Ciberseguridad

Código: 105779
Créditos ECTS: 6

2024/2025

Titulación	Tipo	Curso
2502501 Prevención y Seguridad Integral	FB	2

Contacto

Nombre: Jose Cañabate Perez

Correo electrónico: josep.canabate@uab.cat

Equipo docente

Laura Casas Diaz

Idiomas de los grupos

Puede consultar esta información al final del documento.

Prerrequisitos

No hay prerequisitos.

La docencia de la asignatura se impartirá teniendo en cuenta la perspectiva de los Objetivos de Desarrollo Sostenible.

Objetivos y contextualización

- Conocer los conceptos básicos informáticos y el funcionamiento de un sistema de información que pueden afectar la seguridad de las organizaciones o las personas.

- Conocer los componentes físicos de un sistema informático u ordenador y redes.

- Conocer el proceso de auditoría de sistemas de información.

- Analizar el Gobierno y la Gestión de las Tecnologías de la Información.

- Estudiar los aspectos fundamentales de la Gestión de la Seguridad de la Información.

- Analizar los principales estándares de Seguridad de la información.

- Conocer los conceptos fundamentales de la Ciberseguridad.

- Analizar las tipologías de la delincuencia tecnológica, prueba electrónica y *Forensic Readiness*.

Competencias

- Actuar con responsabilidad ética y con respeto por los derechos y deberes fundamentales, la diversidad y los valores democráticos.
- Aplicar herramientas de software específicas para la resolución de problemas propios de la seguridad.
- Comunicarse de forma eficaz en inglés, tanto de forma oral como escrita.
- Comunicarse y transmitir ideas y resultados de forma eficiente en el entorno profesional y no experto, tanto de forma oral como escrita.
- Contribuir a la toma de decisiones de inversión en prevención y seguridad.
- Desarrollar el pensamiento científico y el razonamiento crítico en temas de prevención y seguridad.
- Generar propuestas innovadoras y competitivas en la investigación y en la actividad profesional desarrollando la curiosidad y la creatividad.
- Gestionar de modo eficiente la tecnología en las operaciones de seguridad.
- Hacer un uso eficiente de las TIC en la comunicación y transmisión de ideas y resultados.
- Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
- Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
- Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- Respetar la diversidad y la pluralidad de ideas, personas y situaciones.
- Valorar el impacto técnico, social y legal de los nuevos descubrimientos científicos y de los nuevos desarrollos tecnológicos.

Resultados de aprendizaje

1. Analizar críticamente los principios, valores y procedimientos que rigen el ejercicio de la profesión.
2. Aplicar herramientas y realizar desarrollos de software específicos para la resolución de problemas propios de la seguridad, medio ambiente, calidad o responsabilidad social corporativa.
3. Aplicar los fundamentos de estadística, economía y finanzas, marco legal aplicable, e informática necesarios para aplicar la prevención y la seguridad integral.
4. Comunicarse de forma eficaz en inglés, tanto de forma oral como escrita.
5. Comunicarse y transmitir ideas y resultados de forma eficiente en el entorno profesional y no experto, tanto de forma oral como escrita.
6. Desarrollar el pensamiento científico y el razonamiento crítico en temas de prevención y seguridad.
7. Explicar el código deontológico, explícito o implícito, del ámbito de conocimiento propio.
8. Formular estrategias de gestión en la empresa.
9. Generar propuestas innovadoras y competitivas en la investigación y en la actividad profesional desarrollando la curiosidad y la creatividad.
10. Hacer un uso eficiente de las TIC en la comunicación y transmisión de ideas y resultados.
11. Proponer proyectos y acciones que estén de acuerdo con los principios de responsabilidad ética y de respeto por los derechos y deberes fundamentales, la diversidad y los valores democráticos.
12. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

13. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
14. Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
15. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
16. Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
17. Respetar la diversidad y la pluralidad de ideas, personas y situaciones.
18. Valorar el impacto técnico, social y legal de los nuevos descubrimientos científicos y de los nuevos desarrollos tecnológicos.

Contenido

El programa de la asignatura abarca un amplio espectro de conceptos y prácticas esenciales en el campo de la ciberseguridad y las tecnologías de la información. Comienza con una introducción a la metodología del curso, proporcionando a los estudiantes una base sólida en los conceptos fundamentales de TI y seguridad de la información. A medida que avanza el curso, se exploran incidentes de ciberseguridad conocidos, diversos tipos de ciberamenazas y el papel de la inteligencia artificial en la detección y respuesta a estos incidentes. También se discuten las estrategias de ciberdefensa y los planes nacionales diseñados para proteger infraestructuras críticas.

El curso también cubre la normativa estatal y europea relacionada con la ciberseguridad, así como la delincuencia tecnológica y la importancia de la prueba electrónica en la investigación de delitos informáticos. Además, se enseña cómo preparar una organización para investigaciones forenses digitales, incluyendo la protección de los activos de información y la aplicación de estándares de ciberseguridad reconocidos a nivel internacional. Por último, se aborda la protección de infraestructuras críticas y el desarrollo de planes de continuidad de negocio para garantizar que una organización pueda seguir operando durante y después de incidentes disruptivos. Este enfoque integral prepara a los estudiantes para enfrentar los desafíos en ciberseguridad de manera efectiva y competente.

BLOQUE 1

Tema 1. Introducción y metodología de la asignatura.
Tema 2. Conceptos básicos de tecnologías de la información.
Tema 3. Conceptos básicos de seguridad de la información y de ciberseguridad.

BLOQUE 2

Tema 4. Eventos de ciberseguridad conocidos
Tema 5. Ciberamenazas: definición y tipos
Tema 6. Inteligencia Artificial y ciberseguridad.
Tema 7. Ciberdefensa y planes nacionales de ciberseguridad.

BLOQUE 3

Tema 8. Normativa estatal y europea en materia de ciberseguridad.
Tema 9. Delincuencia tecnológica.
Tema 10. Prueba electrónica.
Tema 11. Forensic Readiness e Investigación digital forense.

BLOQUE 4

Tema 12. Protección de los activos de sistemas de información.
Tema 13. Análisis de los principales estándares de ciberseguridad.
Tema 14. Infraestructuras críticas y Plan de Continuidad de Negocio.

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Videoconferencias con la participación activa del alumnado	12	0,48	
Tipo: Supervisadas			
RESOLUCIÓN DE DUDAS SOBRE TEMARIO y PRÁCTICAS	6	0,24	
Tipo: Autónomas			
ESTUDIO Y RESOLUCIÓN DE LOS ESCENARIOS DE RIESGO	60	2,4	
PREPARACIÓN DE LAS PRÁCTICAS	60	2,4	

Lengua de docencia: castellano.

Teniendo en cuenta que la modalidad de la clase es Online, con el objetivo de alcanzar los objetivos de aprendizaje descritos en la presente Guía desarrollaremos una metodología que combine el estudio individual a partir del Manual, y las lecturas que se plantearán en cada tema, además de algunos documentales.Cada tema tendrá un foro de dudas, y se establecerá un Foro de "Aportaciones" donde los alumnos pueden introducir lecturas, artículos, webs, documentales, y todo tipo de materiales y recursos relacionados con la asignatura. Por otra parte, se deberán realizar la resolución de dos casos prácticos relacionados con los temas estudiados en la asignatura.Cabe destacar que debido al modelo Online los estudiantes tendrán que preparar los materiales de forma autónoma (documentos, lecturas, vídeos etc..) y los foros y sesiones Online se dedicaran a profundizar sobre los temas tratados así como a resolver posibles duda.

Por otra parte, la asignatura utilizará el Aprendizaje Basado en Problemas para el desarrollo de parte de sus actividades de evaluación. El aprendizaje basado en problemas (ABP) es una metodología educativa que utiliza problemas reales como punto de partida para la adquisición e integración de nuevos conocimientos. En el contexto de ciberseguridad, este enfoque se adapta particularmente bien debido a la naturaleza dinámica y multifacética de los riesgos cibernéticos. Aquí se describe cómo se puede aplicar esta metodología a escenarios de riesgo en ciberseguridad. En un entorno de ABP, se presenta a los estudiantes un escenario de riesgo en ciberseguridad. Este podría ser un ataque de ransomware en una empresa, una brecha de datos en una organización financiera, o una campaña de phishing dirigida. El problema debe ser complejo y abierto, permitiendo múltiples enfoques y soluciones.Los estudiantes se organizan en pequeños grupos colaborativos. Cada grupo trabaja de manera autónoma para analizar y entender el problema presentado. La colaboración fomenta el intercambio de ideas, la discusión y la confrontación de diferentes puntos de vista, lo que enriquece el proceso de aprendizaje. Los estudiantes identifican lo que saben y lo que necesitan aprender para abordar el problema. Esto implica una investigación activa, donde los estudiantes buscan información relevante sobre ciberseguridad, incluyendo técnicas de ataque y defensa, normativas aplicables, y mejores prácticas. La investigación puede incluir la revisión de literatura académica, análisis de casos de estudio previos, y consulta con expertos en la materia.Con la información recopilada, los estudiantes analizan el problema en profundidad, identificando las vulnerabilidades explotadas y las posibles consecuencias. A partir de este

análisis, desarrollan estrategias y planes de acción para mitigar el riesgo y prevenir futuros incidentes. Finalmente, se debe indicar que este proceso requiere pensamiento crítico y la aplicación de conocimientos técnicos y teóricos adquiridos durante el curso.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Evaluación

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
EXAMEN FINAL	50%	2	0,08	3, 2, 6, 1, 18, 7, 8, 9, 5, 10, 11, 17, 15, 16, 14, 13, 12
PARTICIPACIÓN EN FOROS Y CLASSE	10%	5	0,2	2, 15, 16, 14, 13, 12
TRABAJOS PRÁCTICOS	40%	5	0,2	3, 2, 4, 6, 1, 18, 7, 8, 9, 5, 10, 11, 17, 15, 16, 14, 13, 12

La evaluación de la asignación se realizará mediante:

1. EVALUACIÓN CONTINUADA

- Realización de cuatro Prácticas de Evaluación Continuada (40%)

  - Trabajos Individuales:

Consisten en dos PAC.

PEC 1: Sobre los conceptos básicos de ciberseguridad.

PEC 2. Sobre conceptos básicos de criptología.

  - Trabajo en grupo:

Consta de dos PEC grupales:

PEC 3: Definiciones y características principales de una amenaza avanzada y persistente (APT).

PEC 4: Escenarios de riesgo relacionados con una amenaza avanzada y persistente (APT).

- Participación en foros de debate y una clase (10%)

Para superar esta parte, cada alumno deberá realizar una participación de calidad en cada foro de debate (habrá 4 foros, divididos por tres temas) Por tanto, cada alumno deberá esperar un mínimo de 4 intervenciones de calidad (es decir, aportando nociones y comentarios que van más allá de lo que se recoge en los manuales incluyendo bibliografía y referencias) Al inicio, cada alumno deberá introducir un mínimo de 4 aportaciones en el apartado destinado a estos efectos de la asignación. Cada intervención en el foro y cada aportación suponen un 10% de la valoración de este apartado, la calificación se establecerá en base a

criterios de calidad, originalidad, coherencia e interacción, si se cumple. Las intervenciones o aportaciones extra se valorarán positivamente, pero recordemos que más bien podría superar el 1 punto que tenía este apartado en relación a la nota global.

-Examen tipo test de todo el temario (50%)

Asistirás a un examen tipo test de 30 preguntas sobre el temario con cuatro opciones posibles. La pregunta correcta suma 1 sobre 30, la pregunta incorrecta resta 0'25 sobre 30, la no contestadas ni suman ni restan.

REVISIÓN DE LA CALIFICACIÓN FINAL: Se concertará día y hora de revisión con los profesores en un plazo máximo de 48 hs. después de la publicación de las clasificaciones finales.

RECUPERACIÓN

En caso de no superar la asignación de acuerdo con los criterios anteriormente mencionados (evaluación continua), se podrá realizar una prueba de recuperación en los datos programados en el horario, lo que se traducirá en la totalidad de los contenidos del programa.

Para participar en la recuperación el alumnado deberá haber sido previamente evaluado en un conjunto de actividades, el peso de las cuales equivaldría a un mínimo de dos terceras partes de la cualificación total de la asignatura. No obstante, la calificación que constará en el expediente del exalumno es de un máximo de 5 aprobados.

El exalumno que necesite presentar un dato de evaluación deberá presentar la solicitud justificada de empleo, documento que se encontrará en el Espacio Moodle de Tutoría EPSI.

PLAGIO

Sin perjuicio de otras medidas disciplinarias que se estiman oportunas, y de acuerdo con la normativa académica vigente, "en caso de que el estudiante realice alguna irregularidad que pueda conducir a una variación significativa de la calificación de un acto La evaluación se calificará con un 0 en este acto de evaluación, con independencia del proceso disciplinario que se pueda instruir. En caso de que se produzcan diversas irregularidades en los actos de evaluación de una asignatura, la calificación final de esta asignatura será 0. .

Las pruebas/exámenes podrán ser escritos y/o orales a criterio del profesorado.

Si durante la corrección se tienen indicios de que se ha realizado una actividad o trabajo con respuestas asistidas por inteligencia artificial, el/la docente podrá complementar la actividad con una entrevista personal para corroborar la autoría del texto.

NO EVALUABLE

Se evaluará siempre que haya realizado un conjunto de actividades el peso de las cuales equivalga a un mínimo de 2/3 partes de la calificación total de la asignatura. Si el valor de las actividades realizadas no llega a este límite, el profesor/a de la asignatura podrá considerar al alumno como no valorable.

2. EVALUACIÓN ÚNICA

Los/las estudiantes que opten por la evaluación única harán las siguientes pruebas.

- Realización de cuatro prácticas (40%)

PEC 1: Sobre los conceptos básicos de ciberseguridad.

PEC 2. Sobre conceptos básicos de criptología.

PEC 3: Definiciones y características principales de una amenaza avanzada y persistente (APT).

PEC 4: Escenarios de riesgo relacionados con una amenaza avanzada y persistente (APT).

- Realización de comentarios de texto sobre un tema de ciberseguridad relacionado con el programa (10%)

- Examen tipo test de todo el tema (50%)

Examen tipo test de 30 preguntas sobre el tema con cuatro opciones posibles. La pregunta correcta suma 1 sobre 30, la pregunta incorrecta resta 0'25 sobre30, la no contestadas ni suma ni resta.

Recuperación: Se aplicará el mismo sistema de recuperación que para la evaluación continua.

No evaluable: Se aplicarán los criterios básicos de no evaluable que per la evaluación continua.

Revisión de la calificación final: La revisión de la calificación final sigue el mismo procedimiento que para la evaluación continua.

Bibliografía

Alonso Lecuit, Javier (2021). "Directiva NIS2: valoraciones y posiciones desde el sector privado", CIBER elcano No. 65 - abril de 2021: Entidades críticas y resileiencia en la UE | Directiva NIS2 (disponible en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_

Communications-Electronics Security Group (2011). *Digital Continuity to Support Forensic Readiness.* London: The National Archives.

Doménech Pascual, G. (2006) *Derechos fundamentales y riesgos tecnológicos: el derecho del ciudadano a ser protegido por los poderes públicos*. Madrid: Centro de Estudios Constitucionales.

Fojon, E., Coz J. R., Linares, S., Miralles, R. (sin fechar) *La Ciberseguridad Nacional, un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia.* ISMS FORUM: Madrid.

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática*. Madrid: Ra-Ma Editorial.

ISACA (2012). *COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.* ISACA: Rolling Meadows.

ISACA (2014). *Manual de preparación para el examen de* CISM*.* ISACA: Rolling Meadows.

ISACA (2014).*CSX Cybersecurity Fundamentals Study Guide*. ISACA: Rolling Meadows.

ISACA (2014). *Transforming Cybersecurity*. ISACA: Rolling Meadows.

ISACA (2014). *Responding to Targeted Cyberattacks*. ISACA: Rolling Meadows.

ISACA (2016). *Manual de preparación para el examen de* CISA*.* ISACA: Rolling Meadows.

Martín Ávila, A.; Quinto Zumarraga, F. de. (2003). *Manual de seguridad en Internet: soluciones técnicas y jurídicas*. A Coruña: Netbiblo.

Ortiz Plaza, Roberto; Nuñez Baroja, Andrés (2021). "De la concienciación al riesgo humano en la ciberseguridad", Revista SIC: ciberseguridad, seguridad de la información y privacidad, ISSN 1136-0623, Vol. 30, Nº. 143 (Febrero 2021), 2021 (Ejemplar dedicado a: Ciberataques en 2021. Tiempos modernos), págs. 72-73

Piattini Velthuis, M., Peso Navarro, E. del, Peso M. del (2011). *Auditoría de tecnologías y sistemas de información.* Madrid: Ra-Ma Editorial.

Rowlingson R. (2004). "A Ten Step Process for Forensic Readiness". *International Journal of Digital Evidence* (Volume 2, Issue 3)

Velasco Núñez, E. (2013). "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley (*Nº 8183)

Velasco Núñez, E. (2015). "Los delitos informáticos", *Práctica Penal: cuaderno jurídico* (núm.81) pp. 14 a 28.

Recursos on-line:

ENISA (Agencia Europea para la ciberseguridad) - https://www.enisa.europa.eu/

Instituto Nacional de Ciberseguridad - www.incibe.es

Agencia Española de Protección de Datos www.agpd.es

SIC - Revista de Ciberseguridad, Seguridad de la Información y Privacidad - www.revistasic.es

Wired - www.wired.com

CIBER Elcano http://www.realinstitutoelcano.org/wps/portal/rielcano_es/publicaciones/ciber-elcano/

Software

La asignatura no requiere programario.

Lista de idiomas

Nombre	Grupo	Idioma	Semestre	Turno
(TE) Teoría	1	Español	segundo cuatrimestre	tarde