1. DATOS BÁSICOS

Asignatura	Sistemas de Gestión de la Seguridad
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 – 0DCS001101 Online – P630001101
Semestre	Primer semestre
Curso académico	2019/2020
Docente coordinador	Presencial: Dr. Abel Lozoya de Diego Online: Dr. Carlos Bachmaier

2. PRESENTACIÓN

En este módulo se expondrán los principios por los que se rige el gobierno y la gestión de la Seguridad de las Tecnologías de la Información y las Comunicaciones, haciendo hincapié en los métodos de gestión de la Seguridad de la Información y en las Políticas de la Seguridad de la Información, más concretamente en lo concerniente a la seguridad de la información de las personas, seguridad de la información en las instalaciones, seguridad de la Información en la externalización de servicios y seguridad en la información en los sistemas TIC.

El alumno se familiarizará con las normas y estándares más relevantes en la actualidad, y con los criterios y mecanismos de evaluación y certificación de la gestión de la seguridad vigentes en la actualidad. Por último, los estudiantes conocerán la gestión integrada de la seguridad, métricas y comparativas (benchmarks) que permitan su evaluación y organización del mando y la respuesta rápida.

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.

- CG4: Emitir juicios en función de criterios, de normas externas o de reflexiones personales.
- CG5: Presentar públicamente ideas, procedimientos o informes de investigación, de transmitir emociones o de asesorar a personas y a organizaciones

Competencias específicas:

- CE1: Conocer los conceptos de gestión integrada de la seguridad que permitan su evaluación, así como, la organización del mando y respuesta rápida.
- CE2: Comprender los principios por los que se rige el gobierno de la Tecnología de la Información y las Comunicaciones, y ser capaces de analizar las Políticas de la Seguridad de una organización.
- CE3: Conocer las normas y estándares más relevantes, y los criterios y mecanismos de evaluación y certificación de la seguridad vigentes en la actualidad

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.

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
CE1, CE3	RA1
CG1, CG4, CG5, CE1, CE2, CE3	RA2

4. CONTENIDOS

1.1 FUNDAMENTOS DE SEGURIDAD
Unidad 1. Fundamentos de seguridad

- 1.1. Riesgo de negocio.
- 1.2. Riesgo tecnológico.
- 1.3. Amenazas por sectores. Adversarios.
- 1.4. Usuarios. Cumplimiento. Proceso SGSI

1.2 SISTEMAS DE GESTIÓN DE LA SEGURIDAD
Unidad 2. Sistemas de Gestión de Seguridad de la Información I (SGSI I)

- 2.1. Cuestiones internas que afectan al SGSI.
- 2.2. Cuestiones externas que afectan al SGSI. Objetivos y alcance.

Unidad 3. Sistemas de Gestión de Seguridad de la Información II (SGSI II)

- 3.1. Planificación: Análisis de riesgos.
- 3.2. Planificación: Gestión de riesgos.
- 3.3. Soporte.

Unidad 4. Sistemas de Gestión de Seguridad de la Información III (SGSI III)

- 4.1. Operación.
- 4.2. Evaluación del desempeño y mejora continua.

1.3 POLITICAS DE SEGURIDAD
Unidad 5. Políticas de Seguridad I

- 5.1. Políticas de seguridad de la información.
- 5.2. Reglamento de uso de recursos TIC.
- 5.3. Políticas de seguridad en entornos concretos I.
- 5.4. Políticas de seguridad en entornos concretos II.

Unidad 6. Políticas de Seguridad II

- 6.1. Plan director de seguridad.
- 6.2. Certificaciones I.
- 6.3. Certificaciones II.

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	50 h
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	37,5 h
A3. Tutorías y evaluación	31,25 h
A4. Estudio independiente del alumno	31,25 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	Test de conocimientos básicos	10%

Actividad 2	Servicios de Seguridad	10%
Actividad 3	Trabajo de exposición sobre el análisis de un caso por grupos y puesta en común de políticas de seguridad para departamentos concretos	25%
Actividad 4	Informe certificaciones	5%
Actividad 5	Elaboración de políticas de seguridad para un entorno determinado	10%
Actividad 6	Realizar un SGSI según la normativa 27001	40%

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. Una vez superada esta fecha, 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 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

Para superar la asignatura convocatoria extraordinaria deberás entregar las actividades que indique el profesor (correspondientes a las partes no entregadas o suspensas ya sean las mismas actividades u otras equivalentes a éstas). La nota de cada actividad deberá ser igual o mayor que 4. La media ponderada de todas las actividades de evaluación deberá ser igual o mayor a 5.

MODALIDAD ONLINE

Actividad evaluable	Actividad de aprendizaje	Peso (%)
A1	Identificar ataques potenciales y controles a implantar en una organización objetivo	5%
A2	Empleo de COBIT	5%
	Empleo de técnicas de gestión empresarial y ciberseguridad	8%
A4	Análisis GAP	5%
A5	Gestión de Riesgos	7%
A6	Auditoría de la ISO 27001 y 27002	10%

A7	Captación de evidencias	10%
A8	Política de seguridad, reglamento de uso de recursos TIC y certificaciones	15%
A9	Diseñar un plan director de seguridad para una organización objetivo	15%
A10	Prueba de conocimientos	20%

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 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.

7.3. 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

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

MODALIDAD ONLINE

CALENDARIO ACADÉMICO 2019-2020

Universidad Europea
LAUREATE INTERNATIONAL UNIVERSITIES

NOVIEMBRE 2019

L	M	M	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 2019

L	M	M	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 2020

L	M	M	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 2020

L	M	M	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	

MARZO 2020

L	M	M	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 2020

L	M	M	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 2020

L	M	M	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 2020

L	M	M	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 2020

L	M	M	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		

AGOSTO 2020

L	M	M	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 2020

L	M	M	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				

Periodo no lectivo
Entrega TFM
Defensa TFM
Inicio Curso
Festivos

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

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: Fundamentos de seguridad

- ISO 27001:2013. Sistemas de Gestión de Seguridad de la Información (AENOR).

Unidad de aprendizaje 2: Sistemas de Gestión de la Seguridad de la Información I

- ISACA (2009). COBIT 4.1. ISACA.
- ISACA (2012). COBIT 5. ISACA.
- Wiersema, F; Treacy, M (1997). The Discipline of Market Leaders. Basic Books.

Unidad de aprendizaje 3: Sistemas de Gestión de la Seguridad de la Información II

- AENOR (2013). UNE 71505 – Sistemas de Gestión de Evidencias Electrónicas. AENOR.
- AENOR (2013). UNE 71506 – Metodología de Análisis forense de Evidencias Electrónicas. AENOR.
- ISO (2013). ISO 27001 – Sistemas de Gestión de Seguridad de la Información. ISO.
- ISO (2015). ISO 27002 – Código de prácticas para los controles de seguridad de la información. ISO.
- ISO (2012). ISO 27037 – Directrices de Gestión de Evidencias Electrónicas. ISO.
- ISO (2015). ISO 27042 – Guía de análisis e interpretación de Evidencias Electrónicas. ISO.

Unidad de aprendizaje 4: Sistemas de Gestión de la Seguridad de la Información III

- AENOR (2013). UNE 71505 – Sistemas de Gestión de Evidencias Electrónicas. AENOR.

- ISO (2013). ISO 27001 – Sistemas de Gestión de Seguridad de la Información. ISO.
- ISO (2015). ISO 27002 – Código de prácticas para los controles de seguridad de la información. ISO.
- ISO (2012). ISO 27037 – Directrices de Gestión de Evidencias Electrónicas. ISO.

Unidad de aprendizaje 5: Políticas de Seguridad I

- ISO (2013). ISO 27001 – Sistemas de Gestión de Seguridad de la Información. ISO.

Unidad de aprendizaje 6: Políticas de Seguridad II

- ISO (2013). ISO 27001 – Sistemas de Gestión de Seguridad de la Información. ISO.

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.