Universidad Rey Juan Carlos

GUÍA DOCENTE

INFORMATICA APLICADA A LA CRIMINOLOGIA

GRADO EN CRIMINOLOGÍA

CURSO 2026-27

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Fecha de publicación: 08-07-2026

I.-Identificación de la Asignatura	
Tipo	FORMACIÓN BÁSICA
Período de impartición	1 curso, 2Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

II.-Presentación

Dentro del **Módulo de Conocimientos Básicos Comunes**, esta asignatura **Informática aplicada a la Criminología** está enmarcada como materia obligatoria en el **primer curso del Grado en Criminología**. Organizativamente, corresponde su docencia al **Área de Informática** del **Departamento de Economía Financiera y Contabilidad,** con una dedicación de **6 ETCS**. Como objetivo general se persigue que el alumnado adquiera los conceptos fundamentales necesarios para conocer las **tecnologías de la información y las comunicaciones (TIC) en el contexto de las ciencias criminológicas**, así como su utilización en escenarios de seguridad crítica y cibercriminología. Para ello se cuenta con una serie de bloques temáticos relacionados con la **ciberseguridad, la cibercriminalidad y las disciplinas forences digitales**. Desde esta perspectiva, se desarrollarán contenidos sobre fundamentos informáticos, ciberespacio, a protección de archivos y sistemas informáticos, los códigos informáticos maliciosos y otros ataques, que suponen conductas antisociales o criminales, así como el análisis y estudio forense de las evidencias digitales, comprendiendo la necesidad de usar aplicaciones informáticas que especialicen y perfeccionen el trabajo del criminólogo en la sociedad actual. Además, se pretende que el estudiante sea capaz de identificar conceptos relacionadas con las vulnerabilidades, el análisis de riesgos informáticos, la seguridad en Internet, sistemas Windows y Unix/Linux, recolección de evidencias digitales, análisis forense de equipos informáticos y teléfonos inteligentes, el tratamiento y análisis del audio y de la imagen, con especial énfasis en ciberdelincuencia y criminalidad tecnológica, particularmente en la fenomenología criminal de los delitos en el ciberespacio, las ciberestafas y el acoso en Internet, las actividades relacionadas con el ciberterrorismo, el ciberespionaje y los aspectos técnicos en el marco de la delincuencia organizada. Finalmente, el alumnado deberá adquirir las capacidades básicas para comprender las normas jurídicas, jurisprudencia y procedimientos con contenido informático, especialmente en lo que afecta a la seguridad de la información y de las aplicaciones informáticas, redes y bases de datos.

ATENCIÓN: INDICACIONES SOBRE EL FUNCIONAMIENTO DE LA ASIGNATURA DIRIGIDAS A LOS ESTUDIANTES QUE CURSEN ESTA ASIGNATURA EN EL CAMPUS DE ARANJUEZ

- *Asignatura en modalidad de extinción:* solo tienen derecho a examen e informará el profesor sobre la modalidad exacta de dicho examen, que será el 100% de la asignatura y se realizará en la fecha oficial*. Las consideraciones necesarias se dispondrá mediante la plataforma de Aula Virtual de la URJC.*

II.B-Presentación en inglés

In the Module of Common Basic Knowledge, this subject Applied Informatics in Criminology is framed as a mandatory course in the first year of the Criminology Degree. Organizational responsibility for its teaching lies within the Informatics Area of the Department of Financial and Accounting Economics, with a workload of 6 ECTS. The overall objective is for students to acquire the fundamental concepts necessary to understand information and communication technologies (ICT) in the context of criminological sciences, as well as their application in critical security scenarios and cybercrime. To achieve this, the curriculum includes thematic blocks related to cybersecurity, cybercriminality, and digital forensic disciplines. From this perspective, content will cover computer fundamentals, cyberspace, protection of files and computer systems, malicious code, and other attacks that constitute antisocial or criminal behavior. Additionally, students will engage in the analysis and forensic study of digital evidence, recognizing the need to use specialized software applications to enhance the work of criminologists in todays society. Furthermore, students are expected to identify concepts related to vulnerabilities, risk analysis in computing, internet security, Windows and Unix/Linux systems, digital evidence collection, forensic analysis of computer equipment and smartphones, audio and image analysis, with a particular focus on cybercrime and technological criminality. This includes understanding the criminal phenomena of cyber offenses, cyber scams, internet harassment, activities related to cyberterrorism, cyber espionage, and technical aspects within the framework of organized crime. Finally, students should acquire basic skills to comprehend legal norms, jurisprudence, and procedures related to computer content, especially concerning information security and applications, networks, and databases.

III.-Resultados de Aprendizaje

CG01. Capacidad de analizar, reunir, compilar y sintetizar información y datos.
CG02. Capacidad de organización y planificación
CG04. Capacidad de gestión de la información y uso de las TIC
CG09. Capacidad para aplicar los conocimientos adquiridos en entornos nuevos o poco conocidos dentro de contextos más amplios o multidisciplinares
CE09. Manejo y aplicación de las fuentes jurídicas de la criminología.
CE22. Empleo de las diferentes metodologías de investigación en criminología
CE25. Análisis y manejo de las diferentes fuentes de información asociando los datos obtenidos para explicar y sostener hipótesis y conclusiones
CE29. Que los estudiantes sean capaces de aplicar los conocimientos teóricos y competencias adquiridas en las distintas asignaturas que componen el itinerario del grado a la práctica profesional en los distintos ámbitos de la Criminología

- Leyenda para las titulaciones no adaptadas al RD 822/21: **CB** - competencias básicas, **CG** - competencias generales, **CE** - competencias específicas, **CT** - competencias transversales.
- Leyenda para las titulaciones adaptadas al RD 822/21: **CON** - conocimientos, **COM** - competencias, **HAB** - habilidades.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

IV.-Contenido

IV.A.-Temario de la asignatura

I. Fundamentos tecnológicos	I.1. Conceptos generales sobre hardware, software y sistemas Windows/Unix/Linux
	I.2. Redes LAN y WAN
	I.3. Redes Sociales e Internet
II - Organización de la Seguridad de la Información.	II.1. Principios de la ciberseguridad
	II.2. Normas, Políticas y Gestión de la Seguridad de la Información
	II.3. Salvaguardas y medidas de Seguridad
III - Análisis de riesgos	III.1. Definiciones y metodologías de riesgos
	III.2. Vulnerabilidades y amenazas
IV - Códigos maliciosos	IV.1. Conceptos sobre código malicioso
	IV.2. Redes Botnet y equipos Zombies
V - Delincuencia informática	V.1. Introducción a los delitos informáticos
	V.2. Fenomenología criminal en el ciberespacio y delincuencia organizada
	V.3. Tipos delictuales: daños, estafas, acosos, ciberterrorismo y ciberespionaje
VI - Informática forense	VI.1. Introducción análisis forense
	VI.2. Recolección de evidencias
	VI.3. Pericia informática
	VI.4. Telefonía forense
	VI.5. Acústica forense
	VI.6. Imagen forense
VII - Protección de datos	VII.1. Normativa sobre datos personales
	VII.2. Infraestructuras críticas
VIII - Ataques cibernéticos	VIII.1. Conceptualización y tipología
	VIII.2. Ataques activos y pasivos a la información

IV.B.-Actividades formativas

Tipo	Descripción
Lecturas	(AF1) Preparación de los contenidos de la asignatura
Prácticas	(AF2) Actividades de carácter práctico
Laboratorios experimentales y/o tecnológicos	(AF3) Laboratorios de ciberseguridad
Trabajos colectivos	(AF4) Trabajo en grupo
Realización de Pruebas	(AF5) Pruebas
Resolución de ejercicios, problemas, casos	(AF6) Realización de ejercicios sobre plataformas tecnológicas (web)

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

V.-Tiempo de trabajo del alumnado (30h grado y 25h máster)	
Clases teóricas	20
Clases de resolución de ejercicios, problemas, casos, etc.	15
Prácticas en laboratorios experimentales, tecnológicos, clínicos, campo, etc.	15
Realización de pruebas	10
Tutorías académicas	24
Actividades relacionadas: jornadas, seminarios, etc.	24
Preparación de clases teóricas	30
Preparación de prácticas/ejercicios/casos	30
Preparación de pruebas	12
Total de horas de trabajo del alumnado	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Pruebas	Semana 15 a Semana 15	(MD8) Prueba de teoría [AP] * Se desarrollarán preferentemente de forma presencial, siempre y cuando las condiciones sanitarias lo permitan. * Adaptación: [AD] Realización a través del Aula Virtual y, en su caso, sistemas de videoconferencia.
Trabajos colectivos	Semana 1 a Semana 14	(MD4) Trabajo en grupo para el desarrollo de un ejercicio relacionado con la cibercriminalidad [AP] * PC: Si las condiciones sanitarias lo exigen, se activará plan de contingencia mediante el uso de herramientas colaborativas de la Universidad u otras disponibles de software libre
Pruebas	Semana 15 a Semana 15	(MD9) Prueba práctica [AP] * Se desarrollarán preferentemente de forma presencial, siempre y cuando las condiciones sanitarias lo permitan. * Adaptación: [AD] Realización a través del Aula Virtual y, en su caso, sistemas de videoconferencia.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Pruebas	Semana 8 a Semana 15	(MD7) Prueba práctica [AP] * Se desarrollarán preferentemente de forma presencial, siempre y cuando las condiciones sanitarias lo permitan. * Adaptación: [AD] Realización a través del Aula Virtual y, en su caso, sistemas de videoconferencia.
Clases Teóricas	Semana 1 a Semana 15	(MD1) Clases teóricas [AP] * PC: si las condiciones sanitarias lo exigen activar un plan de contingencia (PC) que consistirán en actividades a distancia y adaptación de clases síncronas por videoconferencia
Laboratorios experimentales y/o tecnológicos	Semana 1 a Semana 15	(MD5) Laboratorios para la práctica de la informática relacionada con la criminología [AP] * PC: Si las condiciones sanitarias lo requieren, se adaptarán las actividades formativas a un entorno a distancia (MyApps y equipos domésticos), con permisos de administración y/o mediante la virtualización de entornos Windows/Linux con software libre o aplicaciones disponibles en el entorno descargable de la Universidad
Pruebas	Semana 8 a Semana 15	(MD6) Prueba de teoría [AP] * Se desarrollarán preferentemente de forma presencial, siempre y cuando las condiciones sanitarias lo permitan. * PC: Adaptación a distancia mediante la realización a través del Aula Virtual y, en su caso, sistemas de videoconferencia.
Tutorías académicas	Semana 1 a Semana 14	(MD2) Tutorías académicas [AP] * PC: si las condiciones sanitarias lo exigen activar un plan de contingencia (PC) que consistirán en actividades a distancia. Adaptación de tutorías por videoconferencia y herramientas telemáticas de reunión
Resolución de ejercicios, problemas, casos	Semana 1 a Semana 15	(MD3) Clases prácticas para resolucíón de problemas o casos [AP] * PC: Adaptación si las condiciones sanitarias lo exigen mediante clases síncronas por videoconferencia. Material de virtualización y herramientas informáticas proporcionada por la Universidad o de software libre.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Metodologías activas o de innovación docente	Semana 1 a Semana 15	En las unidades dedicadas al actividades de análisis de ciberseguridad y forense digital que permita utilizar esta técnica, cuidando los contenidos antes de las clases, el durante con el trabajo colaborativo y el después introduciendo el aprendizaje cooperativo.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

VII.-Método de evaluación

El modelo de evaluación general es la evaluación continua, tal como establece el Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

Deberán utilizarse todos los sistemas de evaluación establecidos para la asignatura en la memoria de la titulación, excepto aquellos que tuviesen una ponderación mínima del 0%, que podrán utilizarse en los cursos académicos en los que el profesorado lo considere oportuno. Cada uno de los sistemas de evaluación podrá ser aplicado mediante una o más actividades de evaluación, coherentes con ese sistema. Ninguna de las actividades de evaluación podrá superar individualmente el 60% de la calificación global de la asignatura.

La suma de las actividades de evaluación no revaluables no podrá superar el 40% de la calificación global de la asignatura y, en general, no deberían tener nota mínima (salvo en el caso de actividades de carácter práctico en las que, estrictamente, no pudieran reproducirse en la convocatoria extraordinaria las condiciones de evaluación de la convocatoria ordinaria).

El alumnado que no consiga superar la asignatura en la convocatoria ordinaria, o no se hayan presentado, podrán presentarse a la convocatoria extraordinaria únicamente a las actividades de evaluación revaluables no superadas.

El uso de herramientas basadas en inteligencia artificial está prohibido en cualquier ejercicio y prueba de evaluación de la asignatura salvo que el profesor lo indique de forma explícita en el enunciado o en el material de esta. En caso de que esté permitido, se darán indicaciones precisas de qué usos están permitidos y cuáles no.

La distribución y características de las actividades de evaluación son las que se describen a continuación.

VII.A.- Descripción de las actividades de evaluación y su ponderación

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

El modelo de evaluación general es la evaluación continua, tal como establece el Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos. Deberán utilizarse todos los sistemas de evaluación establecidos para la asignatura en la memoria de la titulación, excepto aquellos que tuviesen una ponderación mínima del 0%, que podrán utilizarse en los cursos académicos en los que el profesorado lo considere oportuno. Cada uno de los sistemas de evaluación podrá ser aplicado mediante una o más actividades de evaluación, coherentes con ese sistema. Ninguna de las actividades de evaluación podrá superar individualmente el 60% de la calificación global de la asignatura.
La suma de las actividades de evaluación no revaluables no podrá superar el 40% de la calificación global de la asignatura y, en general, no deberían tener nota mínima (salvo en el caso de actividades de carácter práctico en las que, estrictamente, no pudieran reproducirse en la convocatoria extraordinaria las condiciones de evaluación de la convocatoria ordinaria).
Los estudiantes que no consigan superar la asignatura en la convocatoria ordinaria, o no se hayan presentado, podrán presentarse a la convocatoria extraordinaria únicamente a las actividades de evaluación revaluables no superadas. La distribución y características de las actividades de evaluación son las que se describen a continuación, evaluandose de acuerdo a las actividades y ponderaciones siguientes:
Se evaluará los contenidos teóricos y prácticos desarrollados en el aula/laboratorio de informática, o su entorno virtualizado remoto en su caso, que podrán seguirse de forma continua.
- *Contenidos teóricos*: Con una valoración del 40% de la calificación final, consistiendo en la realización de una prueba basada en los contenidos y conocimientos del temario de la asignatura (evaluación continua). Se podrá organizar en dos pruebas parciales. El material permitido para la realización de exámenes será determinada expresamente en la convocatoria. Reevaluable.
- *Contenidos prácticos*: Con una valoración del 30% de la calificación final, consistiendo en la realización de una prueba basada en resolución de ejercicios, prácticas y tareas relacionadas con el laboratorio de ciberseguridad y cibercriminalidad, realización de una prueba de conocimientos basada en la realización de trabajos y prácticas dentro del aula,
tanto de casos de laboratorio, presencial o virtualizado (myApps) propias de la asignatura (evaluación continua). Se podrá organizar en dos pruebas parciales. El material y software permitido para la realización de exámenes será determinada expresamente en la convocatoria. Reevaluable.
- Trabajo en grupo (Participación en actividades complementarias y utilización de recursos conexos): Con una valoración del 20% de la calificación final. Consistirá en la realización de un trabajo original relacionado con la cibercriminalidad, a trabajar en grupo que el equipo docente guiará a lo largo del curso con resultado entregable. Excepcionalmente se permitirá trabajo individual, por circunstancias de fuerza mayor a solicitud del estudiante interesado. Reevaluable.
- Participación en clase, actividades complementarias y sesiones de trabajo: 10% de la calificación final. Consistirá en la valoración de la asistencia a clase y las actividades relacionadas con la creación y gestión de contenidos de una página web (tipo weblog) sobre ciberseguridad y ciberdelincuencia. No reevaluable.

Recomendación sobre la asistencia a clase

Se recomienda la asistencia regular a las sesiones de clase debido al elevado componente práctico de la asignatura. El seguimiento continuado de las actividades desarrolladas en el aula de informática, junto con las explicaciones, demostraciones y resolución de dudas por parte del profesorado, facilita la comprensión de los contenidos y favorece la adecuada adquisición de los resultados de aprendizaje previstos. La naturaleza aplicada de la materia hace que muchas de las habilidades trabajadas se desarrollen de forma progresiva mediante la práctica guiada, por lo que la asistencia semanal a las clases contribuye de manera significativa a la correcta asimilación de los conocimientos, competencias y habilidades de la asignatura.

CONVOCATORIA ORDINARIA Y EXTRAORDINARIA:

Se realizarán una prueba con los contenidos teóricos y prácticos (70% de la calificación final).

Deberá entregar trabajo en grupo mediante entregable en las condiciones marcadas sobre un trabajo original sobre cibercriminalidad que debe concertar con el equipo docente (20%).

Para el 10% (no reevaluable) restante de la puntuación, se tendrá en cuenta, en su caso, la participación en actividades complementarias y utilización de recursos conexos.

MUY IMPORTANTE: El alumno que esté involucrado en cualquier tipo de fraude académico (actividades evaluables o no), suspenderá automáticamente la convocatoria correspondiente.

ATENCIÓN: INDICACIONES SOBRE EL SISTEMA DE EVALUACIÓN DE LA ASIGNATURA DIRIGIDAS A LOS ESTUDIANTES QUE CURSEN ESTA ASIGNATURA EN EL CAMPUS DE ARANJUEZ.

Asignatura en modalidad en extinción, evalulable mediante examen. Se considerarán las pruebas de evaluación que han sido

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

cualificadas como actividades reevaluables.

VII.B.- Evaluación del alumnado con dispensa académica de asistencia a clase

La concesión de Dispensa Académica de Asistencia a Clase (DAAC) no implica que se quede automáticamente eximido de participar en las actividades de evaluación continua ni en las actividades formativas presenciales de asistencia obligatoria establecidas en la guía docente. Una vez concedida la dispensa, el alumnado deberá contactar con el docente, que podría proponerle las adaptaciones que considere convenientes, siempre que garanticen la adquisición y adecuada evaluación de los resultados de aprendizaje previstos. El alumnado deberá mantener a lo largo de curso una comunicación fluida con el docente para que este le proporcione información sobre las fechas en que se realizarán esas actividades formativas y de evaluación, en caso de que su programación no estuviese ya fijada y a disposición del alumnado en el momento de la concesión de la dispensa.
Asignatura con posibilidad de dispensa: Sí

VII.C.- Revisión y reclamación de las actividades de evaluación

Se realizará conforme al Reglamento de evaluación de los resultados de aprendizaje de la Universidad Rey Juan Carlos.

VII.D.- Alumnado con discapacidad o necesidades educativas especiales

Con el fin de garantizar la igualdad de oportunidades, la no discriminación, la accesibilidad universal y la mayor garantía de éxito académico, las adaptaciones curriculares para alumnado con discapacidad o con necesidades educativas especiales serán pautadas por la Unidad de Atención a Personas con Discapacidad, de acuerdo con la normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.
Para que esas adaptaciones puedan realizarse, será requisito la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que el alumnado con discapacidad o necesidades educativas especiales deberán contactar con este servicio para analizar conjuntamente las distintas opciones.

VII.E.- Conducta académica, integridad y honestidad académica

La Universidad Rey Juan Carlos está plenamente comprometida con los más altos estándares de integridad y honestidad académica, por lo que estudiar en la URJC supone asumir y suscribir los valores de integridad y la honestidad académica recogidos en el Código Ético de la Universidad.

Para acompañar este proceso, la Universidad dispone de la Normativa de Convivencia de la Universidad Rey Juan Carlos y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

Las herramientas basadas en inteligencia artificial pueden mejorar la experiencia de aprendizaje, pero debe utilizarse de forma ética, legal, honesta y transparente. Por este motivo, deben seguirse las recomendaciones de uso adecuado indicadas por los docentes de la asignatura.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

VIII.-Recursos y materiales didácticos

Bibliografía básica

Principalmente: apuntes, artículos y documentación facilitada por el equipo docente en el Aula Virtual.
Libros suplementarios de interés general:
Cibercriminalidad. AAVV. Dykinson, año 2019. ISBN 978-84-1324-269-9
Manual de Inteligencia. AAVV. Tirant lo Blanch, año 2019. ISBN: 978-84-1336-198-7
Informatica en las Ciencias Criminologícas y de la Seguridad. AAVV. Hernandez Berlinches, R. (coord.) et al.

Bibliografía complementaria

Módulo VIII. Ataques cibernéticos.
Merino Febrero, B. y Holguín, J.M. *Pentesting: recolección de información.* Instituto Nacional de Tecnologías de la Comunicación, CERT INTECO, 2012.

Módulo V. Delincuencia informática.
Avilés, Angel-Pablo. *X1Red+Segura Informando y Educando V1.0.* Creative Common. Angelucho, 2013. En general un libro muy interesante para la materia, en particular capítulos 7 y siguientes.
Gercke, M. *Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica.* Ed. ITU-T, Unión Internacional de Telecomunicaciones, 2014. Se recomienda por su relación con este módulo de la asignatura los capítulos 2 y 3.

Módulo VI. Ingeniería forense.
Haydée Di Iorio, A. et al. *El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense.* InFo-Lab. Ed. Creative Common, 2016. Es un libro extenso editado por capítulos, pero con enfoque hacia criminalistas e informáticos. Interesa el capítulo 1, pp. 45-83; el apartado 2.1 sobre el Convenio de Budapest, pp. 95-101; el capítulo 6, sobre aspectos técnicos, pp. 345-399.
Francisco Lázaro Domínguez. *Introducción a la Informática Forense.* RA-MA Editorial. ISBN: 978-84-9964-209-3.
Rohit Tamma et al: *Practical Mobile Forensics* (Packt Publishing), 3ª ed., 2018. ISBN-10: 1788839196.
Emily Harwood. *Digital CCTV: a security professional's guide.* Elsevier/Butterworth-Heinemann. 1º ed., Amsterdam/Boston, 2008. ISBN: 978-0750677455. Capítulos 1, 2, 3, 4 y 5.
ENFSI - DIWG. *ENFSI-BPM-DI-02 - Best Practice Manual for Forensic Image and Video Enhancement* (European Network of Forensic Sciences – Digital Image) Version 01 – June 2018.
LEVA. *Best Practices for the Acquisition of Digital Multimedia Evidence.* (Law Enforcement & Emergency Services Video Association International. Inc.) Version 3.0. April 14, 2010.

Módulo VII. Protección de datos.
BOE. *Códigos electrónicos: Protección de Datos de Carácter Personal*. Publicaciones de la Agencia Estatal Boletín Oficial del Estado. Este es un compendio de normativa que el BOE publica en su web (www.boe.es) relacionado por temática, interesando esencialmente lo referente a la Ley Orgánica de Protección de Datos y su reglamento de medidas de desarrollo.
AEPD. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento.* Disponible en la web de la Agencia de Protección de Datos (www.aepd.es), de interés por la aplicación del Reglamento Europeo aprobado en 2016 y en vigor desde mayo de 2018.

Módulo I. Fundamentos de Informática.
ITU-T. *Manual sobre redes basadas en el Protocolo Internet (IP) y asuntos conexos.* Unión Internacional de Telecomunicaciones, 2005.
Joyanes Aguilar, L. *Fundamentos de programación: algoritmos y estructura de datos y objetos.* 4ª Ed. MCGRAW-HILL. 2008. Especialmente interesante los capítulos 1, 2 y 3 de introducción a la computación y estructura básica del software, así como el capítulo 9 sobre archivos y su organización.

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Módulo II. Organización de la Seguridad de la Información.
ITU-T. X.1205: *Aspectos generales de la ciberseguridad.* Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. Seguridad en el ciberespacio – Ciberseguridad. Unión Internacional de Telecomunicaciones, 2008.
Carpio Cámara, M., León, A., Cano Carrillo, J., Jiménez, C. E. *Regulación y ciberseguridad. Contribuciones al modelo de Gobernanza.* Capítulo del libro "Gobernanza de Internet en España", IGF Forum Spain, 2015. Aunque el libro completo es interesante como lectura actual del estado de la ciberseguridad en España, especialmente recomendable consultar el Capítulo 3 por su relación con la asignatura.
ITU-T. *Guía de ciberseguridad para los países en desarrollo.* Unión Internacional de Telecomunicaciones, 2009.

Módulo III. Análisis de riesgos.
Comunidad de Madrid. *Análisis y cuantificación del riesgo.*
MINHAP. *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Libro I – Método, 2008.
CCN. *Guía de Seguridad de las TIC CCN-STIC 470 H1 PILAR.* Centro Criptológico Nacional, 2017.

Módulo IV. Códigos maliciosos.
INTECO. *Malware y Robo de datos.* Instituto Nacional de Tecnologías de la Comunicación, 2010.
SIKORSKI, Michael; HONIG, Andrew. *Practical malware analysis: the hands-on guide to dissecting malicious software.*, 2012.
IANELLI, Nicholas; HACKWORTH, Aaron. *Botnets as a vehicle for online crime.* FORENSIC COMPUTER SCIENCE IJoFCS, 2005, vol. 19.

IX.-Profesorado	
Nombre y apellidos	ANGEL TOMÁS LEDO IGLESIAS
Correo electrónico	angeltomas.ledo@urjc.es
Departamento	Economía Financiera y Contabilidad
Campus de impartición	Alcorcón
Categoría	Profesor/a Asociado/a
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0
Nombre y apellidos	FRANCISCO JAVIER GALÁN NOVILLO
Correo electrónico	francisco.galan@urjc.es
Departamento	Economía Financiera y Contabilidad
Campus de impartición	Alcorcón
Categoría	Profesor/a Asociado/a

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0
Nombre y apellidos	JESÚS SALVADOR CANO CARRILLO
Correo electrónico	jesus.cano@urjc.es
Departamento	Economía Financiera y Contabilidad
Campus de impartición	Alcorcón
Categoría	Profesor/a Asociado/a
Titulación académica	Doctor
Responsable de asignatura	Si
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0
Nombre y apellidos	ROBERTO CUESTA CALVO
Correo electrónico	roberto.cuesta@urjc.es
Departamento	Economía Financiera y Contabilidad
Campus de impartición	Madrid - Vicálvaro
Categoría	Profesor/a Asociado/a
Responsable de asignatura	No
Horario de tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/a a través de correo electrónico
Nº de Quinquenios	0

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.

Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Nº de evaluaciones positivas Docentia	0

Q2803011B UNIVERSIDAD REY JUAN CARLOS
Fecha firma: 09/11/2026 21:13 | Hash: 4e9b2b2ed00cf6e60172a7570e028ab9.