

Guía docente de la asignatura “Informática”

I. IDENTIFICACIÓN

- ✓ **Nombre de la asignatura:** Informática
- ✓ **Código:** 101853
- ✓ **Titulación:** Grado en Prevención y Seguridad Integral
- ✓ **Curso académico:** 2016/2017
- ✓ **Tipo de asignatura:**
- ✓ **Créditos ECTS:** 6
- ✓ **Período de impartición:** 2n semestre
- ✓ **Idioma en que se imparte:** castellano
- ✓ **Profesor/a Responsable de la asignatura:** Josep Cañabate Pérez
- ✓ **Correo electrónico:** josep.canabate@uab.cat

Equipo docente:

- ✓ **Profesor/a :** Josep Cañabate Pérez
- ✓ **Correo electrónico:** josep.canabate@uab.cat
- ✓ **Profesor/a :** Xavier Rubiralta Costa
- ✓ **Correo electrónico:** xavier.rubiralta@uab.cat

II. PRESENTACIÓ

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*.

III. OBJETIVOS FORMATIVOS Y COMPETENCIAS ESPECÍFICAS

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*.

Competencias Específicas

CE5	Aplicar herramientas de software específicas para la resolución de problemas propios de la seguridad.
CE8	Gestionar de manera eficiente la tecnología en las operaciones de seguridad.
CE10	Contribuir 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 8.2	Formular estrategias de gestión en la empresa.
RA 10.2	Aplicar los fundamentos de informática necesarios para aplicar la prevención y la seguridad integral.

IV. COMPETENCIAS TRANSVERSALES

CT1	Desarrollar el pensamiento científico y el razonamiento crítico en temas de prevención y seguridad.
CT2	Valorar el impacto técnico, social y legal de los nuevos descubrimientos científicos y los nuevos desarrollos tecnológicos.
CT5	Generar propuestas innovadoras y competitivas en la investigación y en la actividad profesional desarrollando la curiosidad y la creatividad.
CT11	Respetar la diversidad y la pluralidad de ideas, personas y situaciones.
CT12	Comunicarse y transmitir ideas y resultados de manera eficiente en el entorno profesional y no experto, tanto de forma oral como escrita
CT13	Hacer un uso eficiente de las TIC en la comunicación y transmisión de ideas y resultados.
CT14	Comunicarse de manera eficaz en inglés, tanto de forma oral como escrita.
CT15	Asumir la responsabilidad social, ética y profesional que se derive de la práctica del ejercicio profesional.

V. TEMARIO Y CONTENIDOS

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.

VI. 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.

VII. METODOLOGÍAS DOCENTES

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 dudas

VIII. SISTEMA DE 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 una 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

Evaluación continuada	30%
Trabajo Individual (caso)	15%
Trabajos Individuales (buenas prácticas)	15%
Examen	40%

Si tres o más trabajos/ejercicios, comentarios en foros, o palabras del glosario no son realizadas, se pasaría de la evaluación continua a la evaluación final. Es decir, el 100% de la nota será la del examen final de Julio.

"Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, de acuerdo con la normativa académica vigente, las irregularidades cometidas por un estudiante que puedan conducir a una variación de la calificación se calificarán con un cero (0). Por ejemplo, plagiar, copiar, dejar copiar ..., una actividad de evaluación, implicará suspender esta actividad de evaluación con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para aprobar la asignatura, esta asignatura quedará suspendida directamente, sin oportunidad de recuperarla en el mismo curso. "

IX. ORGANIZACIÓN DEL TIEMPO DE DEDICACIÓN DEL ESTUDIANTE

Tipo	Actividades	Horas	ECTS	RESULTADOS DE APRENDIZAJE
Actividades supervisadas	Tutorías de Apoyo para el seguimiento de las Unidades Didácticas	75	3	RA 5.1, RA 8.2. RA 10.2
Actividades autónomas	Realización, exposición y debate relativo a las diferentes Unidades Didácticas	75	3	RA 5.1, RA 8.2. RA 10.2
TOTAL		150	6	RA 5.1, RA 8.2. RA 10.2

X. PREVENCIÓ I SEGURIDAD

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.