Universitat Autònoma de Barcelona

2019/2020

Ciberseguridad

Código: 105779
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: catalán (cat)
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.

Tema17. 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

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

Actividades

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Videoconferencias con la participación activa del alumnado	6	0,24	1, 2, 7
Tipo: Supervisadas			
RESOLUCIÓN DE DUDAS SOBRE TEMARIO y PRÁCTICAS	12	0,48	1, 2, 7
Tipo: Autónomas			
ESTUDIO Y RESOLUCIÓN DE LOS ESCENARIOS DE RIESGO	60	2,4	1, 2, 7
PREPARACIÓN DE LAS PRÁCTICAS	60	2,4	1, 2, 7

Evaluación

La evaluación de la asignatura se realizará mediante:

Evaluación continua (30% de la nota global): Para superar este apartado cada alumno deberá realizar una participación de calidad, en cada foro de debate (habrá 5 foros, divididos por áreas temáticas) Por lo tanto de cada alumno se esperan un mínimo de 5 intervenciones de calidad (es decir, aportando nociones y comentarios que vayan más allá de lo recogido en los manuales incluyendo bibliografía y referencias)

A su vez cada alumno deberá introducir un mínimo de 4 aportaciones en el apartado destinado a esos efectos de la asignatura.

Cada intervención en el foro y cada aportación suponen un 10% de la evaluación de este apartado, la calificación se establecerá en base a criterios de calidad, originalidad, coherencia e interacción, si cabe. Las intervenciones o aportaciones extra, se valorarán positivamente, pero recordamos que nunca se podrá exceder de los 3 puntos que tiene este apartado en relación a la nota global.

Trabajo individual consistente en el análisis de un escenario de riesgo tecnológico (15% de la nota global)

Se planteará al estudiante un escenario de riesgo para TI (Tecnologías de la información) en el cual se deberá analizar el impacto para la seguridad de la información (integridad, confidencialidad y disponibilidad)

Trabajo Individual consistente en la elaboración de unas buenas prácticas de uso de TI en una organización compleja (15% de la nota global)

El estudiante deberá realizar unas buenas prácticas sobre TI para una organización que cuenta con una estructura compleja, lo cual puede comprometer a la seguridad de la información.

Examen final de la asignatura (40% de la nota global)

El examen constará de preguntas tipo test y para desarrollar y se basará en los contenidos del temario del manual más las lecturas de carácter obligatorio.

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, 7, 8, 10, 11
PARTICIPACIÓN EN FOROS Y CLASSE	30%	5	0,2	1, 2, 7
TRABAJOS PRÁCTICOS	30%	5	0,2	1, 2, 3, 4, 5, 6, 9, 7, 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, Eloy. (2013). "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica", *Diario La Ley (*Nº 8183)

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