

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 – P630001107 Online - ODCS001107
Semestre	Segundo semestre
Curso académico	2019/2020
Docente coordinador	Presencial: Dr. Abel Lozoya de Diego Online: Prof. 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 Gestión de continuidad del negocio

7.3 Configuración segura de servidores de correo

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:

Tipo de 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

Tipo de actividad formativa	Número de horas
A3. Tutorías y evaluación	25 h
A4. Estudio independiente del alumno	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	32,5h
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	150 h

7. EVALUACIÓN

En la tabla inferior se indican las actividades evaluables y los pesos de cada una de ella.

MODALIDAD PRESENCIAL:

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Comparación con los controles de SANS Institute	10%
Actividad 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	10%
Actividad 3	Actividades individuales de aplicación de los materiales explicados en clase	15%
Actividad 4	Informe escrito individual sobre el análisis de un caso práctico real y conclusiones	10%

Actividad 5	Informe individual sobre el proceso y programa de gestión de continuidad desde su puesta en marcha hasta la mejora continua	5%
Actividad 6	Ejercicios prácticos de configuración segura de servidores de correo	10%
Actividad 7	Práctica final de configuración segura de correos	10%
Actividad 8	Práctica de monitorización de servidores	10%
Actividad 9	Práctica de monitorización de equipos Microsoft Windows	10%
Actividad 10	Práctica QRadar	10%

MODALIDAD ONLINE:

Actividad evaluable	Actividad de aprendizaje	Peso (%)
Actividad 1	Identificar los controles de seguridad a implantar en una organización objetivo.	5%
Actividad 2	Analizar como implantar el marco del NIST en una organización objetivo	5%
Actividad 3	Analizar como implantar los Controles Críticos de Seguridad en una organización objetivo	5%
Actividad 4	Analizar cómo proteger a una organización frente a posibles APT	10%
Actividad 5	Análisis de estrategias de continuidad e incidentes	15%
Actividad 6	Elaboración de un Plan Continuidad de Negocio	15%
Actividad 7	Empleo y comparativa de herramientas antispam.	10%
Actividad 8	Monitorización y Correlación	15%
Actividad 9	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 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 la prueba objetiva de M5.1 (actividad 2).
- Obtener al menos un 4 en los trabajos y resoluciones de casos prácticos (actividades 1, 4, 5)
- 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 3 y la de las pruebas objetivas igual o mayor que 4. La media ponderada de todas las actividades de evaluación deberá ser igual o mayor 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



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



NOVIEMBRE 2019							DICIEMBRE 2019							ENERO 2020						
L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D
				1	2	3					6	7	8	6	7	8	9	10	11	12
4	5	6	7	8	9	10	9	10	11	12	13	14	15	13	14	15	16	17	18	19
11	12	13	14	15	16	17	16	17	18	19	20	21	22	20	21	22	23	24	25	26
18	19	20	21	22	23	24	23	24	25	26	27	28	29	27	28	29	30	31		
25	26	27	28	29	30		30	31												

FEBRERO 2020							MARZO 2020							ABRIL 2020						
L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D
					1	2						1				1	2	3	4	5
3	4	5	6	7	8	9	2	3	4	5	6	7	8	6	7	8	9	10	11	12
10	11	12	13	14	15	16	9	10	11	12	13	14	15	13	14	15	16	17	18	19
17	18	19	20	21	22	23	16	17	18	19	20	21	22	20	21	22	23	24	25	26
24	25	26	27	28	29		23	24	25	26	27	28	29	27	28	29	30			
							30	31												

MAYO 2020							JUNIO 2020							JULIO 2020							
L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	
				1	2	3	1	2	3	4	5	6	7				1	2	3	4	5
4	5	6	7	8	9	10	8	9	10	11	12	13	14	6	7	8	9	10	11	12	
11	12	13	14	15	16	17	15	16	17	18	19	20	21	13	14	15	16	17	18	19	
18	19	20	21	22	23	24	22	23	24	25	26	27	28	20	21	22	23	24	25	26	
25	26	27	28	29	30	31	29	30						27	28	29	30	31			

AGOSTO 2020							SEPTIEMBRE 2020						
L	M	M	J	V	S	D	L	M	M	J	V	S	D
					1	2					11	12	13
3	4	5	6	7	8	9	7	8	9	10	11	12	13
10	11	12	13	14	15	16	14	15	16	17	18	19	20
17	18	19	20	21	22	23	21	22	23	24	25	26	27
24	25	26	27	28	29	30	28	29	30				
31													

Período 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										
2	Marzo										
	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. BIBLIOGRAFÍA

A continuación, se indica la 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 Ciberseguridad, 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 monitorización y verificación

- 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>
- QRadar Manual:
https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

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.

ANEXO – FICHAS COVID-19

Debido a las adaptaciones necesarias para la formación en online de la modalidad presencial se producen los cambios siguientes:

Actividad formativa descrita en la Guía de aprendizaje	Actividad formativa adaptada a formato a distancia
A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición	A1. Presentación en el aula de conocimientos por parte del profesor utilizando el método de exposición de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual
A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos	A2. Actividades de carácter grupal relativas a la aplicación de casos prácticos de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual
A3. Tutorías y evaluación	A3. Tutorías y evaluación de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual
A4. Estudio independiente del alumno	A4. Estudio independiente del alumno de forma online con las herramientas proporcionadas por la Universidad en su Campus Virtual