Ciberseguridad

Código: 105746
Créditos ECTS: 6

2024/2025

Titulación	Tipo	Curso
2502501 Prevención y Seguridad Integral	FB	2

Contacto

Nombre: Laura Casas Diaz

Correo electrónico: laura.casas@uab.cat

Equipo docente

Laura Casas Diaz

Idiomas de los grupos

Puede consultar esta información al final del documento.

Prerrequisitos

No hay prerequisitos.

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

La informática y por extensión las tecnologías de la información y comunicación (TIC o TI en adelante) han transformado no sólo nuestra sociedad, sino también las formas de organización de las empresas y las instituciones públicas, las maneras de hacer negocio, el ocio y el entretenimiento, y en definitiva las vidas de las personas. Por este motivo, el conocimiento de cómo funcionan los elementos básicos de la informática, así como los principales conceptos de lo que podríamos denominar como un sistema de información complejo forman parte del contenido sustancial de esta asignatura.

Por otro lado, tenemos que situar a los expertos en seguridad integral en el que se conoce como "ciclo de vida" de un sistema de información de una organización, desde su adquisición, donde no sólo se deben tomar decisiones relacionadas con la eficacia o la eficiencia, o la reducción de costes, sino también sobre su alineación con las políticas de seguridad de la empresa. Igualmente, su gestión, mantenimiento y operaciones deben estar directamente en consonancia con las directrices de seguridad de la organización.

Para conseguir estos objetivos, esta asignatura quiere ofrecer al estudiante herramientas de auditoría de sistemas de información, que le permitirán evaluar y medir si se están cumpliendo los niveles de seguridad en la organización. En otro caso, se explicarán modelos de Gobierno y gestión de las Tecnologías de Información, así como los principales estándares COBIT, ISO 27.000, NIST 800-53, Esquema Nacional de Seguridad, así como se analizará la Estrategia de Ciberseguridad Nacional.

Finalmente, desde el punto de vista jurídico se quiere analizar la delincuencia informática y la prueba electrónica ya que suponen retos para la seguridad de la información. Como medidas de prevención se verá que es un plan de preparación forense digital para el caso de sufrir un ataque informático o un evento no deseado, esto es el llamado *Forensic Readiness*.

BLOQUE 1

Tema 1. Introducción y metodología de la materia.

Tema 2. Conceptos básicos de las tecnologías de la información.

Tema 3. Conceptos básicos de seguridad de la información y ciberseguri

BLOQUE 2

Tema 4. Eventos de ciberseguridad conocidos

Tema 5. Ciberamenazas: definición y tipos

Tema 6. Inteligencia artificial y ciberseguridad.

Tema 7. Aviones de ciberdefensa y ciberseguridad nacional.

BLOQUE 3

Tema 8. Normativa estatal y europea en materia de ciberseguridad.

Tema 9. Delitos tecnológicos.

Tema 10. Prueba electrónica.

Tema 11. Preparación Forense e Investigación Forense Digital.

BLOQUE 4

Tema 12. Protección de los activos de los sistemas de información.

Tema 13. Análisis de los principales estándares de ciberseguridad.

Tema 14. Infraestructuras críticas y Plan de Continuidad del Negocio.

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
CLASE TEÓRICA	44	1,76	
Tipo: Supervisadas			
TUTORIAS DE APOYO PARA EL SEGUIMIENTO DE LAS UNIDADES DIDÁCTICAS	2	0,08	
Tipo: Autónomas			
ESTUDIO Y RESOLUCIÓN DE LOS ESCENARIOS DE RIESGO	47	1,88	
PREPARACIÓN DE LAS PRÁCTICAS	47	1,88	

Lengua de docencia: Catalán

Las clases en el aula corresponden a la metodología magistral en la que el profesor expone la materia objeto de estudio, pero también se suscita el debate y resuelven problemas y situaciones, el resto corresponde a sesiones prácticas donde los alumnos trabajarán en grupo, discutiendo sobre materiales reflexivos y resolviendo casos concretos. Los contenidos trabajados en las sesiones teóricas (además de la bibliografía básica obligatoria) serán evaluados mediante pruebas escritas. Por otro lado, los contenidos trabajados en las sesiones prácticas también serán evaluados mediante la entrega de las tareas realizadas.

Asimismo, los alumnos, fuera del aula contribuyen al aprendizaje de la materia con la búsqueda de documentación de temas relacionados con la materia objeto de estudio. Cada alumno, además de su asistencia en el aula y el estudio individual debe realizar búsqueda de documentación y trabajo personal de consolidación sobre lo expuesto en clase.

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, 7, 8, 11, 15, 16, 14, 13, 12
TABAJO EN EQUIPO	25%	4	0,16	3, 6, 1, 18, 8, 17, 15, 16, 12
TRABAJOS PRÁCTICOS	25%	4	0,16	4, 6, 1, 18, 9, 5, 10, 11, 17, 15, 16, 14, 13, 12

A) EVALUACIÓN CONTINUA

Primera y segunda prueba: trabajos prácticos (25% de la nota final)

Estos trabajos prácticos se irán pidiendo en el transcurso del semestre y se centrarán en aspectos concretos que determinará el profesorado. Cada uno de los trabajos deberá ser evaluado por encima del 5 (de un total de 10) y deberá entregarse en la fecha propuesta según el cronograma. La media de los trabajos prácticos supondrá el 25% de la nota del curso.

Ambos trabajos tendrán que tener una nota de 3 (de un total de 10) como mínimo para poder sumar a la evaluación continua.

Los trabajos serán recuperables (a la semana dedicada a tal efecto a finales del semestre). Los alumnos que no hayan presentado ninguno de los trabajos en el momento programado no serán evaluados y no podrán recuperarlos, a excepción de quienes aporten una justificación (documento escrito).

Tercera prueba: trabajo en grupo (25% de la nota final)

La práctica consistirá en la presentación de un trabajo en equipo relacionado con la temática de la asignatura, debiendo los estudiantes desarrollar un programa de prevención dirigido a colectivos vulnerables. Obtener una nota mínima de 3 (sobre un total de 10) para poder añadir la actividad a la evaluación continua.

B) EVALUACIÓN FINAL

a)2 exámenes finales (50% de la nota final)

Los alumnos, de forma individual, realizarán dos exámenes, un parcial liberador durante el transcurso de la asignatura y un examen final que se realizará en la fecha oficial del calendario establecido por la EPSI. En ambas pruebas deberá obtenerse una calificación mínima de un 5 (de un total de 10). Ambos exámenes consistirán en un test de treinta preguntas sobre el programa de la asignatura y la resolución de un caso práctico sobre las materias analizadas. Por lo que respecta a la prueba tipo test consistirá en treinta preguntas con múltiple opción (cuatro respuestas sólo una correcta), con una penalización por pregunta incorrecta de 0,25/30 (o cuatro incorrectas resta una correcta).

El alumnado que no hubiera superado la primera prueba final de acuerdo a los criterios anteriores deberá examinarse de la totalidad del temario en el examen final que se realizará en la fecha oficial del calendario establecido por la EPSI. Los alumnos No Presentados no serán evaluados, a excepción de quienes aporten una justificación (documento escrito). Los exámenes serán recuperables en la semana dedicada a tal efecto a finales del semestre.

Examen de recuperación

En caso de no superar la asignatura de acuerdo con los criterios antes mencionados y se obtenga un resultado del conjunto de las evaluaciones que no llegue a una nota de 5 (de un total de 10) podrá presentarse a un examen final siempre que el alumno se haya evaluado en un conjunto de actividades, cuyo peso equivalga a un mínimo de dos terceras partes de la calificación total de la asignatura. Si no ha sido evaluado de estas dos terceras partes por no haberse presentado en las pruebas obtendrá una calificación de No Presentado, sin que tenga laposibilidad de presentarse al examen final de recuperación.

En este examen se volverá a evaluar el conjunto de los contenidos de la asignatura que no se hayan superado en la evaluación continua.

En caso de superarse el examenfinal, la asignatura quedará aprobada con un 5 como máximo, independientemente de la nota obtenida en el examen.

Las pruebas/exámenes podrán ser escritas y/u orales a criterio del profesorado.

Cambio de fecha de una prueba o examen

El alumnado que necesite cambiar una fecha de evaluación deben presentar la petición justificada cumplimentando el documento que encontrará en el espacio moodle de Tutorización EPSI. Una vez cumplimentado el documento debe enviarse al profesorado de la asignatura y a la coordinación del Grado.

Revisión

En el momento de realizar cada actividad evaluativa, el profesorado informará al alumnado de los mecanismos de revisión de las calificaciones. Para el alumnado de evaluación única, el proceso de revisión será el mismo.

Evaluación Única

Los estudiantes que opten por la evaluación única realizarán una prueba de síntesis final de todo el contenido de la asignatura (50%) y entregarán el trabajo de la asignatura (50%)

La fecha para esta prueba y la entrega del trabajo de la asignatura será la misma programada en el horario para el último examen de evaluación continua.

Se aplica el mismo sistema de recuperación que para la evaluación continua. Las pruebas/exámenes podrán ser escritas y/u orales a criterio del profesorado.

Evaluación del alumnado en segunda o más convocatoria

El alumnado que repita la asignatura deberárealizar las pruebas y exámenes programados y entregar el trabajo de la asignatura en las fechas indicadas en el aula Moodle.

Las pruebas/exámenes podrán ser escritas y/u orales a criterio del profesorado.

Otras consideraciones

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, "en caso de que el estudiante haga cualquier irregularidad que pueda conducir a una variación significativa de la calificación de un acto de evaluación, se calificará con un 0 este acto de evaluación, con independencia del proceso disciplinario que se pueda instruir.

Si concurren circunstancias sobrevenidas que impidan el normal desarrollo de la asignatura, el profesorado podrá modificar tanto la metodología como la evaluación de la asignatura.

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

This subject doesn't use any software.

Lista de idiomas

Nombre	Grupo	Idioma	Semestre	Turno
(TE) Teoría	1	Catalán	segundo cuatrimestre	tarde
(TE) Teoría	2	Catalán	segundo cuatrimestre	tarde
(TE) Teoría	3	Catalán	segundo cuatrimestre	tarde