



UNIVERSIDAD
POLITÉCNICA
DE MADRID

PROCESO DE
COORDINACIÓN DE LAS
ENSEÑANZAS PR/CL/001



E.T.S. de Ingenieros de
Telecomunicacion

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

2024/25 - Primer semestre

Índice

Guía de Aprendizaje

| | |
|--|----|
| 1. Datos descriptivos..... | 1 |
| 2. Profesorado..... | 1 |
| 3. Conocimientos previos recomendados..... | 2 |
| 4. Competencias y resultados de aprendizaje..... | 2 |
| 5. Descripción de la asignatura y temario..... | 4 |
| 6. Cronograma..... | 6 |
| 7. Actividades y criterios de evaluación..... | 8 |
| 8. Recursos didácticos..... | 11 |
| 9. Otra información..... | 11 |

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 | 2024-25 |

2. Profesorado

2.1. Profesorado implicado en la docencia

| Nombre | Despacho | Correo electrónico | Horario de tutorías * |
|--|-----------------|----------------------------|--|
| Julio Cesar Hernandez Castro (Coordinador/a) | 1208 | jc.hernandez.castro@upm.es | Sin horario. Previo contacto y acuerdo via email con los alumnos interesados. |
| Juan Manuel Castelo Gomez | 4105 | juanmanuel.castelo@upm.es | Sin horario. Previo contacto y acuerdo via email con los alumnos interesados. |

| | | | |
|----------------------------|------|---------------------------|---|
| Alejandro Barreiro Morante | 1126 | alejandro.bmorante@upm.es | Sin horario. Previo contacto y acuerdo via email con los alumnos interesados. |
|----------------------------|------|---------------------------|---|

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

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Master Universitario en Ciberseguridad no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Seguridad en redes, desarrollo de software de seguridad, pen-testing, honeypots, IDSs, sniffers, fuzzers, herramientas de diagnostico local y remoto.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CB06 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

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

CB09 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las

sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

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

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

4.2. Resultados del aprendizaje

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

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

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

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

Se presentarán conceptos relacionados con la Ciberseguridad que nos establecerán el ámbito de aplicación de una auditoría en Ciberseguridad.

El alumno desarrollará las habilidades orientadas a planificar una auditoría. Entre estas estrategias se realizarán múltiples tests de penetración y el posterior análisis detallado 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

5.2. 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 mediante metadatos
3. Herramientas para una auditoría de ciberseguridad
 - 3.1. Herramientas Web para la auditoría
 - 3.2. Herramientas en entornos Windows y linux para uso de auditoría
 - 3.3. Kali linux.
 - 3.3.1. Uso de la herramienta para auditoría de ciberseguridad
 - 3.3.2. Instalación de módulos

3.4. Metasploit

3.4.1. Uso de exploit para pentesting

3.4.2. Programación de exploit

4. Hacking ético

4.1. Detección de vulnerabilidades en entornos Windows

4.2. Detección de vulnerabilidades en entornos Linux

4.3. Detección de vulnerabilidades en entornos Web

6. Cronograma

6.1. Cronograma de la asignatura *

| Sem | Actividad tipo 1 | Actividad tipo 2 | Tele-enseñanza | Actividades de evaluación |
|-----|--|--|----------------|--|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | Tema 1 Duración: 04:00 LM: Actividad del tipo Lección Magistral | | | |
| 10 | Tema 2 Duración: 02:00 LM: Actividad del tipo Lección Magistral | Sesión de laboratorio. Tema 2 Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio | | |
| 11 | Tema 3 Duración: 00:30 LM: Actividad del tipo Lección Magistral | Sesión de laboratorio. Tema 3 Duración: 01:30 PL: Actividad del tipo Prácticas de Laboratorio | | Prueba de evaluación relacionada con los conceptos teóricos desarrollados en el tema 1 y 2 EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 02:00 |
| 12 | 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 auditoría 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 TI: Técnica del tipo Trabajo Individual Evaluación Progresiva No presencial Duración: 00:00 |
| 13 | 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 | | Memoria de auditoría 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 3 TI: Técnica del tipo Trabajo Individual Evaluación Progresiva No presencial Duración: 00:00 |

| | | | | |
|----|--|--|--|--|
| 14 | 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 | | |
| 15 | | | | |
| 16 | | | | |
| 17 | | | | Memoria de auditoría 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 Progresiva No presencial Duración: 00:00 |

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.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

| Sem. | Descripción | Modalidad | Tipo | Duración | Peso en la nota | Nota mínima | Competencias evaluadas |
|------|---|---|---------------|----------|-----------------|-------------|--|
| 11 | Prueba de evaluación relacionada con los conceptos teóricos desarrollados en el tema 1 y 2 | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 20% | 0 / 10 | CB07 CB10 CG02 CG05 CT09 CT12 CE01 CE09 |
| 12 | Memoria de auditoría 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 | TI: Técnica del tipo Trabajo Individual | No Presencial | 00:00 | 20% | 0 / 10 | CB07 CB08 CB10 CG02 CG05 CT09 CT12 CE01 CE09 |
| 13 | Memoria de auditoría 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 3 | TI: Técnica del tipo Trabajo Individual | No Presencial | 00:00 | 30% | 0 / 10 | CB07 CB08 CB10 CG02 CG05 CT09 CT12 CE01 CE09 |
| 17 | Memoria de auditoría 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 | 00:00 | 30% | 0 / 10 | CB07 CB08 CB10 CG02 CG05 CT09 CT12 CE01 CE09 |

7.1.2. Prueba evaluación global

No se ha definido la evaluación sólo por prueba final.

7.1.3. 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 auditoría técnica desarrollado a lo largo del curso | EP: Técnica del tipo Examen de Prácticas | Presencial | 04:00 | 100% | 5 / 10 | CB07 CB08 CB10 CG02 CG05 CT09 CT12 CE01 CE09 |

7.2. Criterios de evaluación

Todas las pruebas de evaluación continuas detalladas en esta guía son pruebas de evaluación progresiva según el nuevo reglamento de evaluación que se aplicará en el curso 22/23

Itinerario de evaluación progresiva.

El alumno deberá trabajar de forma progresiva durante todo el cuatrimestre, asistiendo y participando en las clases teóricas y de laboratorio. El objetivo fundamental de la evaluación progresiva 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 progresiva se realizarán cuatro pruebas de evaluación comunes a todos los alumnos. Estas pruebas se realizarán en las semanas indicadas en el anterior cronograma. La duración y peso en la nota final de la asignatura está también reflejada en dicho cronograma. La primera prueba de evaluación será un examen escrito, y el resto de pruebas de evaluación progresivas se entregaran en la plataforma moodle.

Para aprobar la asignatura siguiendo este itinerario, es necesario sacar al menos un 5.0 una vez se sumen las cuatro pruebas con sus pesos anteriormente indicados

Itinerario de evaluación ordinaria.

No existe. El método de evaluación es progresiva, y la última prueba de evaluación progresiva coincide con la fecha prevista de evaluación de esta asignatura, según consta en el calendario

Convocatoria extraordinaria.

El alumno deberá realizar una práctica final que será el compendio de todas y cada una de las pruebas realizadas por los alumnos que realicen una evaluación continua. El peso asignado a esta prueba y su duración está indicado en el diagrama anterior.

Esta prueba se realizará en la semana indicada en el anterior cronograma. Esta prueba se realizará en el aula asignada a esta asignatura ya que será necesario la utilización de dispositivos de información, ordenadores, etc.

8. Recursos didácticos

8.1. 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 | |

9. Otra información

9.1. Otra información sobre la asignatura