Guía docente de la asignatura “Informática”

1. IDENTIFICACIÓN

- ✓ **Nombre de la asignatura: Informática**
- ✓ **Código: 101853**
- ✓ **Titulación: Grado en Prevención y Seguridad Integral**
- ✓ **Curso académico: 2018/2019**
- ✓ **Tipo de asignatura: Formación básica**
- ✓ **Créditos ECTS (horas): 6**
- ✓ **Período de impartición: 2n semestre**
- ✓ **Idioma en que se imparte: Catalán/Castellano/Inglés**
- ✓ **Responsable de la asignatura y e-mail de contacto: Josep Cañabate Pérez
josep.canabate@uab.cat**
- ✓ **Otros profesores: Xavier Rubiralta Costa – xavier.rubiralta@uab.cat**

2. PRESENTACIÓN

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*.

3. OBJETIVOS FORMATIVOS

- 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*.
-

4. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias específicas

CE5Aplicar herramientas de software específicas para la resolución de problemas propios de la seguridad.

CE8Gestionar de manera eficiente la tecnología en las operaciones de seguridad.

CE10Contribuir a la toma de decisiones de inversión en prevención y seguridad.

Resultados de aprendizaje

RA 5.1 Aplicar herramientas de software específicas para la resolución de problemas propios de la seguridad, medio ambiente, calidad y responsabilidad social corporativa

RA 8.2Formular estrategias de gestión en la empresa.

RA 10.2Aplicar los fundamentos de informática necesarios para aplicar la prevención y la seguridad integral.

Competencias transversales

CT1Desarrollar el pensamiento científico y el razonamiento crítico en temas de prevención y seguridad.

CT2Valorar el impacto técnico, social y legal de los nuevos descubrimientos científicos y los nuevos desarrollos tecnológicos.

CT5Generar propuestas innovadoras y competitivas en la investigación y en la actividad profesional desarrollando la curiosidad y la creatividad.

CT11Respetar la diversidad y la pluralidad de ideas, personas y situaciones.

CT12Comunicarse y transmitir ideas y resultados de manera eficiente en el entorno profesional y no experto, tanto de forma oral como escrita

CT13Hacer un uso eficiente de las TIC en la comunicación y transmisión de ideas y resultados.

CT14Comunicarse de manera eficaz en inglés, tanto de forma oral como escrita.

CT15Asumir la responsabilidad social, ética y profesional que se derive de la práctica del ejercicio profesional.

5. TEMARIO Y CONTENIDO

BLOQUE 1

- Tema 1. Introducció a la assignatura y definició 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.

6. BIBLIOGRAFÍA RECOMENDADA

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.

7. METODOLOGÍA DOCENTE

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.

Las tutorías con el profesorado se concertarán por correo electrónico.

7.1 ACTIVIDADES DE FORMACIÓN

Título	UD	Horas	ECTS	Resultados de aprendizaje
Tipos: Dirigidas				
1.1. Clase teórica		47	1,88	RA 5.1, RA 8.2. RA 10.2
1.2.-Clase de casos prácticos		20	0,8	RA 5.1, RA 8.2. RA 10.2
Tipos: Supervisadas				
2.1. Prácticas en el aula		15	0,6	RA 5.1, RA 8.2. RA 10.2
2.2. Sesiones con grupos reducidos		5	0,2	RA 5.1, RA 8.2. RA 10.2
Tipos: Autónomas				
				RA 5.1, RA 8.2. RA 10.2
3.1. Preparación de prácticas		10	0,4	RA 5.1, RA 8.2. RA 10.2
3.2. Estudio y resolución de escenarios de riesgo		10	0,4	RA 5.1, RA 8.2. RA 10.2

8. SISTEMA DE 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.

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 rellenando el documento que encontrará en el espacio moodle de Tutorización EPSI.

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.

8.1 ACTIVIDADES DE EVALUACIÓN

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Exámen final	50 %	2	0,08	RA 5.1, RA 8.2. RA 10.2
Trabajos prácticos		3	0,12	RA 5.1

20 %

Presentación de escenarios de riesgo relacionados con sistemas de la información	20 %	3	0,12	RA 5.1, RA 8.2. RA 10.2
Participación Foros y clase	10%	2	0,08	RA 5.1, RA 8.2. RA 10.2

9. PREVENCIÓN Y SEGURIDAD INTEGRAL

La informática y las tecnologías de la información y la comunicación (TIC) han pasado a ser una parte sustancial de la estructura y del funcionamiento ordinario , tanto de las organizaciones privadas como de las administraciones, así como son una herramienta fundamental en todos los aspectos de la vida actual de las personas. Por estos motivos conocer los riesgos que conllevan, entender cómo funciona la informática y los sistemas de información, y aplicar los conceptos básicos de seguridad de la información es crítico y totalmente imprescindible en la formación de un graduado en prevención y seguridad.