

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Optativas	SEGURIDAD DE REDES Y TELECOMUNICACIONES	4º	7º	6	Optativa
PROFESORES			DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)		
<ul style="list-style-type: none"> <li>José Antonio Gómez Hernández: Teoría y prácticas</li> </ul>			Dpto. Lenguajes y Sistemas Informáticos, 3ª planta, E.T.S. de Ingenierías Informática y de Telecomunicación. Despachos nº 10. Correo electrónico: <a href="mailto:jagomez@ugr.es">jagomez@ugr.es</a>		
COORDINADOR DE LA ASIGNATURA: José Antonio Gómez Hernández			HORARIO DE TUTORÍAS Y/O ENLACE A LA PÁGINA WEB DONDE PUEDAN CONSULTARSE LOS HORARIOS DE TUTORÍAS*  <a href="https://lsi.ugr.es/lsi/jagomez">https://lsi.ugr.es/lsi/jagomez</a>		
GRADO EN EL QUE SE IMPARTE			OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR		
Grado en Criminología			Cumplimentar con el texto correspondiente, si procede		
PRERREQUISITOS Y/O RECOMENDACIONES (si procede)					
Ninguno					
BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)					
<ul style="list-style-type: none"> <li>Análisis técnico-profesional de la seguridad de las redes y telecomunicaciones.</li> <li>Protección de sistemas informáticos y certificados digitales. Seguridad en sistemas de tiempo real y distribuidos. Vulnerabilidad de sistemas operativos.</li> <li>Principales delitos cometidos en Internet: ciberterrorismo, ataques a la propiedad intelectual en Internet, intervención de las comunicaciones, intromisiones en la intimidad y el derecho a la propia imagen y tratamientos no autorizados de datos personales, ataques al honor y suplantación de</li> </ul>					



personalidad, fraude de tarjetas de crédito en Internet, *phishing* o captación de datos para ser usados de manera fraudulenta, *bullying* o maltrato psicológico a menores en la Red, ciberacoso, difusión de material pornográfico en Internet, etc., virus y daños informáticos.

## COMPETENCIAS GENERALES Y ESPECÍFICAS

### Competencias básicas y generales

- G2. Dominar las técnicas e instrumentos para la evaluación y predicción de la criminalidad.
- G5. Comprender la complejidad y diversidad del fenómeno criminal en un mundo global.
- G11. Conocer y utilizar adecuadamente las Tecnologías de la Información y la Comunicación en la resolución de problemas y búsqueda de información en el ámbito de la Criminología y la Seguridad.
- G12. Ser capaz de trabajar en equipo con otros profesionales en las diferentes vertientes de la actividad criminológica.
- G13. Desarrollar una aptitud crítica frente a la realidad social respetando los principios de igualdad, derechos humanos, paz y accesibilidad universal.

### Competencias específicas

- E2. Interpretar las fuentes de datos relacionados con la criminalidad: gráficos, estadísticas, etc.
- E5. Atender las necesidades de la víctima a nivel individual, grupal y comunitario, con especial referencia a colectivos muy victimizados como las víctimas de violencia de género, los menores o los incapaces.
- E7. Elaborar de informes para evaluar las situaciones de riesgo de los menores, medidas aplicables a los infractores y medidas de protección a los que estén en situación de abandono.
- E11. Aplicar las técnicas de investigación adecuadas para la persecución de delitos garantizando la seguridad ciudadana, los derechos fundamentales y la resolución de conflictos sociales.
- E16. Conocer y aplicar las técnicas y estrategias para la evaluación y predicción de la conducta criminal.
- E17. Capacidad de aplicar los conocimientos psicosociales al estudio y comprensión de las nuevas formas de criminalidad.

## OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

- Conocer la tipología de delitos informáticos y la legislación vigente al respecto.
- Comprender los conceptos básicos de informática y de los componentes de un sistema informático y de redes de computadores.
- Utilizar las herramientas básicas para la detección y prevención de delitos frecuentes.
- Conocer las bases de la seguridad de sistemas informáticos.
- Profundizar en el método de investigación forense informática.
- Saber elaborar un informe pericial informático.

## TEMARIO DETALLADO DE LA ASIGNATURA

### TEMARIO TEÓRICO:

- **Tema 1.** Informática para criminólogos.
  - 1.1. Conceptos básicos de Informática.
  - 1.2. Componentes de un sistemas informático: hardware y software.
  - 1.3. Redes de comunicaciones: hardware, protocolos y servicios.



- **Tema 2.** Cibercriminalidad.
  - 2.1. El crimen en el ciberespacio: características y cuantificación del problema.
  - 2.2. Tipos y cibercrímenes.
  - 2.3. Los cibercriminales.
  - 2.4. Las cibervíctimas.
  - 2.55. Legislación.
- **Tema 3.** Prevención y detección del cibercrimen.
  - 3.1. Intrusiones y ataques a sistemas.
  - 3.2. Seguridad en sistemas operativos y redes de comunicaciones.
  - 3.3. Criptografía y certificados digitales.
  - 3.4. Técnicas y herramientas para la detección y prevención del cibercrimen.
- **Tema 4.** Peritaje informático
  - 4.1. El perito informático.
  - 4.2. Aspectos legales y jurídicos del peritaje,
  - 4.3. Tipos de peritajes.
  - 4.4. Fases del peritaje.
  - 4.5. La prueba pericial.
  - 4.6. El informe pericial.
- **Tema 5.** Informática forense.
  - 5.1. Fundamentos de la informática forense.
  - 5.2. El proceso de investigación forense informático.
  - 5.3 Laboratorio de Informática Forense.
  - 5.4. Metodologías y procedimientos para la obtención, gestión y análisis de evidencias digitales.
  - 5.5. Informática forense en dispositivos móviles.

#### TEMARIO PRÁCTICO:

##### Seminarios

- Realización de un trabajo trabajo grupal y su exposición relacionado con la materia.

##### Prácticas de Laboratorio

1. Herramientas básicas de seguridad
2. Identidad digital y privacidad.
2. Herramientas para la prevención y detección de delitos informáticos.
3. Informática forense e informe pericial.

#### BIBLIOGRAFÍA

##### BIBLIOGRAFÍA FUNDAMENTAL:

- 1. Fernández Teruelo, J. G., Cibercrimen. Los delitos cometidos a través de Internet, Constitutio



Criminalis Carolina, 2007.

- 2. Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2010.
- 3. P.W. Singer y Allan Friedman, Cybersecurity and Cyberware: What Everyone Needs to Know, Oxford University Press, 2014.
- 4. Raoul Chiesa, Stefania Ducci, y Silvio Ciappi, Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking, CRC Press, 2009.
- 5. Debra Littlejohn y Michael Cross, Scene of the Cybercrime, 2nd Ed., Syngress, 2008.
- 6. Chuch Easttom y Det Jeff Taylor, Computer Crime, Investigation, and the Law, Course Technology, CENGAGE Learning, 2011.
- 7. ITU, Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica, Unión Internacional de Telecomunicaciones (ITU), Sept. 2012. (disponible en <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcimeS.pdf>).
- 8. K. Jaishandar, Ed., Cybercriminology. Exploring Internet crimes and Criminal Behavior, CRC Press, 2011.
- 9. Fernando Miró Llinares, El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio, Marcial Pons, 2012.
- 10. Ernesto Martínez de Carvajal Hedrich, Informática Forense. 44 casos reales, Editorial Ernesto Martínez de Carvajal Hedrich, 2012.
- 11. Rafael López Rivera, El peritaje informático y tecnológico, Editor Rafael López Rivera, 2012.
- 12. Juan Diego Pérez Villa, Guía Visual de Introducción a la Informática, Anaya, 2014.
- 13. Brett Shavers, Cybercrime Case Presentation. Using Digital Forensics and Investigative Techiques to Identify Cybercrime Suspects, Syngress, 2013.
- 14. Eoghan Casey, Digital Evidence and Computer Crime. Forensic Science, Computers and The Internet, 3th Ed., Academic Press, Elsevier, 2011.
- 15. Glenn Brookshear, J., Introducción a la Computación, Pearson Educación, 2012.
- 16. Barceló Ordinas, J.M., et al. Redes de Computadores, Universitat Oberta de Catalunya, 2004.
- 17. Stallings, W. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares, Pearson Educación, 2004.
- 18. Stallings, W. y Brown, L., Computer Security. Principles and Practice, Pearson, 2012.
- 19. Tori, C. Hacking Ético, Carlos Tori, 2008.

#### BIBLIOGRAFÍA COMPLEMENTARIA:

- 1. Romero Casanova, C.M., El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales, Granada, 2006.
- 2. Tomasi, S. N., Peritaje judicial informático, Ediciones del Autor, 2010.
- 3. Michael G. Solomon et al., Computer Forensics Jumpstart, Indianapolis, IN : Wiley, 2011.
- 4. Velasco Núñez, E., Delitos cometidos a través de Internet : cuestiones procesales, Madrid, La Ley, 2010.
- 5. Seminario Duque de Ahumada, Seguridad y nuevas tecnologías, XX Seminario "Duque de Ahumada", (7 y 8 de mayo de 2008), Madrid, Ministerio del Interior, 2009
- 6. Bryant, R. (Ed.), Investigating digital crime, Chichester, England ; Hoboken, N.J. : J. Wiley & Sons, 2008.
- 7. Bejtlich, R. The Tao of Networking Security Monitoring. Beyond Instruction Detection, Addison-Wesley Professional, 2004.



- 8. Aissi, S., Dabbous, N. y Prasad, A. R., Security for Mobile Network and Platforms, Artech House, 2006.
- 9. Rash, M. et al., Intrusión Prevention and Active Response. Deploying Network and Host IPS, Syngress, 2005.
- 10. Cuesta Arzamendi, J. L. de la, Derecho Penal Informático, Civitas, 2010.
- 11. Marjie T. Britz, Computer Forensics and Cyber Crime: An Introduction, 2/E, Prentice Hall, 2009.
- 12. Altheide, C. y Carvey, H., Digital Forensics with Open Source Tools, Syngress, 2011.
- 13. Mahid Yar, Cybercrime and Society, Sage Publications, 2006.
- 14. Panagiotis Kanellis et al., Digital Crime and Forensic Science in Cyberspace, Idea Group Publishing, 2006.

#### ENLACES RECOMENDADOS

Plataforma docente: <https://prado.ugr.es>  
 Página web del Departamento: <https://lsi.ugr.es/lsi/node/2844>

#### METODOLOGÍA DOCENTE

La metodología que se propone parte de combinar distintas herramientas docentes –clases presenciales, seminarios, actividades alternativas y trabajo autónomo- con objeto de crear una metodología activa y participativa que permita que el estudiante no solo adquiera los conceptos fundamentales de la Asignatura sino que pueda seguir profundizando en la materia de forma autónoma.

##### 1) CLASES PRESENCIALES (teóricas y prácticas).

- El método propuesto parte de combinar la lección magistral, complementada con el desarrollo de clases prácticas en la que se debaten casos prácticos. Esto permite un equilibrio entre la adquisición de conocimientos y su aplicación práctica. Tanto en las clases prácticas como teóricas la implicación del alumno con sus aportaciones en la valoración de las cuestiones objeto de estudio es fundamental para favorecer su proceso de aprendizaje tanto en la asignatura como en su desarrollo profesional.

##### 3) TRABAJOS MONOGRÁFICOS TUTORIZADOS Y PRESENTACIONES

- Durante el desarrollo del curso, se propondrá el estudio monográfico por parte de los alumnos, en pequeños grupos, de algunas figuras delictivas informáticas así como las herramientas para prevenirlas y detectarlas. Tales trabajos serán supervisados periódicamente por el profesor, suministrando bibliografía básica a utilizar, material jurisprudencial e informático, así como la metodología para su elaboración. Los mejores trabajos pueden ser expuestos y discutidos en clase.

##### 4) ACTIVIDADES INDIVIDUALES Y GRUPALES

- Parte importante en el aprendizaje del estudiante es el estudio y trabajo autónomo destinado a abordar bien actividades, guiadas o no, por el profesor para profundizar en el conocimiento de la materia, bien como estudio de los contenidos.

##### 5) TUTORÍAS INDIVIDUALES O GRUPALES

- Destinadas tanto a orientar el trabajo autónomo individual como grupal de los estudiantes como para



profundizar o aclarar los contenidos de la materia.

#### EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

Como establece el punto 2 del Artículo 6 de la Normativa de Evaluación y de calificación de los estudiantes de la Universidad de Granada (NCG71/2, accesible desde el enlace [https://lsi.ugr.es/lsi/normativa\\_examenes](https://lsi.ugr.es/lsi/normativa_examenes)), la evaluación de la asignatura será en la convocatoria ordinaria mediante la modalidad de evaluación continua. Quienes deseen la realización de un "Examen Único Final" deberán solicitarlo en los términos que establece la citada normativa (Art. 8).

##### - Convocatoria ordinaria

La evaluación continua constará de las siguientes actividades:

- Teoría: Se realizarán dos pruebas objetivas individuales por escrito que constarán cuestiones concretas de respuesta corta sobre los contenidos teóricos del tema (similares a las existentes en la relaciones de ejercicios propuestos). Esta parte contribuye con un 40% de peso a la calificación final.
- Prácticas: Para cada una de las prácticas, que se realizan en individualmente, o en grupo dependiendo del número de matriculados, se deberá entregar una memoria de la misma donde se expliquen los pasos seguidos para la solución a un caso práctico propuesto en la Guía de Prácticas. Esta parte contribuye con un 40% a la calificación final si se realizan todos los supuestos.
- Trabajo grupal tutorizado: durante el semestre se realizará un trabajo en grupo tutorizado que será evaluado mediante rúbrica y se expondrá en clase. Esta parte contribuye con 20% a la calificación final: 10% para el trabajo y 10% la presentación del mismo.
- La calificación final es la suma de las calificaciones de teoría, prácticas y seminarios y trabajos tutorizados. Condición previa para realizar la suma de cada parte calificable es que se debe obtener al menos un 2 sobre 5 de la calificación en teoría y, otro tanto, en prácticas.

Además se establecen las siguientes consideraciones generales:

- Para poder superar la evaluación continuada será necesario haber realizado un mínimo del 80% de todas las actividades propuestas, tanto para teoría como en prácticas.
- La calificación final de la asignatura es la suma de las calificaciones de cada una de las actividades descritas anteriormente.
- Para superar la Asignatura es necesario obtener un mínimo de 5 puntos en la calificación final.
- Se recomienda la asistencia tanto a clases teóricas como prácticas, si bien la misma no es obligatoria, y hacer uso de las tutorías (individuales o grupales) para resolver dudas surgidas en el desarrollo de la materia.
- En todas las actividades se tendrá especial cuidado en adjuntar, en virtud del Art. 15 de la Normativa, una declaración explícita de autoría.

##### - Convocatoria extraordinaria y convocatoria especial

Tanto en la convocatoria extraordinaria como en la Convocatoria Especial (Artículo 21 de la Normativa) se



establece el mismo sistema y consideraciones que en el Examen Único Final que se describe en el siguiente Apartado.

#### DESCRIPCIÓN DE LAS PRUEBAS QUE FORMARÁN PARTE DE LA EVALUACIÓN ÚNICA FINAL ESTABLECIDA EN LA "NORMATIVA DE EVALUACIÓN Y DE CALIFICACIÓN DE LOS ESTUDIANTES DE LA UNIVERSIDAD DE GRANADA"

El sistema de evaluación que se describe a continuación es válido para las convocatorias de examen extraordinarias, especiales y exámenes únicos finales, y consta de:

- Teoría – examen final escrito sobre el temario de la Asignatura. Constará de preguntas cortas y/o ejercicios similares a los propuestos en clase. Su contribución a la calificación final es del 50% y para superarlo es necesario obtener un mínimo de 2 puntos sobre 5.
- Prácticas – examen final en laboratorio o con computador personal. Constará de preguntas relacionadas con los ejercicios propuestos en la Guía de Prácticas. Previo al examen el estudiante habrá tenido que realizar una memoria documentando las soluciones a los ejercicios propuestos en la Guía de prácticas. El examen de prácticas tiene un peso de 30% en la calificación final y la memoria de prácticas de un 20%. Para superarla es necesario obtener un mínimo de 2 puntos sobre 5.

Además se aplican las consideraciones generales:

- La calificación final de la asignatura es la suma de las calificaciones de cada una de las actividades descritas anteriormente.
- Para superar la Asignatura es necesario obtener un mínimo de 5 puntos en la calificación final.
- En todas las actividades se tendrá especial cuidado en adjuntar, en virtud del Art. 15 de la Normativa, una declaración explícita de autoría.

#### INFORMACIÓN ADICIONAL

