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	2024/2025
Docente coordinador	
Docente	Presencial: Zulayka Vera Urueña/Jose Manuel Sacristán Online: Dr. Jordi Serra Ruiz y Dr. José Antonio Rubio

2. PRESENTACIÓN

En este módulo se expondrán los principios por los que se rige el gobierno de la Tecnología de la Información y las Comunicaciones, haciendo hincapié 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 seguridad vigente en la actualidad. Por último, los estudiantes conocerán la gestión integrada de la seguridad, métricas y 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, CE2, CE1, CE3	RA2

4. CONTENIDOS

La materia está organizada en los siguientes contenidos:

1.1 Fundamentos de seguridad

1.2 Políticas de Seguridad

1.3 Sistema de Gestión de la 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	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:

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

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
Actividad 1 Revisa tu Conocimiento	20%
Actividad 2 Política de Seguridad: Comunicación y contenido mínimo	5%
Actividad 3 Norma y procedimientos	10%
Actividad 4. Procedimiento completo nuevo	15%
Actividad 5. Aprobación del procedimiento nuevo ante el Comité de Seguridad	10%
Actividad 6. Realizar un SGSI según la normativa 27001 Memoria	25%
Actividad 7. Exposición Oral SGSI según la normativa 27001	15%

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.

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. Identificar ataques potenciales y controles a implantar en una organización objetivo	15%
A2. Gestión empresarial y alineamiento de la ciberseguridad. La auditoría de la ISO 27001	20%
A3. Política de seguridad, reglamento de uso de recursos TIC y certificaciones	20%
A4. Diseñar un plan director de seguridad para una organización objetivo	25%
A5. Prueba de conocimiento	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 las actividades que figuran en la tabla (A1 hasta A4), 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 hasta A4), 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
Actividad 1 Revisa tu Conocimiento	SEM 1
Actividad 2 Política de Seguridad:	SEM 3
Actividad 3 Norma y procedimientos	SEM 6
Actividad 4 Procedimiento completo nuevo	SEM 6
Actividad 5. Aprobación del procedimiento nuevo ante el Comité de Seguridad	SEM 7
Actividad 5 Exposición oral en clase de los resultados de las actividades 3 y 4, y presentación final ante Comité de Seguridad	SEM 8
Actividad 6. Realizar un SGSI según la normativa 27001 Memoria	SEM 10
Actividad 7. Exposición Oral SGSI según la normativa 27001	SEM 12

Modalidad online:

Actividades evaluables	Fecha
A1. Identificar ataques potenciales y controles a implantar en una organización objetivo	SEM 3
A2. Gestión empresarial y alineamiento de la ciberseguridad. La auditoría de la ISO 27001	SEM 7
A3. Política de seguridad, reglamento de uso de recursos TIC y certificaciones	SEM 9
A4. Diseñar un plan director de seguridad para una organización objetivo	SEM 10
A5. Prueba de conocimiento	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 la bibliografía recomendada.

M1.1. Fundamentos de Seguridad

- Computer Security: Art and Science, Matt Bishop. ISBN-13: 978-0134289519
- ISO (2017). ISO 27001 – Sistemas de Gestión de Seguridad de la Información. ISO.

M1.2. Políticas de Seguridad

- ISO (2017). ISO 27001 – Sistemas de Gestión de Seguridad de la Información. ISO.
- Symantec Threat Report, disponible: https://www.symantec.com/security-center/threat-report.
- Incident Response Insights Report 2018, disponible: https://www.secureworks.com/resources/rp-incident-response-insights-report-2018
- EMC's total revenue from RSA information security products and services from 2009 to 2016, by quarter (in million U.S. dollars), disponible: https://www.statista.com/statistics/208611/total-security-revenue-of-emc-since-2009/

M1.3. Sistemas de Gestión de la Seguridad

- ISO JTC 1/SC 27: Página del subcomité ISO/IEC a cargo de normas de seguridad informática.
- Definiciones y términos según la ISO27000, disponible: http://www.iso27000.es/glosario.html
- Amenazas y ataques del Instituto Nacional de Ciberseguriad, disponible: https://incibe.es/
- ISO 27001.es: Portal en español con información sobre la serie ISO 27000.

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.