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**	54561
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	Adriana Suárez Corona		
Datos de contacto (e-mail, teléfono…)	asuac@unileon.es		
Horario de tutorías	Previa petición por email		
Coordinador			
Departamento	Matemáticas		
Web	https://ubuvirtual.ubu.es		
Descripción General			

1. Situación / Sentido de la asignatura

1.1 Contextualización

En esta materia al alumno se le proporcionan conocimientos de seguridad en el almacenamiento de los datos y en su transmisión. El alumno aprenderá los conceptos y técnicas básicas en este campo, y aprenderá a aplicarlas a grandes volúmenes de datos, problema con características particulares. El objetivo es que el alumno comprenda tanto los principios básicos como las tendencias emergentes. Otro elemento importante que el alumno aprenderá son los aspectos legales relacionados con la adquisición, almacenamiento, gestión y uso de los datos.

1.2 Relación con otras asignaturas

1.3 Prerrequisitos

2. Competencias

2.1 Generales del título

CG2. Capacidad de planificar y construir sistemas que permitan una gestión segura de los datos.

2.2 Específicas materia

CSD5 - Capacidad de diseñar y aplicar soluciones relativas a los aspectos relativos a temas de la seguridad y privacidad en entornos de Big Data

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

3. Resultados de aprendizaje

Al finalizar la asignatura, el alumno conocerá las últimas tendencias y tecnologías emergentes del ámbito de la privacidad y la seguridad en Big Data, sabrá modelar una red, calcular el flujo en ella y la tasa de infección en red, así como modelar la propagación de virus. Además, el alumno será capaz de describir alguna amenaza persistente de ciberseguridad, conocerá la comunicación segura en redes, así como los distintos tipos de medidas de seguridad pasiva y activa en distintos entornos.

4. Contenido / Programa de la asignatura

4.1 Unidades docentes (bloques de contenidos)

- Redes de comunicaciones: modelado y estudio ·
- Amenazas persistentes en redes de comunicación ·
- Protocolos de compartición segura de información en redes ·
- Ciberseguridad pasiva y activa.

4.2 Bibliografía

- D.G. Zill, W.S. Wright, Advanced Engineering Mathematics, Jones and Bartlett Publishers Series in Matehmatics, 2011 o posterior
- E. Kreyszig, Advanced Engineering Mathematics, Wiley, 2011 o posterior
- R. Cohen, S. Havlin, Complex Networks, Structure, Robustness and Function, Cambridge University Press, 2010
- Douglas B. West, Introduction to graph theory, Prentice Hall, 2001 o posterior
- Dan A Smovici, Linear Algebra Tools for Data Mining, World Scientific, 2012 o posterior

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

Actividad Formativa	Competencias relacionadas	Horas	Presencialidad (%)
Clases, conferencias y técnicas expositivas	CG2, CSD5, CSD6	12	0
Actividades autónomas y en grupo (trabajos y lecturas dirigidas)	CSD5, CSD6	45	0
Pruebas de seguimiento y exposición de trabajos	CSD5, CSD6	10	50
Tutoría individual, participación en foros y otros medios colaborativos	CSD5, CSD6	8	0

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Redes de comunicaciones: modelado y estudio	1,5	
Amenazas persistentes en redes de comunicación	0,5	
Protocolos de compartición segura de información en redes	0,5	
Ciberseguridad pasiva y activa	0,5	

7. Evaluación

Instrumento / Procedimiento	Peso primera convocatoria	Peso segunda convocatoria
Evaluación sumativa, que incluye pruebas parciales individuales y prueba final	40%	40%
Realización de trabajos, proyectos, resolución de problemas y casos	50%	50%
Participación en foros y otros medios participativos	10%	10%

Criterios / Comentarios a la evaluación
• **Convocatoria ordinaria:** se realizarán los trabajos propuestos, entregándolos en tiempo y forma y la autoría será del alumno. Además, se comprobará la autoría de los mismos mediante algún mecanismo como entrevista personal o algún tipo de prueba. Por último, se tendrá que realizar de forma satisfactoria las pruebas de evaluación de respuesta corta o similar que se planteen a lo largo del curso. • **Convocatoria extraordinaria:** se realizará una prueba de evaluación que permita comprobar que se han adquirido las competencias desarrolladas en la asignatura.

8. Recursos de aprendizaje y apoyo tutorial del curso online

Transparencias

Enunciados de ejercicios

Cuestionarios de autoevaluación

Páginas web relacionadas

Bibliografía disponible en la Biblioteca

Tutorías individualizadas o en grupo a demanda de los alumnos

9. Consideraciones / Comentarios adicionales