1. Datos básicos de la asignatura/módulo

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 – P630001102 Online - 0DCS001102
Semestre	Primer semestre
Curso académico	2019/2020
Docente coordinador	Presencial: Dr. José Antonio Rubio Online: Prof. Marcos Gómez Hidalgo

2. Presentación del módulo

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 generales:

- 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.

El estudiante demostrará su capacidad para trabajar en equipo, comunicarse de forma oral y escrita y aplicar los contenidos de las asignaturas para realizar juicios críticos 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

1.1 RIESGOS Y AMENAZAS DE LOS SISTEMAS DE INFORMACIÓN

Unidad 1. Riesgos y amenazas en los sistemas de información I

- 1.1. Fundamentos de análisis de riesgos.
- 1.2. Conceptos de análisis de riesgos.
- 1.3. Principios generales del análisis de riesgos.

Unidad 2. Riesgos y amenazas en los sistemas de información II

- 2.1. Evolución de las ciberamenazas.
- 2.2. Análisis del ciberdelito.
- 2.3. La respuesta institucional a las ciberamenazas.
- 2.4. Casos de estudio: amenazas y ciberdelitos

1.2 ANÁLISIS DE RIESGOS

Unidad 3. Metodología para el análisis y evaluación de riesgos I

- 3.1. Modelos de análisis de riesgos.
- 3.2. Análisis de activos, amenazas e impacto.
- 3.3. Análisis de salvaguardas y cálculo de riesgo.
- 3.4. Análisis de riesgos y continuidad de negocio

Unidad 4. Metodología para el análisis y evaluación de riesgos II

- 4.1. El alcance del análisis de riesgos.
- 4.2. El proyecto de análisis de riesgos.

- 4.3. El informe de análisis de riesgos.

1.3 PRÁCTICA PROFESIONAL DE INSPECCIÓN DE SISTEMAS
Unidad 5. Práctica profesional de inspección y auditoría de sistemas y redes I
- 5.1. Introducción y conceptos de auditorías e inspecciones.
- 5.2. Controles de auditoría e inspección y tipos de auditorías.

Unidad 6. Práctica profesional de inspección y auditoría de sistemas y redes I
- 6.1. Fases de auditoría e inspección.
- 6.2. Proyecto de inspección de auditoría.

5. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE

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

- Clases magistrales
- 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

Tipo de 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 h**

MODALIDAD ONLINE

Tipo de 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	**150 h**

7. EVALUACIÓN

Para desarrollar las competencias y alcanzar los resultados de aprendizaje indicados, deberás realizar las actividades que se indican en la tabla inferior:

MODALIDAD PRESENCIAL

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Elaboración y presentación de trabajos 1	15%
Actividad 2	Elaboración y presentación de trabajos 2	15%
Actividad 3	Resolución de un caso práctico aplicando la metodología de análisis de riesgos	20%
Actividad 4	Práctica individual del análisis de un área de seguridad de una organización basándose en la metodología EDR	15%
Actividad 5	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%
Actividad 6	Análisis de riesgos en entorno financiero	15%

MODALIDAD ONLINE

Actividad evaluable	Actividad de aprendizaje	Peso (%)
A1	Análisis de la amenaza cibernética conocidas como botnet	15%
A2	Trabajo Integrador: Realizar un proyecto de análisis de riesgos	25%

A3	Debate Foro: Conferencia SGSI/Análisis de Riesgos	10%
A4	Trabajo Integrador: Realizar una auditoría e inspección de sistemas y redes de una organización	25%
A5	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.

MODALIDAD PRESENCIAL

7.1. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota mínima de 4 en todas las actividades.
- Obtener una media ponderada de todas las actividades igual o superior a 5.

7.2. Convocatoria extraordinaria

Obtener una nota media ponderada de todas las actividades que figuran en la tabla igual o superior a 5, y obtener en la prueba de conocimiento una calificación igual o superior a 5.

MODALIDAD ONLINE

7.3. Convocatoria ordinaria

Para superar la asignatura en convocatoria ordinaria deberás:

- Obtener una nota media ponderada de todas las actividades que figuran en la tabla igual o superior a 5, y obtener en la prueba de conocimiento una calificación igual o superior a 5.

7.4. Convocatoria extraordinaria

- Para superar la asignatura convocatoria extraordinaria deberás entregar las actividades que indique el profesor, cuya nota media ponderada debe ser igual o superior a 5, y obtener en las pruebas de conocimiento una calificación igual o superior a 5.

8. CRONOGRAMA

MODALIDAD PRESENCIAL

NOVIEMBRE 2020

L	M	X	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

DICIEMBRE 2020

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

ENERO 2021

L	M	X	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

FEBRERO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

MARZO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

ABRIL 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

MAYO 2021

L	M	X	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JUNIO 2021

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULIO 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTIEMBRE 2021

L	M	X	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26

Periodo no lectivo
Entrega TFM
Defensa TFM
Festivos

Calendario sujeto a cambios en relación con las festividades: los días festivos serán fijados por el Estado y la Comunidad Autónoma correspondiente

MES	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
Noviembre										
Diciembre										
Enero										
Febrero										
Marzo										
Abril										
Mayo										
Junio										
Julio										

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

MODALIDAD ONLINE

NOVIEMBRE 2020

L	M	X	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

DICIEMBRE 2020

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

ENERO 2021

L	M	X	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

FEBRERO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

MARZO 2021

L	M	X	J	V	S	D
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

ABRIL 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

MAYO 2021

L	M	X	J	V	S	D
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JUNIO 2021

L	M	X	J	V	S	D
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

JULIO 2021

L	M	X	J	V	S	D
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SEPTIEMBRE 2021

L	M	X	J	V	S	D
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

OCTUBRE 2021

L	M	X	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Periodo no lectivo
Entrega TFM
Defensa TFM
Festivos
Examen

SEMESTRE	MES	M1	M2	M3	M4	M5	M6	M7	M8	M9.B	M10
1	Octubre										
	Noviembre										
	Diciembre										
	Enero										
	Febrero										
	Marzo										
2	Abril										
	Mayo										
	Junio										
	Julio										
	Agosto										
	Septiembre										

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

9. BIBLIOGRAFIA

A continuación, se indica la bibliografía recomendada.

Unidad de aprendizaje 1: Riesgos y Amenazas de los Sistemas de Información I

- 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).

Unidad de aprendizaje 2: Riesgos y Amenazas de los Sistemas de Información II

- 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).

Unidad de aprendizaje 3: Metodología para el Análisis y Evaluación de Riesgos I

- 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.

Unidad de aprendizaje 4: Metodología para el Análisis y Evaluación de Riesgos II

- 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).

Unidad de aprendizaje 5: Práctica Profesional de Inspección y Auditoría de Sistemas y Redes I

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

Unidad de aprendizaje 6: Práctica Profesional de Inspección y Auditoría de Sistemas y Redes II

- ISO 19011.
- ISO 27000.

COBIT versión 4 y COBIT versión 5.

10. UNIDAD DE ATENCIÓN A LA DIVERSIDAD

Estudiantes con necesidades específicas de apoyo educativo:

Las adaptaciones o ajustes curriculares para estudiantes con necesidades específicas de apoyo educativo, a fin de garantizar la equidad de oportunidades, serán pautadas por la Unidad de Atención a la Diversidad (UAD).

Será requisito imprescindible la emisión de un informe de adaptaciones/ajustes curriculares por parte de dicha Unidad, por lo que los estudiantes con necesidades específicas de apoyo educativo deberán contactar a través de: unidad.diversidad@universidadeuropea.es al comienzo de cada semestre.