Proyecto docente

Asignatura	Tendencias Emergentes en Ciberseguridad		
Materia	Seguridad de datos y Ciberseguridad		
Titulación	Máster Universitario en Inteligencia de Negocio y Big Data en Entornos Seguros		
Plan	621	**Código**	
Periodo de impartición	Segundo semestre	**Tipo/Carácter**	Obligatoria
Nivel/Ciclo	Máster	**Curso**	1
Créditos ECTS	3		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Ángel Luis Muñoz Castañeda		
Datos de contacto (e-mail, teléfono…)	amunc@unileon.es		
Horario de tutorías	Previa petición por email		
Coordinador			
Departamento	Matemáticas		
Web	https://ubuvirtual.ubu.es		
Descripción General	Se introduce la teoría de grafos como modelo matemático de una red de comunicaciones. Es estudian los modelos teóricos fundamentales, las medidas más importantes y se estudian aplicaciones a la ciberseguridad en redes de comunicaciones.		

1. Situación / Sentido de la asignatura

1.1 Contextualización

En esta materia, al alumnado se le proporcionarán conocimientos de seguridad en datos estructurados y análisis de amenazas en redes, así como de los protocolos actuales de compartición segura de información en redes.
El modelado de datos estructurados, así como el modelado de redes, descansa en la teoría de grafos. Se estudiarán los conceptos básicos de la teoría de grafos, los algoritmos utilizados para la detección de comunidades en grafos y los conceptos básicos sobre procesos dinámicos en grafos. Se aplicarán los conceptos teóricos estudiados al análisis de detección de anomalías en datos estructurados y al análisis de amenazas persistentes avanzadas distribuidas (DAPTs) en redes de computadores.
El objetivo es que el alumno comprenda tanto los principios básicos como las tendencias emergentes.

1.2 Relación con otras asignaturas

1.3 Prerrequisitos

Se recomienda haber cursado las matemáticas y programación básicas correspondientes a un primer curso de un grado de ingeniería. En concreto, se recomienda haber cursado: Álgebra Lineal, Cálculo Diferencial, Probabilidad y Estadística, Programación en Python.

2. Competencias

2.1 Generales del título

- CG1. Adquisición de competencias teóricas y prácticas para el análisis y diseño de soluciones empresariales en Big Data (almacenamiento y procesamiento de grandes volúmenes de información heterogénea).
- CG2. Capacidad de planificar y construir sistemas que permitan una gestión segura de los datos.

2.2 Específicas materia

- CSD6. Conocer y aplicar las últimas tendencias y tecnologías/técnicas emergentes en el campo de la seguridad con aplicaciones a Big Data.

3. Resultados de aprendizaje

Al finalizar la asignatura, el alumno será capaz de:

1.- Modelar una red, calcular las medidas fundamentales en ella, detectar anomalías en bases de datos estructurados.

2.- Modelar la propagación de virus y describir alguna amenaza persistente de ciberseguridad.

3.- Reconocer protocolos de comunicación segura en redes.

4. Contenido / Programa de la asignatura

Bloque 1: Redes. Modelado y estudio.

Carga de trabajo en créditos ECTS: 1,72 ECTS

a. Contextualización y justificación

El modelado de datos estructurados, así como el modelado de redes, descansa en la teoría de grafos. Se estudiarán los conceptos básicos de la teoría de grafos, las medidas fundamentales y los algoritmos utilizados para la detección de comunidades en grafos. Se aplicarán al estudio de detección de anomalías en datos estructurados y en redes.

b. Objetivos de aprendizaje

Sabrá modelar una red, calcular las medidas fundamentales en ella y detectar anomalías en bases de datos estructurados y en redes.

c. Contenidos y materiales de aprendizaje

Contenidos:
1.- Grafos.
2.- Medidas.
3.- Modelos.
4.- Detección de comunidades.
5.- Aplicaciones.
Materiales:
1.- Documentación aportada en plataforma digital

d. Métodos docentes

1.- Clases on-line y/o vídeos explicativos.
2.- Tutorías on-line a petición de los alumnos, tanto grupales como individuales.

e. Bibliografía básica

Mark Newman, *Networks: An Introduction*, Oxford University Press.

f. Bibliografía complementaria

Artículos de investigación científica actuales.

g. Recursos necesarios

1.- Plataforma docente
2.- Herramientas de comunicación:
- Foros, emails.
- Sala de videoconferencia, Google Meet o similares.

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
1,8 ECTS	SEMANA 1 - SEMANA 4

Bloque 2: Amenazas Persistentes en redes de comunicación

Carga de trabajo en créditos ECTS: 0,86 ECTS

a. Contextualización y justificación

El modelado de redes descansa en la teoría de grafos. Se estudiarán los conceptos básicos sobre procesos dinámicos en grafos. Se aplicarán los conceptos teóricos estudiados al análisis de amenazas persistentes avanzadas distribuidas (DAPTs) en redes de computadores.

b. Objetivos de aprendizaje

Saber modelar un proceso dinámico en una red y obtener las ecuaciones diferenciales que lo gobiernan, resolver las ecuaciones con software matemático (librerías matemáticas de Python) e interpretar los resultados.

c. Contenidos y materiales de aprendizaje

Contenidos:
1.- Procesos dinámicos en grafos.
2.- Ejemplos clásicos.
3.- Aplicación al estudio de amenazas persistentes en redes.

d. Métodos docentes

1.- Clases on-line y/o vídeos explicativos.
2.- Tutorías on-line a petición de los alumnos.

e. Bibliografía básica

Mark Newman, *Networks: An Introduction*, Oxford University Press.

f. Bibliografía complementaria

Artículo de investigación científica actuales.

g. Recursos necesarios

1.- Plataforma docente
2.- Herramientas de comunicación:
- Foros, emails.
- Sala de videoconferencia, Google Meet o similares.

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0,9 ECTS	SEMANA 5 / SEMANA 6

Bloque 3: Protocolos de compartición segura

Carga de trabajo en créditos ECTS: 0,42 ECTS

a. Contextualización y justificación

Las técnicas de compartición segura de información en redes forman una parte fundamental de lo englobado en ciberseguridad activa. Se estudiarán aspectos básicos de algunos de los protocolos de compartición segura actuales.

b. Objetivos de aprendizaje

Conocer aspectos básicos de algunos de los protocolos de compartición segura actuales.

c. Contenidos y materiales de aprendizaje

Contenidos:

1.- Protocolos de compartición segura.

d. Métodos docentes

1.- Clases on-line y/o vídeos explicativos.

2.- Tutorías on-line a petición de los alumnos.

e. Bibliografía básica

Cie Wang, Zachary Kissel, *Introduction to network security. Theory and practice,* Wiley Higher Education Press.

f. Bibliografía complementaria

Artículos de investigación científica actuales.

g. Recursos necesarios

1.- Plataforma docente

2.- Herramientas de comunicación:

- Foros, emails.
- Sala de videoconferencia, Google Meet o similares.

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0,3 ECTS	SEMANA 7

5. Metodología de enseñanza y dedicación del estudiante a la asignatura

Actividad Formativa	Competencias relacionadas	Horas	Presencialidad (%)
Clases, conferencias y técnicas expositivas		12	0
Actividades autónomas y en grupo (trabajos y lecturas dirigidas)		45	0
Pruebas de seguimiento y exposición de trabajos		10	50
Tutoría individual, grupal, participación en foros y otros medios colaborativos		8	0

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1	1,72 ECTS	SEMANA 1 / SEMANA 4
Bloque 2	0,86 ECTS	SEMANA 4 / SEMANA 6
Bloque 3	0,42 ECTS	SEMANA 7

7. Evaluación

Instrumento / Procedimiento	Peso primera convocatoria	Peso segunda convocatoria
Tests/Cuestionarios individuales	30 %	30 %
Realización de trabajos y/o resolución de problemas	60 %	60 %
Participación en foros y otros medios participativos	10 %	10 %

Criterios / Comentarios a la evaluación

- **Convocatoria ordinaria:** Suma ponderada de los ítems de evaluación. En cada actividad de evaluación se exigirá una calificación mínima para que la misma pueda formar parte de la evaluación continua. Este valor se fijará al comienzo del curso. Cualquier tarea copiada o plagiada obtendrá la calificación 0. Las actividades se han de entregar en tiempo y forma. La asignatura se supera sumando 50 puntos o más entre todas las actividades de evaluación computables en la evaluación continua.
- **Convocatoria extraordinaria:** Suma ponderada de los ítems de evaluación. Se entregará, en la fecha que corresponda, los ítems de evaluación correspondientes a trabajos y/o resolución de problemas. Éstos mantendrán la misma orientación que los correspondientes a los de la evaluación continua de la convocatoria ordinaria pero con enunciados diferentes. Se podrá conservar la calificación de las tareas que se superen en la evaluación continua de primera convocatoria. Se realizará un único test, en la fecha que corresponda, correspondiente al temario evaluado de esta manera en la primera convocatoria.

9. Consideraciones / Comentarios adicionales

La profundidad de los contenidos de la asignatura se modulará en función de los conocimientos previos del alumnado en matemáticas y programación.