Proyecto docente

Asignatura	Informática forense y auditoría de seguridad		
Materia	Seguridad de datos y ciberseguridad		
Titulación	Máster Universitario en Inteligencia de Negocio y Big Data en Entornos Seguros		
Plan		**Código**	01742015
Periodo de impartición	Primer semestre	**Tipo/Carácter**	Obligatoria
Nivel/Ciclo	Máster	**Curso**	1
Créditos ECTS	3		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Adrián Campazas Vega		
Datos de contacto (e-mail, teléfono…)	acamv@unileon.es		
Horario de tutorías	Lunes, martes y jueves de 11:00 a 13:00h		
Coordinador			
Departamento	Ingenierías Mecánica, Informática y Aeroespacial		
Web	https://ubuvirtual.ubu.es		
Descripción General	En esta asignatura se abordan los fundamentos sobre cómo auditar un sistema informático y las técnicas forenses más importantes. Además se estudia cómo tratar los datos desde el punto de vista de la ciberseguridad		

1. Situación / Sentido de la asignatura

1.1 Contextualización

En el almacenamiento y tratamiento de los datos de los sistemas informáticos, es necesario cumplir con unos mecanismos de seguridad que permitan garantizar la integridad y fiabilidad de los mismos. Además, se debe velar por el cumplimiento de los protocolos recomendados para garantizar la seguridad de los mismos. Realizando una auditoría de un sistema informático se puede evaluar el grado de cumplimiento de los planes establecidos, identificando posibles vulnerabilidades. Ante determinadas situaciones, puede ser necesaria la recolección de evidencias digitales mediante técnicas forenses y su análisis para determinar cómo está el sistema o recuperar información relevante. Todo ello debe estar debidamente documentado para que pueda ser utilizar en el proceso de mejora de las infraestructuras y protocolos empleados.

1.2 Relación con otras asignaturas

Tendencias emergentes en seguridad de datos

Fundamentos de ciberseguridad

1.3 Prerrequisitos

Conocimientos básicos en sistemas Windows

Conocimientos básicos en sistemas Linux

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

CSD2. Capacidad para la aplicación de técnicas de auditoría de sistemas de seguridad y de técnicas de análisis forense, en el contexto de la seguridad informática y la ciberseguridad

3. Resultados de aprendizaje

Al finalizar la asignatura, el alumno será capaz de comprender y saber aplicar las principales técnicas de análisis forense en el contexto de seguridad informática y la ciberseguridad. Además, el alumno conocerá los principales contenidos relacionados con la auditoría de sistemas de seguridad. Por último, conocerá y aprenderá a aplicar la normativa existente en materia de ciberseguridad.

4. Contenido / Programa de la asignatura

Bloque 1: Seguridad de la información

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

En este bloque se muestra como se han de tratar los datos dentro de una organización, como han de almacenarse y gestionarse desde un punto de vista de la seguridad informática atendiendo a la confidencialidad, disponibilidad e integridad de los mismos.

b. Objetivos de aprendizaje

Ser capaz de saber como manejar, almacenar o eliminar los datos de forma correcta y segura.

c. Contenidos y materiales de aprendizaje

- Introducción a la seguridad de la información
- Confidencialidad, integridad y disponibilidad
- Cifrado y codificación de datos
- Anonimato
- Almacenamiento de documentos

Apuntes en pdf. Vídeos explicativos de los apuntes. Prácticas guiadas. Informes y vídeos de otras fuentes.

d. Métodos docentes

Clase magistral. Aprendizaje basado en casos. Prácticas TIC. Elaboración de informes. Tutorías por email y videoconferencia.

e. Bibliografía básica

- Bill Nelson, Amelia Philips, Christopher Steuart, Guide to computer forensics and investigations. Processing Digital Evidence, Cengage Learning, 5ª Edición
- Patrick Engebretson, The basics of hacking and penetration testing, Syngress, Elsevier, 2ª Edición

f. Bibliografía complementaria

g. Recursos necesarios

Moodle en ubuvirtual

Comunicación por foro, email y videoconferencia.

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0,5	Semana 1
0,5	Semana 2

Bloque 2: **"**Auditoría y análisis forense**"**

Carga de trabajo en créditos ECTS: 2

a. Contextualización y justificación

Las técnicas forenses permiten obtener evidencias digitales que permitan emitir juicios sobre el estado de un sistema, si ha habido intrusiones, qué daños se han producido, etc. Al auditar un sistema, se analiza y se estudia cómo está de protegido, documentando todo el proceso. Actualmente, la ciberseguridad es crucial puesto que es necesario garantizar la protección de los datos frente a operaciones o accesos no deseados.

b. Objetivos de aprendizaje

Conocer las herramientas para realizar análisis forense en sistemas Windows, Linux y móviles. Comprender en qué consiste una auditoría, qué fases las forman y cómo se elabora un informe.

c. Contenidos y materiales de aprendizaje

- Vulnerabilidades
- Auditoría de sistemas
- Ingeniería social
- Análisis forense

Apuntes en pdf. Vídeos explicativos de los apuntes. Prácticas guiadas. Informes y vídeos de otras fuentes.

d. Métodos docentes

Clase magistral. Aprendizaje basado en problemas. Prácticas TIC. Elaboración de informes. Tutorías por email y videoconferencia.

e. Bibliografía básica

- Bill Nelson, Amelia Philips, Christopher Steuart, Guide to computer forensics and investigations. Processing Digital Evidence, Cengage Learning, 5ª Edición
- Patrick Engebretson, The basics of hacking and penetration testing, Syngress, Elsevier, 2ª Edición

f. Bibliografía complementaria

- Peter Kim, The hacker playbook 2, Secure Planet LLC, 2014
- Sara Baase, A gift of fire, Pearson, 4ª Edición
- Ben Clark, Red Team Field Manual, , 2013

g. Recursos necesarios

Moodle en ubuvirtual

Ordenador con máquinas virtuales

h. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO (detallar orden semanas)
0,5	Semana 3
0,5	Semana 4
0,5	Semana 5
0,5	Semana 6

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

Actividad Formativa	Competencias relacionadas	Horas	Presencialidad (%)
Clases, conferencias y técnicas expositivas	CG2, CSD2	12	0
Actividades autónomas y en grupo (trabajos y lecturas dirigidas)	CSD2	45	0
Pruebas de seguimiento y exposición de trabajos	CSD2	10	50
Tutoría individual, participación en foros y otros medios colaborativos	CSD2	8	0

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Seguridad de la información	1	Semana 1 y 2
Auditoría y análisis forense	2	Semana 3, 4, 5 y 6

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 en cada bloque, 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. Para ello, o bien se entregarán trabajos similares a los de la convocatoria ordinaria o bien se realizará un examen final donde se comprueben todas las competencias adquiridas

8. Consideraciones / Comentarios adicionales