1. DATOS BÁSICOS

Asignatura	Análisis de Riesgos
Titulación	Máster Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones
Escuela/ Facultad	Arquitectura, Ingeniería y Diseño
Curso	Primero
ECTS	6 ECTS
Carácter	Obligatorio
Idioma/s	Castellano
Modalidad	Presencial – 0DCS001102 Online – P630001102
Semestre	Primer semestre
Curso académico	2024/2025
Docente coordinador	
Docente	Presencial: Prof. Zulayka Vera Urueña y Prof. Nestor Soiza Vázquez Online: Dr. José Antonio Rubio y Prof. Marcos Gómez Hidalgo

2. PRESENTACIÓN

En este módulo el estudiante profundizará en las metodologías para el Análisis y Evaluación de Riesgos, así como técnicas para su gestión profundizando en una de estas metodologías a través de su aplicación a un caso de estudio.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias básicas:

- CG6: 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.
- CG7: 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.

Competencias específicas:

- CE4: Ser capaces de aplicar una metodología para el análisis y evaluación de riesgos, así como saber utilizar las herramientas para su gestión.
- CE5: Identificar la combinación de controles técnicos, humanos y de procedimiento para ayudar a eliminar o reducir los riesgos de seguridad hasta un nivel manejable.
- 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 elaborar informes para su aceptación por parte de la empresa cliente sobre la resolución del caso práctico de aplicación de la metodología de análisis de riesgos.

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
CE4, CE5, CE20	RA1
CG6, CG7, CE4, CE5, CE20	RA2

4. CONTENIDOS

La materia está organizada en los siguientes contenidos:

2.1 Riesgos y amenazas de los Sistemas de Información

2.2 Análisis de riesgos

2.3 Práctica de inspección de seguridad de los sistemas

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

AA 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	50 h

A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	50 h
TOTAL	**150**

Modalidad online:

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

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
Elaboración y presentación de trabajos 1	15%
Elaboración y presentación de trabajos 2	15%
Resolución de un caso práctico aplicando la metodología de análisis de riesgos	20%
Práctica individual del análisis de un área de seguridad de una organización basándose en la metodología EDR	15%
Práctica grupal, aplicando metodología para la inspección de seguridad ante un tipo de empresa planteada utilizando herramientas de auditoría, OSINT y/o metodología EDR	20%
Análisis de riesgos en entorno financiero	15%

Sistema de evaluación	Peso
A1. Análisis de la amenaza cibernética conocidas como botnet.	15%
A2. Trabajo Integrador: Realizar un proyecto de análisis de riesgos	30%
A3. Trabajo Integrador: Realizar una auditoría e inspección de sistemas y redes de una organización	30%
A4 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.

En ambas convocatorias (ordinaria y extraordinaria) se permitirá la entrega tardía con un máximo de una semana a partir de la fecha de entrega fijada, con una **penalización de 0,25 puntos sobre 10 por día de retraso**. Una vez superada la semana, no se permitirá la entrega salvo casos excepcionales de fuerza mayor que deba estudiar el personal docente implicado.

Las actividades se entregarán en el campus virtual, no siendo válida la entrega por correo electrónico.

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.
.

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.

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.

Modalidad online:

Sistema de evaluación	Peso
A1. Análisis de la amenaza cibernética conocidas como botnet.	15%
A2. Trabajo Integrador: Realizar un proyecto de análisis de riesgos	30%

A3. Trabajo Integrador: Realizar una auditoría e inspección de sistemas y redes de una organización	30%
A4 Prueba de conocimientos	25%

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

En ambas convocatorias (ordinaria y extraordinaria) se permitirá la entrega tardía con un máximo de una semana a partir de la fecha de entrega fijada, con una **penalización de 0,25 puntos sobre 10 por día de retraso**. Una vez superada esta semana, no se permitirá la entrega salvo casos excepcionales de fuerza mayor que deba estudiar el personal docente implicado.

Las actividades se entregarán en el campus virtual, no siendo válida la entrega por correo electrónico.

7.3. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota media ponderada de las actividades que figuran en la tabla (A1, A2 y A3), exceptuando la prueba de conocimiento, igual o superior a 5.
- Obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.4. Convocatoria extraordinaria

Para superar la asignatura en convocatoria extraordinaria deberás:

- Obtener una nota media ponderada de las actividades que figuran en la tabla (A1, A2 y A3), exceptuando la prueba de conocimiento, igual o superior a 5.
- Obtener en la prueba de conocimiento una calificación igual o superior a 5.

8. CRONOGRAMA

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

Modalidad presencial:

Actividades evaluables	Fecha
Elaboración y presentación de trabajos 1	SEM3
Elaboración y presentación de trabajos 2	SEM5
Resolución de un caso práctico aplicando la metodología de análisis de riesgos	SEM7

Práctica individual del análisis de un área de seguridad de una organización basándose en la metodología EDR	SEM8
Práctica grupal, aplicando metodología para la inspección de seguridad ante un tipo de empresa planteada utilizando herramientas de auditoría, OSINT y/o metodología EDR	SEM10
Análisis de riesgos en entorno financiero	SEM12

Modalidad online:

Actividades evaluables	Fecha
A1. Análisis de la amenaza cibernética conocidas como botnet.	SEM 3
A2. Trabajo Integrador: Realizar un proyecto de análisis de riesgos	SEM 7
A3. Trabajo Integrador: Realizar una auditoría e inspección de sistemas y redes de una organización	SEM 11
A4 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

La obra de referencia para el seguimiento de la asignatura es:

2.1 Riesgos y amenazas de los Sistemas de Información

- Informe INCIBE de tendencias del mercado 2016. <https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf> (consultado en Junio de 2017).
- Informe GARTNER. Predicts 2016: Security Solutions. <https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf> (consultado en Junio de 2017).

- MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WUuzufkuzT8> (consultado en Junio de 2017).
- INCIBE, Bitácora de Ciberseguridad.

  <http://www.certsi.es> (consultado en junio de 2017).
- Informe de Cibercriminalidad del Ministerio del Interior

  <http://www.interior.gob.es/documents/10180/3066430/Informe+Cibercriminalidad+2015.pdf/c10f398a-8552-430c-9b7f-81d9cc8e751b > (consultado en Junio de 2017).
- Informe de la Fiscalía de Cibercriminalidad.

  <https://www.fiscal.es/memorias/memoria2016/FISCALIA_SITE/recursos/pdf/MEMFIS16.pdf > (consultado en junio de 2017).

2.2 Análisis de riesgos

- MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WUuzufkuzT8> (consultado en Junio de 2017).
- ENISA: Inventario de modelos y herramientas de análisis y gestión de riesgos. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods> (consultado en Agosto de 2017).
- ENS, Esquema Nacional de Seguridad.

  < https://administracionelectronica.gob.es/ctt/ens> (consultado en Agosto de 2017).
- ISO 22301.

2.3 Práctica de inspección de seguridad de los sistemas

- ISO 19011.
- ISO 27000.
- COBIT versión 4 y COBIT versión 5.

10. UNIDAD DE ATENCIÓN A LA 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

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.

REGLAMENTO PLAGIO

Atendiendo al Reglamento disciplinario de los estudiantes de la Universidad Europea:

- El plagio, en todo o en parte, de obras intelectuales de cualquier tipo se considera falta muy grave.
- Las faltas muy graves relativas a plagios y al uso de medios fraudulentos para superar las pruebas de evaluación, tendrán como consecuencia la pérdida de la convocatoria correspondiente, así como el reflejo de la falta y su motivo, en el expediente académico.

REGLAMENTO DE LA IA

El estudiante debe ser el autor o autora de sus trabajos/actividades.

El uso de herramientas de Inteligencia Artificial (IA) debe ser autorizado por el docente en cada trabajo/actividad, indicando de qué manera está permitido su uso. El docente informará previamente en qué situaciones se podrá usar herramientas de IA para mejorar la ortografía, gramática y edición en general. El estudiante es responsable de precisar la información dada por la herramienta y declarar debidamente el uso de cualquier herramienta de IA, en función de las directrices que marque el docente. La decisión final sobre la autoría del trabajo y la idoneidad del uso reportado de una herramienta de IA recae en el docente y en los responsables de la titulación.