Universitat Autònoma de Barcelona

2019/2020

Ciberseguridad

Código: 105746
Créditos ECTS: 6

Titulación	Tipo	Curso	Semestre
2502501 Prevención y Seguridad Integral	FB	2	2

Contacto

Nombre: Josep Cañabate Pérez
Correo electrónico: Josep.Canabate@uab.cat

Uso de idiomas

Lengua vehicular mayoritaria: español (spa)
Algún grupo íntegramente en inglés: No
Algún grupo íntegramente en catalán: Sí
Algún grupo íntegramente en español: No

Equipo docente

Xavier Rubiralta Costa

Prerequisitos

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

- Aplicar herramientas de software específicas para la resolución de problemas propios de la seguridad.
- Asumir la responsabilidad social, ética y profesional que se derive de la práctica del ejercicio profesional.
- 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.
- 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. Aplicar herramientas y realizar desarrollos de software específicos para la resolución de problemas propios de la seguridad, medio ambiente, calidad o responsabilidad social corporativa.
2. Aplicar los fundamentos de estadística, economía y finanzas, marco legal aplicable, e informática necesarios para aplicar la prevención y la seguridad integral.
3. Asumir la responsabilidad social, ética y profesional que se derive de la práctica del ejercicio profesional.
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. Formular estrategias de gestión en la empresa.
8. Generar propuestas innovadoras y competitivas en la investigación y en la actividad profesional desarrollando la curiosidad y la creatividad.
9. Hacer un uso eficiente de las TIC en la comunicación y transmisión de ideas y resultados.
10. Respetar la diversidad y la pluralidad de ideas, personas y situaciones.
11. 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 a la asignatura y definición de conceptos básicos.

Tema 2. Componentes físicos de un sistema informático u ordenador y redes.

Tema 3. Programario de un sistema informático u ordenador (sistema operativo, aplicaciones, licencias).

Tema 4. Adquisición, desarrollo e implementación de sistemas de Información.

Tema 5. Gobierno y Gestión de TI / COBIT (*Control Objectives for Information and Related Technology*).

BLOQUE 2

Tema 6. Proceso de auditoría de sistemas de información.

Tema 7. Delincuencia tecnológica.

Tema 8. Prueba electrónica.

Tema 9. *Forensic Readiness* e Investigación digital forense.

BLOQUE 3

Tema 10. Protección de los activos de sistemas de información.

Tema 11. Gestión de la seguridad de la información y cumplimiento

Tema 12. Desarrollo del programa de seguridad de la información.

BLOQUE 4

Tema 13. Gestión de incidentes de seguridad de la información.

Tema 14. Análisis de la ISO 27000 (Sistema de Gestión de la Seguridad de la Información) y la NIST 800_53.

Tema 15. Infraestructuras críticas y Plan de Continuidad de Negocio.

BLOQUE 5

Tema 16. Tendencias: *Cloud Computing, BYOD, Big Data*, movilidad, redes sociales, *Internet of Things*, etc.

Tema 17. Diferencias y alcance de la ciberseguridad y la seguridad de la información. Planes Nacionales de Ciberseguridad.

Tema 18. Recomendaciones y buenas prácticas en la gestión de la seguridad en el ámbito empresarial y particular.

Metodología

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.

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
CLASE TEÓRICA	44	1,76	1, 2, 6, 7
Tipo: Supervisadas			
TUTORIAS DE APOYO PARA EL SEGUIMIENTO DE LAS UNIDADES DIDÁCTICAS	2	0,08	1, 2, 7
Tipo: Autónomas			
ESTUDIO Y RESOLUCIÓN DE LOS ESCENARIOS DE RIESGO	47	1,88	1, 2, 7
PREPARACIÓN DE LAS PRÁCTICAS	47	1,88	1, 2, 5, 6, 7

Evaluación

La evaluación de la asignatura se basa en reunir diferentes fondos de evidencias para la puntuación sobre la participación de los estudiantes que permite evaluar de forma continuada del estudiante. Planteamos, pues, una evaluación continua, medida a través de los comentarios escritos sobre los trabajos, problemas y foros dirigidos por la asignatura, la entrega del trabajo trabajada en grupo en las sesiones de prácticas y exámenes escritos.

Para obtener una evaluación positiva hay que superar, como mínimo, todos los apartados (A, B y C) por encima del 50%.

A) 2 EXAMEN FINAL (50% DE LA NOTA FINAL)

Los alumnos, de forma individual, realizarán un examen final, éste se hará en la fecha oficial del calendario establecido por la EPSI. En este examen se deberá obtener una calificación mínima de un 40%. Este examen consistirá en un test de treinta preguntas sobre el programa de la asignatura y la resolución de un caso práctico sobre las materias analizadas. En cuanto 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 incorrectos resto una correcta).

Los exámenes serán recuperables a la semana dedicada a tal efecto al final del semestre. Los alumnos No Presentados no serán evaluados, a excepción de los que aporten una justificación (documento escrito).

B) TRABAJOS PRÁCTICOS (20% 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 40% y deberá ser entregado en la fecha propuesta según el cronograma. La media de los trabajos prácticos supondrá el 20% de la nota del curso.

Los trabajos serán recuperables (en la semana dedicada a tal efecto al final 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 los que aporten una justificación (documento escrito).

C) PRESENTACIÓN DE ESCENARIOS DE RIESGO RELACIONADO CON EL SISTEMA DE INFORMACIÓN (20% DE LA NOTA FINAL)

Durante el semestre se irán proponiendo problemas en clase que se deberán resolver individualmente y presentar la solución por escrito. La entrega de los informes correspondientes supondrá su evaluación y la media de ambas supondrá el 10% de la nota final. Estas tareas pueden ser también reflexiones individuales, ejercicios, presentaciones de casos, etc. Dada su naturaleza, no son susceptibles de recuperación al final del semestre

D) PARTICIPACIÓN EN LOS FOROS Y EN CLASE (10% DE LA NOTA FINAL)

Durante el semestre se irán proponiendo temas de debate / opinión tanto en clase como en los foros previstos en la web de la asignatura (MOODLE). El objetivo es que los estudiantes debatan entre ellos de manera pública y moderada con el profesores sobre estas cuestiones. La evaluación supondrá el 10% de la nota final. Dada su naturaleza, no son susceptibles de recuperación al final del semestre.

RECUPERACIÓN

En caso de no superar la asignatura de acuerdo con los criterios antes mencionados (evaluación continuada), se podrá hacer una prueba de recuperación en la fecha programada en el horario, y que versará sobre la totalidad de los contenidos del programa.

Para participar a la recuperación el alumnado tiene que haber sido previamente evaluado en un conjunto de actividades, el peso de las cuales equivalga a un mínimo de dos terceras partes de la calificación total de la asignatura. No obstante, la calificación que constará al expediente del alumno es de un máximo de 5-Aprobado.

El alumnado que necesite cambiar una fecha de evaluación han de presentar la petición justificada rellenando el documento que encontrará en el espacio moodle de Tutorización EPSI.

PLAGIO

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, "en caso que el estudiante realice 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. En caso que se produzcan diversas irregularidades en los actos de evaluación de una misma asignatura, la calificación final de esta asignatura será 0".

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

Actividades de evaluación

Título	Peso	Horas	ECTS	Resultados de aprendizaje
EXAMEN FINAL	40%	2	0,08	1, 2, 5, 6, 9, 7, 8, 10, 11
PARTICIPACIÓN EN FOROS Y CLASSE	10%	2	0,08	1, 2, 5, 6, 9, 7, 8, 10, 11
PRESENTACIÓN DE ESCENARIOS DE RIESGO RELACIONADOS CON SISTEMAS DE INFORMACIÓN	20%	3	0,12	1, 2, 3, 5, 6, 11
TRABAJOS PRÁCTICOS	30%	3	0,12	1, 3, 4, 5, 6, 9, 8, 10, 11

Bibliografía

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.

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.