CEDEU CENTRO DE ESTUDIOS UNIVERSITARIOS

CIBERSEGURIDAD

GUÍA DOCENTE MODALIDAD ONLINE

MÁSTER UNIVERSITARIO EN NEGOCIOS DIGITALES

2025/2026

I. IDENTIFICACIÓN DE LA ASIGNATURA

ASIGNATURA: Ciberseguridad
TIPO: Obligatoria
PERIODO DE IMPARTICIÓN: Primer semestre
NÚMERO DE CRÉDITOS: 3,0 ECTS
IDIOMA EN EL QUE SE IMPARTE: Castellano
CALENDARIOS Y HORARIOS: Ver en la web

II. PROFESORADO

PERSONAL DOCENTE: Álvaro Gárriz Oyarzun
CORREO ELECTRÓNICO: academicoonline@cedeu.es
TUTORÍAS: Para consultar las tutorías póngase en contacto con el/la profesor/a
TIEMPO ESTIMADO DE RESPUESTA AL ALUMO: 48 h (días lectivos) desde la recepción del correo electrónico

III. PRESENTACIÓN

Dentro de esta asignatura, buscamos capacitar a los estudiantes en la creación y gestión de estrategias de ciberseguridad, esenciales para la integridad de cualquier negocio en el entorno digital actual.

La transformación digital ha impulsado la economía, pero con ella han surgido amenazas y puntos vulnerables que deben ser abordados para garantizar un negocio seguro en el espacio virtual. Por lo tanto, introduciremos a los alumnos en el ámbito de la seguridad tecnológica, resaltando la situación actual y desglosando conceptos clave y vulnerabilidades comunes, como malware, ransomware, ataques DoS, phishing, entre otros.

Estudiaremos en detalle las conexiones y aplicaciones seguras, centrándonos en la estructura OSI y los posibles riesgos asociados con la protección de redes. Además, profundizaremos en los sistemas modernos de identidad digital, explorando técnicas de autenticación, gestión de usuarios, firma digital y biometría, además de abordar temas críticos de privacidad. Realizaremos un análisis profundo de los riesgos tecnológicos, la protección de la información y cómo evaluar y formalizar políticas y estrategias de seguridad. Además, abordaremos cómo se llevan a cabo auditorías informáticas y forenses, con el objetivo de detectar ciberdelitos y otros tipos de amenazas digitales.

Al concluir la asignatura, los alumnos podrán:

1. Tener una comprensión amplia del panorama de la ciberseguridad.
2. Comprender y categorizar las diferentes vulnerabilidades.
3. Familiarizarse con los riesgos presentes en la estructura OSI.
4. Evaluar y gestionar potenciales amenazas y sus impactos en las empresas, así como manejar incidentes de seguridad adecuadamente.
5. Detectar y responder a delitos y amenazas digitales, asegurando la defensa y protección adecuada.

IV. COMPETENCIAS

COMPETENCIAS BÁSICAS

CB6. Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
CB7. Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
CB8. Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
CB9. Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
CB10. Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

COMPETENCIAS GENERALES

CG1. Desarrollar las habilidades necesarias para la correcta gestión de las relaciones interpersonales en un entorno multidisciplinar especializado en el mundo digital.
CG2. Resolver problemas en entornos empresariales digitales que favorezca tomar decisiones y/o emitir juicios en situaciones complejas.
CG3. Comprender y evaluar las tendencias en el mercado de la Economía Digital, así como estimar su impacto en el desarrollo social, económico y cultural, e incorporarlo en la orientación estratégica de los proyectos de su organización.
CG4. Analizar, de forma critica, las tecnologías digitales aplicadas al mundo empresarial.
CG5. Resolver, mediante la aplicación de la innovación y la creatividad, qué diseño o solución tecnología es adecuada para la implementación de mejoras en la empresa, dentro del ámbito digital.

COMPETENCIAS ESPECÍFICAS

CE04. Identificar y analizar las principales amenazas y riesgos tecnológicos inherentes a la tecnología digital, su impacto en las empresas, y las principales contramedidas existentes, siendo capaz de establecer y formalizar un Plan de Seguridad al efecto.

V. ACTIVIDADES FORMATIVAS

TIPO	CONTENIDO	HORAS	PRESENCIALIDAD OBLIGATORIA
AD1. Clase magistral	Actividad formativa para la explicación de conceptos y teorías. Metodología expositiva donde se prioriza la acción del profesor y que se realiza por videoconferencia de manera síncrona o asíncrona.	18	0%
AD2. Actividades de aprendiza sobre casos prácticos	Actividad formativa que se orienta a la realización de informes, memorias, etc. y/o resolución de problemas bajo la supervisión y asesoramiento del profesor o tutor	6	0%
AD4. Tutorías	Resolución de dudas y orientación sobre actividades formativas o de evaluación por teléfono, por email o por videoconferencia.	6	0%
AD5. Trabajo autónomo	Actividades formativas fuera del aula en la que el estudiante desarrolla su capacidad de aprendizaje autónomo a través de la realización de trabajos, búsquedas de recursos e información, estudio, etc.	43	0%
AD6. Prueba de evaluación	Actividad destinada a la realización de pruebas de evaluación para valorar la adquisición de las competencias en la materia por parte de los estudiantes	2	100%
		75	

VI. METODOLOGÍAS DOCENTES

MD1. CLASE MAGISTRAL: Exposición por parte del profesor de los contenidos de cada unidad didáctica por medio de explicaciones y presentaciones, junto con indicaciones sobre fuentes de información y bibliografía. Serán sesiones por videoconferencia o video-streaming de forma síncrona o asíncrona.

MD2. ACTIVIDADES DE APRRENDIZAJE SOBRE CASOS PRÁCTICOS: Selección y presentación de actividades o situaciones con las que el alumno puede encontrarse en su práctica para analizar diferentes aspectos a partir de la consulta de bibliografía especializada. Se llevará a cabo por videoconferencia o video-streaming de forma síncrona o asíncrona.

MD3. APRENDIZAJE ON-LINE: Metodología donde el estudiante puede organizarse para repasar contenidos teóricos o realizar actividades prácticas según sus necesidades o su tiempo disponible, así como consultar dudas o intercambiar información con los profesores o compañeros.

En cada asignatura se establecerán los horarios de tutorías, tanto individuales como grupales, para la mejor atención de los estudiantes, en las horas previstas para la docencia de cada asignatura.

VII. SISTEMA DE EVALUACIÓN

NOTA IMPORTANTE:

No se podrá superar la asignatura en el caso de que la parte correspondiente a las actividades de evaluación (Prueba 1) o la parte correspondiente a la realización de la prueba escrita (Prueba 2) no estén aprobadas con una calificación final igual o superior a 5 puntos en una escala de 0 a 10.

El alumno que no supere la Prueba 1 y/o 2 no podrá superar la asignatura en la evaluación ordinaria, obteniendo una calificación máxima de 4,0, independientemente de la nota obtenida en la prueba teórico-práctica.

Para poder aprobar la asignatura el alumno debe superar obligatoriamente, con una calificación superior a 5,0, las pruebas 1 y 2 por separado, siempre y cuando la media de la asignatura sea superior a 5,0.

En el caso de que el alumno no supere la asignatura, la calificación obtenida en las pruebas 1 y 2 de la asignatura durante el curso en cualquier evaluación no se reservará para el curso siguiente.

CRITERIOS APLICABLES A LA EVALUACIÓN ORDINARIA				
SISTEMA DE EVALUACIÓN	**CRITERIOS APLICABLES A LA EVALUACIÓN CONTINUA**		**PON.**	**PERIODO**
PRUEBA 1:		**ACUMULATIVA**		
Resolución de actividades prácticas	Liberatoria: puntuación mínima 5.0 (de 1 a 10).	Reevaluable (podrá evaluarse en la convocatoria extraordinaria).	40%	Durante el curso o semestre
PRUEBA 2:		**ACUMULATIVA**		
Prueba teórico-práctica presencial con preguntas que podrán ser cortas y/o tipo test, y/o a desarrollar, etc.	Liberatoria: puntuación mínima 5.0 (de 1 a 10).	Reevaluable (podrá evaluarse en la convocatoria extraordinaria).	60%	Durante el curso o semestre

CRITERIOS APLICABLES A LA EVALUACIÓN EXTRAORDINARIA				
SISTEMA DE EVALUACIÓN	CRITERIOS APLICABLES A LA EVALUACIÓN CONTINUA		PON.	PERIODO
PRUEBA 1:		**ACUMULATIVA**		
Presentación de trabajos académicos	Liberatoria: puntuación mínima 5.0 (de 1 a 10).	No Reevaluable	40%	En la convocatoria extraordinaria
PRUEBA 2:		**ACUMULATIVA**		
Prueba teórico-práctica presencial con preguntas que podrán ser cortas y/o tipo test, y/o a desarrollar, etc.	Liberatoria: puntuación mínima 5.0 (de 1 a 10)	No Reevaluable	60%	En la convocatoria extraordinaria

y/o a desarrollar, etc.				

i tras la realización de la evaluación extraordinaria, el alumno no supera la media de 5,0 en todas las pruebas acumulativas liberatorias 1 y 2, la asignatura quedará finalmente como suspensa, calificada con el menor valor obtenido en las pruebas realizadas en las dos convocatorias

VIII. TEMARIO

1. Introducción a la seguridad de la tecnología digital. Situación Actual, conceptos y principales vulnerabilidades (malware, virus, randsomeware, bootnets, DoS, phissing, etc.)
2. Conexiones y aplicaciones seguras: Los niveles OSI y riesgos/vulnerabilidades asociadas a la protección de redes.
3. Identidad Digital: Técnicas de autenticación, autorización y gestión de usuarios, firma digital, bimetría. Privacidad y anonimato.
4. Análisis evolución y gestión de riesgos tecnológicos. Seguridad de la información (integridad, confiabilidad y disponibilidad). Evaluación del impacto y formalización de políticas y Planes de Seguridad.
5. La auditoría informática y la auditoría forense.
6. Ciberdelitos, ciberterrorismo, ciberguerra.

IX. BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA

Fundación Telefónica (2018). *Ciberseguridad, la protección de la información en el mundo digital*. Ed. Ariel

BIBLIOGRAFÍA RECOMENDADA

BEJTLICH, R. *The Practice of network security monitoring: Understanding incident detection and response*

SALLIS, E., CARACCIOLO, C. y RODRÍGUEZ, M. *Ethical Hacking. Un enfoque metodológico para profesionales.*

SALAS, A. Los hombres que susurraban a las máquinas

VALLE, M. *Ciberseguridad: consejos para tener vidas digitales más seguras.*