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

2021/22 - 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 responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2021-22

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. Sin horario.Se especificará en el directorio personal existente en la Web de la ETSIS Telecomunicación

David Jesus Meltzer Camino	A4403	david.meltzer@upm.es	Sin horario. Sin horario.Se especificará en el directorio personal existente en la Web de la ETSIS Telecomunicación

* 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

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

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 la Ciberseguridad que nos establecerán el ámbito de aplicación de una auditoria en Ciberseguridad.

El alumno desarrollará las habilidades orientadas a planificar una auditoria. Entre estas estratégias se realizarán múltiples tests de penetración y su posterior análisis de la información recopilada. Para la realización de estos tests se tendrá en cuenta técnicas de ingeniería social. El objetivo de estos tests es detectar posibles fallos de seguridad en el sistema a auditar.

La asignatura tiene una fuerte componente práctica. Para el desarrollo de la asignatura se utilizarán máquinas virtuales con diferentes roles (Auditora, auditada, etc).

Al final de la asignatura, el alumno tendrá el conocimiento de hacker ético o auditor de ciberseguridad

4.2. Temario de la asignatura

1. Introducción a la ciberseguridad
2. Técnicas de evaluación de la seguridad de una red y un sistema
    2.1. Test de penetración
    2.2. Recopilación de información. Footprinting
    2.3. Recopilación de información mediate metadatos
3. Herramientas para una auditoría de ciberseguridad
    3.1. Herramientas Web para la auditoria
    3.2. Herramientas para identificar fuga de información
    3.3. Herramientas en entornos Windows y linux para uso de auditoría
    3.4. Kali linux.
        3.4.1. Uso de la herramienta para auditoría de ciberseguridad

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Tele-enseñanza	Actividades de evaluación
1				
2				
3				
4				
5				
6	**Tema 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral		**Tema 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral	
7	**Tema 2** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Sesión de laboratorio. Tema 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Sesión de laboratorio. Tema 5** Duración: 01:00 OT: Otras actividades formativas		**Tema 2** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Sesión de laboratorio. Tema 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio **Sesión de laboratorio. Tema 5** Duración: 01:00 OT: Otras actividades formativas	
8	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Sesión de Laboratorio. Tema 3** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio		**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Sesión de Laboratorio. Tema 3** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio	
9				
10	**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Sesión de laboratorio. Tema 3** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio		**Tema 3** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Sesión de laboratorio. Tema 3** Duración: 03:30 PL: Actividad del tipo Prácticas de Laboratorio	**Memoria de auditoria técnica basada en la información obtenida en el proceso de auditoría. El eje de esta información será las vulnerabilidades en temas de ciberseguridad existentes en los diferentes dominios analizados con las herramientas del tema 2 y 3** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 00:30
11				

12				
13				
14	**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		**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	
15	**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Sesión de laboratorio. Tema 4** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio		**Tema 4** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Sesión de laboratorio. Tema 4** Duración: 03:00 PL: Actividad del tipo Prácticas de Laboratorio	**Memoria de auditoria técnica basada en la información obtenida en el proceso de auditoría. El eje de esta información será las vulnerabilidades en temas de ciberseguridad existentes en los diferentes dominios analizados con las herramientas del tema 4** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 00:30
16				
17				**Examen supuesto práctico. Detección de vulnerabilidades en entornos reales o virtuales** EP: Técnica del tipo Examen de Prácticas Evaluación continua Presencial Duración: 04:00 **Convocatoria Itinerario Solo Final. Examen supuesto práctico. Incluye todo el trabajo de auditoria técnica desarrolado a lo largo del curso** EP: Técnica del tipo Examen de Prácticas Evaluación sólo prueba final Presencial Duración: 04:00

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 derivadas de la situación creada por la COVID-19.

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
10	Memoria de auditoria técnica basada en la información obtenida en el proceso de auditoría. El eje de esta información será las vulnerabilidades en temas de ciberseguridad existentes en los diferentes dominios analizados con las herramientas del tema 2 y 3	TI: Técnica del tipo Trabajo Individual	No Presencial	00:30	30%	3 / 10	CT12 CG05 CB07 CB08 CB10 CT09 CE08 CE09 CG02 CE01
15	Memoria de auditoria técnica basada en la información obtenida en el proceso de auditoría. El eje de esta información será las vulnerabilidades en temas de ciberseguridad existentes en los diferentes dominios analizados con las herramientas del tema 4	TI: Técnica del tipo Trabajo Individual	No Presencial	00:30	30%	3 / 10	CT12 CG05 CB07 CB08 CB10 CT09 CE08 CE09 CG02 CE01
17	Examen supuesto práctico. Detección de vulnerabilidades en entornos reales o virtuales	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	40%	4 / 10	CT12 CG05 CB07 CB08 CB10 CT09 CE08 CE09 CG02 CE01

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas

17	Convocatoria Itinerario Solo Final. Examen supuesto práctico. Incluye todo el trabajo de auditoria técnica desarrolado a lo largo del curso	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	100%	5 / 10	CE01 CG02 CT12 CG05 CB07 CB08 CB10 CT09 CE08 CE09

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Convocatoria Extraordinaria. Examen supuesto práctico. Incluye todo el trabajo de auditoria técnica desarrolado a lo largo del curso	EP: Técnica del tipo Examen de Prácticas	Presencial	04:00	100%	5 / 10	CT12 CE01 CG02 CG05 CB07 CB08 CB10 CT09 CE08 CE09

6.2. Criterios de evaluación

El alumno **podrá elegir** entre dos itinerarios de evaluación según la normativa de la UPM en esta materia, como son:

- De evaluación continua.
- De sólo prueba final.

Itinerario de evaluación continua.

Es el itinerario por defecto. El alumno deberá trabajar de forma continuada durante todo el cuatrimestre, asistiendo y participando en las clases teóricas y de laboratorio. El objetivo fundamental de la evaluación continua es que los alumnos estudien y comprendan 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 todas las actividades relacionadas con los contenidos estudiados en las clases teóricas. En el itinerario de evaluación continua se realizarán tres pruebas de evaluación comunes a todos los alumnos. Estas pruebas se realizarán en las semanas indicadas en el anterior cronograma. La duración, peso en la nota final de la asignatura y nota mínima requerida está tambieén reflejada en dicho cronograma. Todas las pruebas se realizarán en el aula asignada a esta asignaturam ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

Itinerario de evaluación solo prueba final.

El alumno deberá realizar una práctica final que será el compendio de todas y cada una de las prácticas realizadas por los alumnos que realicen una evaluación continua. Además se realizará una examen-práctica más que se realizará el día programado. Por lo tanto, será objeto de examen todo los conceptos impartidos en las diferentes actividades que se realicen, incluido aquellas presentaciones realizadas por profesionales expertos en el ámbito de la ciberseguridad.

Esta prueba se realizará en la semana indicada en el anterior cronograma. La duración, peso en la nota final de la asignatura y nota mínima requerida está tambieén reflejada en dicho cronograma. Está prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

Convocatoria extraordinaria.

Es común a las dos modalidades.

El alumno deberá realizar una práctica final que será el compendio de todas y cada una de las prácticas realizadas por los alumnos que realicen una evaluación continua. Además se realizará una examen-práctica más que se realizará el día programado. Por lo tanto, será objeto de examen todo los conceptos impartidos en las diferentes

actividades que se realicen, incluido aquellas presentaciones realizadas por profesionales expertos en el ámbito de la ciberseguridad.

Esta prueba se realizará en la semana indicada en el anterior cronograma. La duración, peso en la nota final de la asignatura y nota mínima requerida está tambieén reflejada en dicho cronograma. Está prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

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	
Exposiciones temáticas	Otros	Se invitarán a profesionales relacionados con el ámbito de la ciberseguridad
Plataforma Teams	Recursos web	
Máquinas virtuales	Otros	

8. Otra información

8.1. Otra información sobre la asignatura

La situación sanitaria causada por la pandemia COVID-19 obliga a restringir el aforo de las aulas y por ello se ha decidido que el modelo de docencia de este semestre sea híbrido o mixto. Se establecerán turnos de presencialidad dentro de los grupos, de forma que cada semana un turno asistirá a clase en el aula (columna "actividad en el aula" del cronograma), mientras el resto de los turnos se conectarán a la clase de forma telemática (columna "tele-enseñanza). Y cada semana será un turno diferente el que acuda al aula. Si cambian las condiciones sanitarias y se pudieran impartir clases presenciales con normalidad, todos los estudiantes acudirán a las aulas a recibir las clases indicadas en la columna "actividad en el aula". Si, por el contrario, empeoraran las condiciones sanitarias, todos los alumnos pasarían a conectarse a las clases en remoto de la columna "teleenseñanza".