

## 1. DATOS BÁSICOS

<b>Asignatura</b>	Auditoria y Cumplimiento del Marco Jurídico
<b>Titulación</b>	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones
<b>Escuela/ Facultad</b>	Arquitectura, Ingeniería y Diseño
<b>Curso</b>	Primero
<b>ECTS</b>	6 ECTS
<b>Carácter</b>	Obligatorio
<b>Idioma/s</b>	Castellano
<b>Modalidad</b>	Presencial - ODCS001108 Online - P630001108
<b>Semestre</b>	Segundo semestre
<b>Curso académico</b>	2024/2025
<b>Docente coordinador</b>	Presencial: D. Pablo González Pérez Online: Prof. Santiago Hernández Ramos

## 2. PRESENTACIÓN

El estudiante se familiarizará con la normativa vigente. Además, aprenderá a realizar análisis forense y a realizar auditorías informáticas poniéndolo en práctica a través de las herramientas más utilizadas hoy en día.

## 3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

### Competencias básicas:

- CG1: Capacidad para la dirección técnica y la dirección de proyectos en el ámbito de la Seguridad de las Tecnologías de la Información y las Comunicaciones.
- CG.2. Aprender a aplicar a entornos nuevos o poco conocidos, dentro de contextos más amplios (o multidisciplinares), los conceptos, principios, teorías o modelos relacionados con su área de estudio.
- CG.6. Capacidad para integrarse en equipos de trabajo multidisciplinares de manera eficaz y cooperativa.

### Competencias específicas:

- CE.17. Ser capaces de hacer un análisis forense sobre un sistema.
- CE.18. Comprender y aplicar el marco legislativo vigente.
- CE20. Conocer los métodos de trabajo de las empresas consultoras de seguridad y aprender a escribir informes y procedimientos sobre las tareas básicas relacionadas con la seguridad de la organización.

### Resultados de aprendizaje:

- RA1. El estudiante será capaz de aplicar los conceptos básicos utilizando técnicas de aprendizaje cooperativo.
- RA2: El estudiante será capaz de trabajar en equipo, comunicarse de forma oral y escrita y aplicar los contenidos de las asignaturas para realizar juicios críticos.

- RA6. Desarrollo de informes para su aceptación por parte de la empresa cliente sobre la verificación e inspección de la seguridad de sus sistemas.

En la tabla inferior se muestra la relación entre las competencias que se desarrollan en la asignatura y los resultados de aprendizaje que se persiguen:

Competencias	Resultados de aprendizaje
CG2, CG6, CE17, CE18, CE20	RA1
CG6, CE20	RA2, RA6

## 4. CONTENIDOS

- 8.1 Cumplimiento del marco jurídico
- 8.2 Análisis forense
- 8.3 Práctica de utilización de herramientas de seguridad

## 5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

A continuación, se indican los tipos de metodologías de enseñanza-aprendizaje que se aplicarán:

- Clase magistral.
- Método del caso.
- Aprendizaje cooperativo.
- Aprendizaje basado en proyectos.
- 

## 6. ACTIVIDADES FORMATIVAS

A continuación, se identifican los tipos de actividades formativas que se realizarán y la dedicación en horas del estudiante a cada una de ellas:

### Modalidad presencial:

Actividad formativa	Número de horas
A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición	25 h
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	56,25 h
A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	43,75 h
<b>TOTAL</b>	<b>150h</b>

**Modalidad online:**

Actividad formativa	Número de horas
A1. Participación en debates y foros de discusión moderados por el profesor	32,5h
A2. Realización de actividades aplicativas: estudios de caso, resolución de problemas, elaboración de planes, análisis de situaciones profesionales, etc.	25h
A3. Trabajo integrador del módulo	10h
A4. Realización de actividades aplicativas: estudios de caso, resolución de problemas, elaboración de planes, análisis de situaciones profesionales, etc.	25h
A5. Estudio independiente del alumno	32,5h
A6. Tutoría y evaluación	25h
<b>TOTAL</b>	<b>150h</b>

## 7. EVALUACIÓN

A continuación, se relacionan los sistemas de evaluación, así como su peso sobre la calificación total de la asignatura:

**Modalidad presencial:**

Sistema de evaluación	Peso
Ejercicios para resolver	15%
Cuestionario de cumplimiento del marco jurídico	25%
Análisis forense	30%
Informe auditoría	30%

**Modalidad online:**

Sistema de evaluación	Peso
A1. Análisis del artículo 197 y 197bis del Código Penal	10%
A2. La evaluación del impacto a la privacidad	15%
A3. Sujetos obligados en la LSSI	10%
A4. Elaboración de un informe de análisis forense	20%
A5. Realización de una auditoría práctica de seguridad	20%
A6. Prueba de Conocimientos	25%

En el Campus Virtual, cuando accedas a la asignatura, podrás consultar en detalle las actividades de evaluación que debes realizar, así como las fechas de entrega y los procedimientos de evaluación de cada una de ellas.

### **7.1. Convocatoria ordinaria**

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

En la modalidad online será necesario obtener en la prueba de conocimiento una calificación igual o superior a 5.

### **7.2. Convocatoria extraordinaria**

Para superar la asignatura en convocatoria ordinaria deberás obtener una calificación mayor o igual que 5,0 sobre 10,0 en la calificación final (media ponderada) de la asignatura.

En todo caso, será necesario que obtengas una calificación mayor o igual que 4,0 en la prueba final, para que la misma pueda hacer media con el resto de actividades.

En la modalidad online será necesario obtener en la prueba de conocimiento una calificación igual o superior a 5.

Se deben entregar las actividades no superadas en convocatoria ordinaria, tras haber recibido las correcciones correspondientes a las mismas por parte del docente, o bien aquellas que no fueron entregadas.

## **8. CRONOGRAMA**

En este apartado se indica el cronograma con fechas de entrega de actividades evaluables de la asignatura:

### **Modalidad presencial:**

<b>Actividades evaluables</b>	<b>Fecha</b>
Ejercicios para resolver	Sem 3
Cuestionario de cumplimiento del marco jurídico	Sem 6
Análisis forense	Sem 9

Informe auditoría	Sem 12
-------------------	--------

**Modalidad online:**

Actividades evaluables	Fecha
A1. Análisis del artículo 197 y 197bis del Código Penal	Sem 2
A2. La evaluación del impacto a la privacidad	Sem 4
A3. Sujetos obligados en la LSSI	Sem 6
A4. Elaboración de un informe de análisis forense	Sem 8
A5. Realización de una auditoría práctica de seguridad	Sem 10
A6. Prueba de Conocimientos	Sem 12

Este cronograma podrá sufrir modificaciones por razones logísticas de las actividades. Cualquier modificación será notificada al estudiante en tiempo y forma.

## 9. BIBLIOGRAFÍA

A continuación, se indica bibliografía recomendada:

### M6.1. La Seguridad en la comunicaciones

- La Segmentación de red, <https://www.cisco.com/c/en/us/about/securitycenter/framework-segmentation.html>
- Wifi Alliance: <https://www.wi-fi.org>
- IEEE EAP and 802.1x: <http://ieeexplore.ieee.org/document/1561920/>
- Wikipedia [https://en.wikipedia.org/wiki/IEEE\\_802.11](https://en.wikipedia.org/wiki/IEEE_802.11)
- Modelo OSI: [https://es.wikipedia.org/wiki/Modelo\\_OSI](https://es.wikipedia.org/wiki/Modelo_OSI)
- "Comunicaciones y Redes de Computadores". 7ª edición. William Stallings. Ed. Prentice-Hall. 2004.
- "Redes de computadores". 4ª edición. Andrew S. Tanenbaum. Ed. Prentice-Hall. 2003.

### M6.2. Práctica profesional de configuración segura de redes inalámbricas

- "Hacking Exposed Wireless" (3ª Ed): <http://www.hackingexposedwireless.com>

- "Kali Linux Wireless Penetration Testing: Beginner's Guide" (3ª Ed): <https://www.packtpub.com/networking-and-servers/kali-linux-wireless-penetration-testing-beginner%E2%80%99s-guide-third-edition>
- DinoSec Lab: <http://www.dinosec.com/es/lab.html>
- DinoSec Blog: <http://blog.dinosec.com>

### **M6.3. Práctica profesional de instalación y configuración cortafuegos**

- "Ataques a redes de datos IPv4 e IPv6" (3ª Ed). Chema Alonso, Juan Luis G. Rambla. Pablo González. Ed. Oxword.
- Flu Project Blog: <http://flu-project.com>
- "Linux Iptables". Gregor N. Purdy. Ed. O'Reilly. 2004.

## **10. UNIDAD DE ORIENTACIÓN EDUCATIVA Y DIVERSIDAD**

Desde la Unidad de Orientación Educativa y Diversidad (ODI) ofrecemos acompañamiento a nuestros estudiantes a lo largo de su vida universitaria para ayudarles a alcanzar sus logros académicos. Otros de los pilares de nuestra actuación son la inclusión del estudiante con necesidades específicas de apoyo educativo, la accesibilidad universal en los distintos campus de la universidad y la equiparación de oportunidades.

Desde esta Unidad se ofrece a los estudiantes:

1. Acompañamiento y seguimiento mediante la realización de asesorías y planes personalizados a estudiantes que necesitan mejorar su rendimiento académico.
2. En materia de atención a la diversidad, se realizan ajustes curriculares no significativos, es decir, a nivel de metodología y evaluación, en aquellos alumnos con necesidades específicas de apoyo educativo persiguiendo con ello una equidad de oportunidades para todos los estudiantes.
3. Ofrecemos a los estudiantes diferentes recursos formativos extracurriculares para desarrollar diversas competencias que les enriquecerán en su desarrollo personal y profesional.
4. Orientación vocacional mediante la dotación de herramientas y asesorías a estudiantes con dudas vocacionales o que creen que se han equivocado en la elección de la titulación.

Los estudiantes que necesiten apoyo educativo pueden escribirnos a:

[orientacioneducativa@universidadeuropea.es](mailto:orientacioneducativa@universidadeuropea.es)

## **11. ENCUESTAS DE SATISFACCIÓN**

¡Tú opinión importa!

La Universidad Europea te anima a participar en las encuestas de satisfacción para detectar puntos fuertes y áreas de mejora sobre el profesorado, la titulación y el proceso de enseñanza-aprendizaje.

Las encuestas estarán disponibles en el espacio de encuestas de tu campus virtual o a través de tu correo electrónico.

Tu valoración es necesaria para mejorar la calidad de la titulación.

Muchas gracias por tu participación.