GUIA DOCENTE DE LA ASIGNATURA

SEGURIDAD EN REDES Y TELECOMUNICACIONES

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS
Optativas	SEGURIDAD EN REDES Y TELECOMUNICACIONES	3º	5º	6

PROFESOR(ES)	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)
José Antonio Gómez Hernández	Dpto. Lenguajes y Sistemas Informáticos, 3ª planta, Despacho 10, E.T.S. de Ingenierías Informática y de Telecomunicación. Correo electrónico: jagomez@ugr.es Web: http://lsi.ugr.es/lsi/jagomez
	HORARIO DE TUTORÍAS
	http://lsi.ugr.es/lsi/jagomez
GRADO EN EL QUE SE IMPARTE	OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR
Criminología	

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)
Ninguno
BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)
– Análisis técnico-profesional de la seguridad de las redes y telecomunicaciones. – Protección de sistemas informáticos y certificados digitales. Seguridad en sistemas de tiempo real y distribuidos. Vulnerabilidad de sistemas operativos. – 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 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 generales instrumentales**

  G2. Conocer las técnicas e instrumentos para la evaluación y predicción de la criminalidad.

  G5. Conocer la complejidad y diversidad del fenómeno criminal en un mundo global.

  G11. Utilizar 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.

- **Competencias generales interpersonales**

  G12. Ser capaz de trabajar en equipo con otros profesionales en las diferentes vertientes de la actividad criminologíca.

  G13. Ser capaz de tener una conciencia crítica frente a la realidad social y los problemas sociales respetando los principios de igualdad, derechos humanos, paz y accesibilidad universal.

- **Competencias específicas**

  E2. Saber interpretar las fuentes de datos relacionados con la criminalidad: gráficos, estadísticas, etc.

  E5. Saber atender o cubrir 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. Elaboración de informes para evaluar la situaciones de riesgo de los menores, medidas aplicables a los infractores y medidas de protección a los que estén en situación de abandono.

  E11. Saber 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. Ser capaz de aplicar los conocimientos psicosociales al estudio y comprensión de las nuevas formas de criminalidad.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

Con el desarrollo del curso se pretende fundamentalmente alcanzar los siguientes objetivos:

- 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. Delitos informáticos.

I. Conceptos básicos. II. Tipos de delitos informáticos y cibernéticos. III. Delincuentes y víctimas. IV. Legislación sobre Tecnologías de la Información y Comunicaciones.

Tema 2. Informática criminalista.

I. Conceptos de Informática aplicados a la criminología. II. Elementos hardware de sistemas informáticos y redes de computadores. III. Software de sistemas informáticos y redes. IV. Aspectos tecnológicos de los delitos informáticos.

Tema 3. Seguridad y protección.

I. Seguridad y protección de sistemas operativos frente a delitos informáticos. II. Seguridad y protección de redes de computadores y telecomunicaciones frente a amenazas. III. Herramientas hardware y software para la prevención y detección de delitos informáticos.

Tema 4. Informática forense.

I. Fundamentos de la informática forense. II El proceso de investigación forense informático. III Laboratorio de Informática Forense. IV Metodologías y procedimientos para la obtención, gestión y análisis de evidencias digitales. V. Informática forense en dispositivos móviles.

Tema 5. Peritaje informático

I. El perito informático, II. Aspectos legales y jurídicos del peritaje, III. Tipos de peritajes. IV. Fases del peritaje, V. La prueba pericial, VI. El informe pericial. VII. Tasaciones y arbitrajes, VIII. Áreas de interés para peritajes informáticos.

TEMARIO PRÁCTICO:

1. Realización de casos prácticos y discusión en clase sobre ciberdelitos.
2. Utilización de herramientas para la prevención y detección de delitos informáticos.
3. Desarrollo de un supuesto de informática forense y presentación de resultados.
4. Realización de seminarios, trabajos y exposiciones relacionados con la materia.

BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA:

1. Oronzo Greco. A., *Problemas de criminología informática*, Aracne, 2005.
2. Sueiro, C. C., Fillia, L. C., Monteleone, R., y Nager, H. S., *Análisis integrado de la criminalidad informática*, Di Plácido, 2007.
3. Fernández Teruelo, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, 2007.
4. Marjie T. Britz, *Computer Forensics and Cyber Crime: An Introduction*, 2/E, Prentice Hall, 2009.
5. Arellano González, L. E., y Darahuge, M. E., *Manual de Informática forense. Bases metodologícas:*

Científica sistémica criminalista y marco legal, Errepar, 2011.
6. Brookshear, J. G., *Introducción a la Computación*, Pearson, 2012.
7. Stamp, M., *Information Security. Principles and Practice*, Wiley-Interscience, 2005.
8. Altheide, C. y Carvey, H., *Digital Forensics with Open Source Tools*, Syngress, 2011.
9. Amoroso, E., *Cyber Attacks. Protecting National Infraestructure*, Butterworth-Heinemann, 2010.
10. Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2010.
11. Mahid Yar, Cybercrime and Society, Sage Publications, 2006.
12. P.W. Singer y Allan Friedman, Cybersecurity and Cyberware: What Everyone Needs to Know, Oxford University Press, 2014.
13. Panagiotis Kanellis et al., *Digital Crime and Forensic Science in Cyberspace*, Idea Group Publishing, 2006.
14. Raoul Chiesa, Stefania Ducci, y Silvio Ciappi, Profiling Hackers. *The Science of Criminal Profiling ass Applied to the World of Hacking*, CRC Press, 2009.
15. Debra Littlejohn y Michael Cross, *Scene of the Cybercime, 2nd Ed*., Syngress, 2008.
16. Chuch Easttom y Det Jeff Taylor, *Computer Crime, Investigation, and the Law*, Course Technology, CENGAGE Learning, 2011.
17. 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/CybcrimeS.pdf).
18. K. Jaishandar, Ed., *Cybercriminology. Exploring Internet crimes and Criminal Behavior*, CRC Press, 2011.
19. Fernando Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, 2012.
20. Ernesto Martínez de Carvajal Hedrich, *Informática Forense. 44 casos reales*, Editorial Ernesto Martínez de Carvajal Hedrich, 2012.
21. Emilio del Peso Navarro (Dtor.), *Peritajes informáticos, 2º Ed*., Diaz de Santos, 2001.
22. Rafael López Rivera, *El peritaje informático y tecnológico*, Editor Rafael López Rivera, 2012.
23. Juan Diego Pérez Villa, *Guía Visual de Introducción a la Informática*, Anaya, 2014.
24. Brett Shavers, *Cybercrime Case Presentation. Using Digital Forensics and Investigative Techiques to Identify Cybercrime Suspects*, Syngress, 2013.
25. Eoghan Casey, *Digital Evidence and Computer Crime. Forensic Science, Computers and The Internet, 3th Ed*., Academic Press, Elsevier, 2011.

BIBLIOGRAFÍA COMPLEMENTARIA:

1. Romero Casanova, C.M., *El cibercrimen: nuevos retos juridicos-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*, Indianopolis, 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. Deploing Network and Host IPS*, Syngress, 2005.
10. José Luis de la Cuesta Arzamendi, *Derecho Penal Informático*, Civitas, 2010.
11. Xabiel García Pañeda y David Melendi Palacio, *La peritación informática. Un enfoque práctico*, Colegio Oficial de Ingenieros en Informática del Principado de Asturias (COIIPA), 2008.

ENLACES RECOMENDADOS

Revistas electrónicas:

- Ciencia Penal y Criminología en http://criminet.ugr.es/recpc/
- El Derecho Informático en: http://www.elderechoinformatico.com
- Informes anuales de Internet Crime Complaint Center (IC3), disponibles en http://www.ic3.gov/media/annualreports.aspx.
- Blog Cibercrimen: http://www.cibercrimen.es/

Plataforma y web docentes:

http://tutor.ugr.es
http://lsi.ugr.es

El material relacionado con la Asignatura se va a migrar a la plataforma Prado2 (http://innovacampus.ugr.es/neoprado_oracle/).

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.

2) SEMINARIOS

Los seminarios son otra actividad docente de interés al permitir profundizar en determinados aspectos o temas de la asignatura que, ya sea por las limitaciones de tiempo u otra índole, no pueden explicarse en las clases teóricas y prácticas. Son de carácter voluntario, tienen una participación restringida de alumnos y el tema es elegido por ellos, de forma que se logre una participación mayor a la conseguida en clases de teoría o prácticas. Favoreciendo competencias transversales derivadas de la preparación, exposición y discusión del tema que han elegido, así como la elaboración de una memoria final del mismo.

3) TRABAJOS MONOGRÁFICOS TUTORIZADOS

Durante el desarrollo del curso, se propondrá el estudio monográfico por parte de los alumnos, individualmente o 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, http://secretariageneral.ugr.es/bougr/pages/bougr71/ncg712/!), la evaluación de la asignatura será principalmente mediante evaluación continua. Quienes deseen la realización de un examen final único deberán solicitarlo en los términos que establece la citada normativa.

La evaluación continua constará

- Teoría: Se realizará una prueba objetiva individual por tema que constará de una o dos cuestiones sobre los contenidos teóricos del tema. Esta parte contribuye con un 40% contribuye con un punto a la calificación final.
- Prácticas: Para cada una de las prácticas, que se realizan en grupo, se deberá entregar una memoria de la misma donde se resuelve un caso práctico. Esta parte contribuye con un 40% a la calificación final.
- Seminarios y trabajos tutorizados: durante el semestre se realizará al menos un seminario y/o trabajo en grupo tutorizado que será evaluado mediante rúbrica y que se expondrá en clase. Esta parte contribuye con 20% a la calificación final.

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 20% de la calificación en teoría y, otro tanto, en prácticas. Quienes superen la evaluación continuada no deben realizar el examen final.

El examen final constará de dos partes. En la primera, se realizaran dos preguntas objetivas por cada tema de teoría. En la segunda, la resolución de tres supuestos prácticos. La duración máxima del examen escrito será de 180 minutos. La calificación de cada parte es sobre 5. Para sumar ambas calificaciones es necesario que la calificación de cada una de ellas sea igual o superior al 40%. Para aprobar el examen escrito es imprescindible obtener una calificación mínima de 5.

INFORMACIÓN ADICIONAL

Recomendaciones para la evaluación

Asistir a las actividades presenciales y realizar las actividades de trabajo autónomo propuestas. Hacer uso de las tutorías (individuales o grupales) para resolver dudas surgidas en el desarrollo de la materia.

Régimen de asistencia a clase

Para poder superar la evaluación continuada será necesario haber realizado un mínimo del 85% de todas las actividades propuestas, tanto para teoría como en prácticas.