1. DATOS BÁSICOS

Asignatura	La seguridad en las operaciones
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 - 0DCS001107 Online - P630001107
Semestre	Segundo semestre
Curso académico	2024/2025
Docente coordinador	Presencial:Juan Luis Grau/Javier González González Online: Prof. D. Marcos Gómez Hidalgo

2. PRESENTACIÓN

En este módulo el estudiante aprenderá cómo se planifica, organiza, gestiona e implantan las medidas de seguridad en la operación y gestión de los sistemas. Además, el estudiante aprenderá algunos conceptos básicos y obtendrá nociones relativas a los principales procesos y respuesta ante incidentes. Por último, el estudiante pondrá en práctica la seguridad en las operaciones a través de la configuración segura de uno de los servicios más utilizados en la empresa: el correo electrónico, y aprenderá la configuración segura de redes y servicios en entornos empresariales.

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:

• CE15: Ser capaces de planificar, organizar, gestionar e implantar las medidas de seguridad en la operación y gestión de los sistemas.

• CE16: Conocer los conceptos básicos de los principales procesos y respuesta ante incidentes y su aplicación a casos reales.

• 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.

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
CG4, CG5, CE16, CE20	RA1
CG1, CG4, CG5, CE15, CE16, CE20	RA2

4. CONTENIDOS

La materia está organizada en los siguientes contenidos:

- 7.1 Controles de seguridad
- 7.2 Configuración segura de servidores de correo
- 7.3 Gestión de continuidad del negocio
- 7.4 Práctica de monitorización y verificación

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	37,5 h

A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	62,5 h
A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	25 h
TOTAL	**150h**

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
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
Comparación con los controles de SANS Institute	10%
Trabajo grupal en el que los estudiantes deberán resolver un caso práctico real planteando los controles necesarios para mitigar un ataque conocido y presentarlo públicamente	15%
Actividades individuales de aplicación de los materiales explicados en clase	15%
Informe escrito individual sobre el análisis de un caso práctico real y conclusiones	10%
Ejercicios prácticos de configuración segura de servidores de correo	10%
Práctica final de configuración segura de correos	10%
Práctica de monitorización de servidores	10%
Práctica de monitorización de equipos Microsoft Windows	10%

Monitorización SIEM	10%

Modalidad online:

Sistema de evaluación	Peso
A1.Identificar los controles de seguridad a implantar en una organización objetivo	10%
A2. Analizar cómo implantar los Controles Críticos de Seguridad en una organización objetivo protegiéndose frente a posibles APTs	15%
A3. Análisis y aplicación de normativas, estándares, estrategias y planes de continuidad	30%
A4. Empleo y comparativa de herramientas antispam.	10%
A5. Monitorización y Correlación	15%
A6. Prueba de conocimientos	20%

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 ncesario 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 ncesario 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:

Actividades evaluables	Fecha
Comparación con los controles de SANS Institute	Sem 2
Trabajo grupal en el que los estudiantes deberán resolver un caso práctico real planteando los controles necesarios para mitigar un ataque conocido y presentarlo públicamente	Sem 4
Actividades individuales de aplicación de los materiales explicados en clase	Sem 6
Informe escrito individual sobre el análisis de un caso práctico real y conclusiones	Sem 7
Ejercicios prácticos de configuración segura de servidores de correo	Sem 8
Práctica final de configuración segura de correos	Sem 9
Práctica de monitorización de servidores	Sem 10
Práctica de monitorización de equipos Microsoft Windows	Sem 11
Monitorización SIEM	Sem 12

Modalidad online:

Actividades evaluables	Fecha
A1.Identificar los controles de seguridad a implantar en una organización objetivo	Sem 2
A2. Analizar cómo implantar los Controles Críticos de Seguridad en una organización objetivo protegiéndose frente a posibles APTs	Sem 4
A3. Análisis y aplicación de normativas, estándares, estrategias y planes de continuidad	Sem 7
A4. Empleo y comparativa de herramientas antispam.	Sem 9
A5. Monitorización y Correlación	Sem 11
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:

M7.1. Controles de seguridad en las operaciones

• ISO (2013). ISO 27001 - Sistemas de Gestión de Seguridad de la Información (AENOR). • Definiciones y términos según la ISO27000, disponible: http://www.iso27000.es/glosario.html

• Critical Security Controls del Instituto SANS (SANS Institute), disponible: https://www.sans.org/

• Amenazas y ataques del Instituto Nacional de Ciberseguriad, disponible: https://incibe.es/

M7.2. Gestión de la Continuidad de Negocio

• ISO (2015). ISO 22301, Sistema de Gestión de Continuidad de Negocio

• ISO (2011). ISO 27031 – Guía para la Gestión de la Tecnología de la Información y Comunicación y obtención de Continuidad de Negocio. ISO.

• ISO (2015). ISO 22317 – Análisis de Impacto en Negocio. ISO.

• BCI (2018). Good Practice Guidelines. Business Continuity Institute.

• Guías de DRJ - https://www.drj.com/resources/white-papers.html

• Recursos Profesionales del Disaster Recovery Institute - https://drii.org/resources/professionalpractices/EN

M7.3. Práctica de Configuración segura de servidores de correo

• Mastering Microsoft Exchange Server 2016 (ISBN 978-1119232056)

• Microsoft Exchange Server: Quick Reference (ISBN 978-1983802430)

• E-mail Security (ISBN 978-1849280969)

• Enhancement of Email Security Services (ISBN 978-3330073456)

M7.4. Práctica de verificación de sistemas

• Zabbix Guide. https://www.zabbix.com/documentation/1.8/manual/quickstart

• Herramientas verificación, disponible: https://github.com/obscuresec/PowerShell/blob/master/Find-MsfPSExec

• MBSA Guide Microsoft: https://technet.microsoft.com/en-us/library/cc179871.aspx

- 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.

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

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.