CEDEU CENTRO DE ESTUDIOS UNIVERSITARIOS

CIBERSEGURIDAD

GUÍA DOCENTE

MÁSTER UNIVERSITARIO EN NEGOCIOS DIGITALES

2024/2025

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: Ángel Camaño
CORREO ELECTRÓNICO: a.camano@cedeu.es
CATEGORÍA: Máster
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
AF1. Clase magistral	Actividad formativa para la explicación de conceptos y teorías. Metodología expositiva donde se prioriza la acción del profesor	18	85%
AF2. 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	85%
AF3. Tutorías	Resolución de dudas y orientación sobre actividades formativas	6	25%
AF4. 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%
AF5. 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.
MD2. ACTIVIDADES DE APRRENDIZAJE SOBRE CASOS PRÁCTICOS: Selección y presentación de casos prácticos, problemas o situaciones con las que el alumno puede encontrarse en su práctica para analizar diferentes aspectos a partir de la consulta de bibliografía especializada.

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 los trabajos 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.

Para poder acogerse a las condiciones de la evaluación ordinaria que figuran al final del apartado el alumno debe haber superado la asistencia en la materia, igual o superior a 85%.

En el caso de que la asistencia sea inferior al 85%, la calificación final ordinaria de la asignatura se calculará solo teniendo en cuenta el porcentaje del examen (Prueba 2). No obstante, para poder aprobar, debe cumplirse obligatoriamente la condición de tener los trabajos de la asignatura (Prueba 1) aprobados con una calificación igual o superior a 5 puntos.

En la convocatoria extraordinaria no se tendrá en cuenta la asistencia, por lo que, en caso de tener las pruebas reevaluables aprobadas y que la calificación final ponderada, en función a los porcentajes de la Tabla VI. B, sea superior a 5 puntos, la asignatura estará aprobada en convocatoria extraordinaria.

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.

EVALUACIÓN ORDINARIA

La distribución y características de las pruebas de evaluación son las que se describen en el apartado V. Los criterios aplicables a la evaluación ordinaria que se encuentra a continuación.

Para poder superar la evaluación ordinaria, los alumnos con una asistencia igual o superior al 85%, deben haber presentado y superado obligatoriamente la prueba 1 acumulativa liberatoria (presentación de trabajos) y superado la prueba 2 (prueba teórico-práctica presencial). 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.

Todos los alumnos que no superen la evaluación ordinaria deberán realizar y superar las pruebas correspondientes a la evaluación extraordinaria para verificar la adquisición de las competencias establecidas en esta guía en el caso de: A) no superar la prueba escrita final correspondiente a la Evaluación Ordinaria; B) no haberse presentado a la evaluación de la convocatoria reseñada; o C) no haber entregado y superado o igualado la calificación media de 5.0 puntos, en una escala de 0.0 a 10.0 puntos, en la entrega de la prueba 1 acumulativa liberatoria (presentación de trabajos).

Para poder acogerse a las condiciones de la evaluación ordinaria que figuran en el apartado V el alumno debe haber superado la asistencia en la materia, igual o superior a 85%.

Todas las Pruebas 1 en evaluación ordinaria que se entreguen fuera del plazo señalado en el campus virtual, o indicado por el docente en la clase, no serán tenidas en cuenta.

EVALUACIÓN EXTRAORDINARIA

Los alumnos que no consigan superar la evaluación ordinaria o no se hayan presentado serán objeto de la realización de una evaluación extraordinaria (reevaluación) para verificar la adquisición de las competencias establecidas en esta guía docente. Los criterios aplicables se encuentran al final de este apartado.

El alumno que no supere la prueba 1 de la evaluación ordinaria deberá realizar una nueva en la evaluación extraordinaria. No será necesario realizar de nuevo la prueba 2, el examen final, si ya lo ha superado en la evaluación ordinaria con una calificación superior a 5,0. En cualquier caso, para poder obtener una media igual o superior a 5,0 será necesario, en las pruebas 1 y 2 por separado, tener una calificación superior a 5,0.

El alumno que no supere la prueba 2 en la evaluación ordinaria deberá realizar una nueva en la evaluación extraordinaria. No será necesario realizar de nuevo la prueba 1 si ya la ha superado en la evaluación ordinaria con una calificación superior a 5,0. En cualquier caso, para poder obtener una media igual o superior a 5,0 será necesario, en las pruebas 1 y 2 por separado, tener una calificación superior a 5,0.

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.

Todas las Pruebas 1 en evaluación extraordinaria que se entreguen fuera del plazo señalado en el campus virtual, o indicado en la clase por el docente, no serán tenidas en cuenta.

EJEMPLO DE POSIBLES CASOS

1. **CASO 1**: En el caso de haber entregado la prueba 1 acumulativa liberatoria (presentación de trabajos) requerida en la evaluación ordinaria y que la calificación de ella sea superior a 5,0 puntos, en una escala de 0,0 a 10,0 puntos, pero no haber superado o no haberse presentado a la prueba 2 final liberatoria (prueba teórico-práctica presencial) en evaluación ordinaria, los alumnos deberán realizar prueba 2 final liberatoria de la evaluación extraordinaria, en la que tendrán que obtener una calificación igual o superior a 5,0 puntos, en una escala de 0,0 a 10,0 puntos, para que ponderen con la calificación de las pruebas acumulativas ya realizadas. En cualquier caso, para poder obtener una media igual o superior a 5,0 será necesario, en las pruebas 1 y 2 por separado, tener una calificación superior a 5,0.
2. **CASO 2**: En el caso de haber superado la prueba 2 liberatoria final (prueba teórico-práctica presencial) en la evaluación ordinaria con una calificación final mayor de 5,0 en una escala de 0,0 a 10,0 puntos, pero no haber superado la prueba 1 acumulativa liberatoria (presentación de trabajos) en la evaluación ordinaria, se planteará una nueva prueba 1, tras la evaluación ordinaria, que el alumno deberá entregar, como fecha límite, el día antes del comienzo del periodo de exámenes de evaluación extraordinaria. Todas las pruebas 1 en evaluación extraordinaria que se entreguen fuera del plazo señalado no serán

tenidas en cuenta. En cualquier caso, para poder obtener una media igual o superior a 5,0 será necesario, en las pruebas 1 y 2 por separado, tener una calificación superior a 5,0.

3. **CASO 3:** En el caso de que el alumno no haya entregado o no haya superado las pruebas 1 y 2 acumulativas en la evaluación ordinaria, deberá presentar y superar la prueba 1 acumulativa (presentación de trabajos) con una calificación superior a 5,0 puntos, en una escala de 0,0 a 10,0 puntos y superar la prueba 2 final liberatoria (prueba teórico-práctica presencial) con una calificación superior a 5,0 puntos en una escala de 0,0 a 10,0 puntos. Esta prueba 1 acumulativa estará disponible en el campus virtual tras el periodo de evaluación ordinaria. Tendrá que ser entregada, como fecha límite, el día antes del comienzo del periodo de exámenes de evaluación extraordinaria. Todas las pruebas 1 en evaluación extraordinaria que se entreguen fuera del plazo señalado no serán tenidas en cuenta. En cualquier caso, para poder obtener una media igual o superior a 5,0 será necesario, en las pruebas 1 y 2 por separado, tener una calificación superior a 5,0.

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).	50%	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).	50%	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	50%	Durante el curso o semestre
PRUEBA 2:		**ACUMULATIVA**		
Prueba teórico-práctica presencial con preguntas que podrán ser cortas y/o tipo test,	Liberatoria: puntuación mínima 5.0 (de 1 a 10)	No Reevaluable	50%	Durante el curso o semestre

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.*