ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

93001003 - Auditoría técnica de seguridad

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2018/19 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001003 - Auditoría técnica de seguridad
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Primer semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	09AW - Master universitario en ciberseguridad
Centro en el que se imparte	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2018-19

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Carlos Carrillo Sanchez (Coordinador/a)	A4401	carlos.carrillo@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Competencias y resultados de aprendizaje

3.1. Competencias

CB07 - 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

CB08 - 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

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

CE01 - Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un sistema de ciberseguridad en una organización

CE08 - Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa

CE09 - Capacidad de realizar una auditoría de ciberseguridad de un sistema, tanto a nivel técnico como organizativo

CG02 - Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización

CG05 - Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia

CT09 - Capacidad de análisis y síntesis

3.2. Resultados del aprendizaje

RA26 - Realización de una auditoría de ciberseguridad para las organizaciones.

RA3 - .Conocer y comprender los elementos que intervienen en un sistema de ciberseguridad así como crear las infraestructuras y procesos necesarios para ello

RA4 - Comprender la importancia de la Ingeniería Social, los atacantes y ataques más comunes y aplicar las técnicas para prevenir dichos ataques

RA1 - .Comprender la importancia de la ciberseguridad para las organizaciones y su gobernanza corporativa así como los principios, estructuras, roles y responsabilidades que deben seguirse para su gestión

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

SE presentarán conceptos relacionados con el Ciberespacio, la Ciberseguridad y los Delitos Informáticos, que nos establecerán el ámbito de aplicación de una auditoria en Ciberseguridad.

Se presentarán las principales amenazas existentes en el mundo global y cual es la respuesta que diferentes organismos nacionales e internacionales plantean para evitar, y en su defecto, minimizar las consecuencias de una brecha en ciberseguridad

El alumno desarrollarás las habilidades orientadas a planificar una auditoria desarrollando las estrategias para realizar múltiples tests de penetración, análisis de la información recopilada empleando diferentes técnicas, en las que se incluye técnicas de ingeniería social. El objetivo de estas técnicas es detectar posibles fallos de seguridad en el sistema a auditar.

4.2. Temario de la asignatura

1. Introducción a la ciberseguridad

2. La seguridad real de la infraestructura

   2.1. Introducción a un Sistema de Gestion de Seguridad de la Información (SGSI)

   2.2. Metodología

   2.3. Modelo de Seguridad

3. Técnicas de evaluación de la seguridad de una red y un sistema

   3.1. Test de penetración

   3.2. Recopilación de información. Footprinting

4. Herramientas y Análisis de Datos.

   4.1. En entornos Linux

      4.1.1. Kali linux

         4.1.1.1. Instalación

         4.1.1.2. Uso de herramientas para auditoria ciberseguridad

            4.1.1.2.1. Introducción a la obtención de datos con Maltego

            4.1.1.2.2. Recon-Ng

            4.1.1.2.3. Introducción a NEssus

            4.1.1.2.4. Herramientas de escaneo de red. Wireshark.

            4.1.1.2.5. Uso de otras herramientas

         4.1.1.3. Instalación de otras herramientas

   4.2. En entornos Windows

      4.2.1. Instalación de herramientas para auditoria ciberseguridad

      4.2.2. Uso de Herramientas para auditoria ciberseguridad

         4.2.2.1. Introducción a la obtención de datos con Maltego

         4.2.2.2. Introducción a Nessus

         4.2.2.3. Herramientas de escaneo de red

         4.2.2.4. Uso de otras herramientas en el entorno Windows

   4.3. Metasploit

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**Tema 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral			
2	**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 3** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Sesión de laboratorio. Tema 3** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio		
3	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Sesión de Laboratorio. Tema 3** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio **Sesión de laboratorio. Tema 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
4	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Sesión de laboratorio. Tema 4** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio		
5	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Sesión de laboratorio. Tema 4** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio		
6	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral	**Sesión de laboratorio. Tema 4** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio		
7				**Examen supuesto práctico** EP: Técnica del tipo Examen de Prácticas Evaluación continua y sólo prueba final Duración: 04:00
8				
9				
10				
11				
12				

13				
14				
15				
16				
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
7	Examen supuesto práctico	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	100%	0 / 10	CB07 CB08 CB10 CG02 CG05 CT09 CE01 CE08 CE09

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
7	Examen supuesto práctico	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	100%	0 / 10	CB07 CB08 CB10 CG02 CG05 CT09 CE01 CE08 CE09

6.1.3. Evaluación convocatoria extraordinaria

No se ha definido la evaluación extraordinaria.

6.2. Criterios de evaluación

El alumno deberá trabajar de forma continuada, asistiendo y participando en las clases teóricas y de laboratorio. El objetivo fundamental de la evaluación continua es que los alumnos estudien, comprendan y apliquen los principales conceptos de la asignatura de forma gradual. Por ello, se considera que es de especial importancia la asistencia a clase y el trabajo sistemático que incluye la realización de programas y ejercicios sobre los contenidos estudiados en las clases teóricas.

Examen supuesto práctico. El alumno deberá realizar una auditoria a una sistema de información. Este sistema estará formado por un equipo vulnerable frente a deferentes amenazas vistas en las sesiones teóricas y prácticas. Se valorará la capacidad del alumno en analizar el sistema, detectar las vulnerabilidades conocidas y en descubrir otras posibles vulnerabilidades que puedan presentar el sistema

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Plataforma institucional de tele-enseñanza de la UPM: Moodle.	Recursos web	Herramienta telemática que incluye informaciones, avisos, documentación y actividades de autoevaluación para el correcto seguimiento de la asignatura por los alumnos
Equipamiento audiovisual e informático en aulas de teoría y módulos de laboratorio	Equipamiento	
Videos relacionados con Ciberseguridad	Recursos web	
Documentación generada a tal fin	Bibliografía	