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	Lidia Sánchez González		
Datos de contacto (e-mail, teléfono…)	lidia.sanchez@unileon.es 987291000 ext 5285		
Horario de tutorías	Lunes, martes y jueves de 11:00 a 13:00h		
Coordinador			
Departamento	Ingenierías Mecánica, Informática y Aeroespacial		
Web			
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 gestionar los riesgos existentes y cómo recoger y procesar evidencias digitales. Por último, se trata la elaboración de informes sobre todos los aspectos estudiados.		

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

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

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

4. Contenido / Programa de la asignatura

4.1 Unidades docentes (bloques de contenidos)

- Auditoría y tecnología forense.
- Gestión de riesgos.
- Evidencias digitales
- Procesado de pruebas y elaboración de informes.

4.2 Bibliografía

- 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
- 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

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
Auditoría y tecnología forense	1,5	
Gestión de riesgos	0,5	
Evidencias digitales	0,5	
Procesado de pruebas y elaboración de informes	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:** • **Convocatoria extraordinaria:**

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