórmula:

Nota_Final = 50% NE + 20% NPEC + 30% NTF

donde NE es la Nota del Examen (de 0 a 10), NPEC es la Nota media de las PECs (de 0 a 10) y NTF es la Nota del Trabajo Final (de 0 a 10).

Si la calificación de la prueba presencial es menor de 4, entonces:

Nota_Final = 50% NE + 30% NTF

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**, a través del repositorio actualizado indicado **dentro del curso virtual** en la plataforma online de la UNED correspondiente a la asignatura.
En el **curso virtual de la asignatura también se podrá descargar un Manual Didáctico específico** elaborado por el equipo docente, en el que se proporcionará información adicional sobre el libro base y otros materiales necesarios para estudiar la asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

Dentro del curso virtual, en el Manual Didáctico específico elaborado por el equipo docente, se pueden encontrar 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.

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.