Fecha de aprobación: **26/06/2023**

Guía docente de la asignatura

Seguridad de Redes y Telecomunicaciones (24511B4)

Grado	Grado en Criminología	**Rama**	Ciencias Sociales y Jurídicas
Módulo	Técnicas y Pericia Criminal	**Materia**	Seguridad de Redes y Telecomunicaciones

Curso	3º	**Semestre**	1º	**Créditos**	6	**Tipo**	Optativa

PRERREQUISITOS Y/O RECOMENDACIONES

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 ASOCIADAS A MATERIA/ASIGNATURA

COMPETENCIAS GENERALES

- CG02 - Dominar las técnicas e instrumentos para la evaluación y predicción de la criminalidad (Acuerdo Andaluz).
- CG05 - Comprender la complejidad y diversidad del fenómeno criminal en un mundo global (Acuerdo Andaluz).
- CG11 - 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. (Acuerdo Andaluz).
- CG12 - Ser capaz de trabajar en equipo con otros profesionales en las diferentes vertientes de la actividad criminológica (Acuerdo Andaluz).

- CG13 - Desarrollar una actitud crítica frente a la realidad social respetando los principios de igualdad, derechos humanos, paz y accesibilidad universal (Acuerdo Andaluz).

COMPETENCIAS ESPECÍFICAS

- CE02 - Interpretar las fuentes de datos relacionados con la criminalidad: gráficos, estadísticas, etc. (Acuerdo Andaluz y Libro Blanco).
- CE05 - 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. (Acuerdo Andaluz, RD 1393/2007).
- CE07 - Elaborar 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 (Acuerdo Andaluz y Libro Blanco).
- CE11 - Aplicar las técnicas de investigación adecuadas para la persecución de delitos garantizando la seguridad ciudadana, los derechos fundamentales y la resolución de conflictos sociales (RD 1393/2007, Libro Blanco y Acuerdo Andaluz).
- CE16 - Conocer y aplicar las técnicas y estrategias para la evaluación y predicción de la conducta criminal (Acuerdo Andaluz, RD 1393/2007 y Libro Blanco).
- CE17 - Capacidad para aplicar los conocimientos psicosociales al estudio y comprensión de las nuevas formas de criminalidad (Libro Blanco de la Criminología y Acuerdo andaluz).

RESULTADOS DE APRENDIZAJE (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 y de las personas en el ciberespacio.
- Profundizar en el método de investigación forense informática.
- Saber elaborar un informe pericial informático.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

- **Tema 1. Informática para criminólogos.**

1.1. Conceptos básicos de Informática.
1.2. Componentes de un sistema informático: hardware, firmware y software.
1.3. Redes de comunicaciones: hardware, protocolos y servicios.
1.4. Elementos avanzados de computación: computación en la nube e Inteligencia Artificial.

- **Tema 2. Cibercriminalidad.**

2.1. Definición y contexto.
2.2 El crimen en el ciberespacio: características y cuantificación del problema.
2.3. Clasificación y tipología de cibercrímenes.
2.4. Los cibercriminales.
2.5. Las cibervíctimas.
2.6. Aspectos normativos del cibercrimen.

- **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: certificados digitales y firma digital.
3.4. Técnicas y herramientas para la detección y prevención del cibercrimen.

- **Tema 4. Informática forense.**

4.1. Fundamentos de la informática forense.
4.2. La evidencia digital.
4.3. Modelo de procesos de investigación forense informático.
4.4. Laboratorio de Informática Forense.
4.5. Metodologías, estándares y guías de buenas prácticas.
4.6. Informática forense en la red, dispositivos móviles y en la nube.

- **Tema 5. Peritaje informático**

5.1. El perito informático.
5.2. Aspectos legales y jurídicos del peritaje
5.3. Tipos y fases de peritajes.
5.4. La prueba y el informe pericial.

PRÁCTICO

- **Práctica 1. Herramientas básicas de seguridad**:

1.1. Obtener información de la configuración y del funcionamiento del sistema.
1.2. Administración básica del sistema operativo y aplicaciones.
1.3. Herramientas para gestionar/administrar la seguridad del sistema operativo.

- **Práctica 2. Identidad digital y privacidad**.

2.1. Identidad digital, egosurfing y google hacking.
2.2. Navegación privada, rastreo (cookies) y complementos de seguridad/privacidad para la navegación.
2.3. Técnicas anti-phishing.
2.4. Cifrado de datos y de dispositivos. Esteganografía.
2.5. Filtrado de correo y limpieza de metadatos.

- **Práctica 3. Herramientas para la prevención y detección de delitos informáticos**.

3.1. Configuración de cortafuegos. Análisis de malware.
3.2. Análisis de vulnerabilidades. Creación de listas blancas. Análisis de la red. Actualizaciones.

- **Práctica 4. Informática forense e informe pericial**.

4.1 Preservación y análisis forense de sistemas y redes.

- **Seminario 1. TOR y la DarkWeb**.
- **Seminario 2. Seguridad en dispositivos móviles.**
- **Seminario 3. Securización de routers.**

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

1. H. Jahankhani, Cyber Criminology, Springer International Publishing, 2018.
2. Agustina Sanllehí, José R. Montiel Juan, Irene Gámez-Guadix, Manuel, Cibercriminología y victimización online, Síntesis, 2020.
3. Rudger Leukfeldt, Thomas J. Holt, The Human Factor of Cybercrime, Routledge, 2019.
4. Roderick S. Graham, Shawn K. Smith, Cybercrime and Digital Deviance, Routledge, 2019.
5. Janine Kremling, Amanda M. Sharp Parker, Cyberspace, Cybersecurity, and Cybercrime, SAGE Publishing, 2017.

6. Troia, V. (2020). Hunting cyber criminals : a hacker's guide to online intelligence gathering tools and techniques (1st edition). Wiley. https://granatensis.ugr.es/permalink/34CBUA_UGR/1p2iirq/alma991014340747404990
7. Le-Khac, N., & Choo, K. (2020). Cyber and Digital Forensic Investigations A Law Enforcement Practitioner's Perspective (1st ed. 2020.). Springer International Publishing. https://doi.org/10.1007/978-3-030-47131-6. https://granatensis.ugr.es/permalink/34CBUA_UGR/1p2iirq/alma991014304536304990
8. López-Muñoz, J. (2020). Cibercriminalidad e investigación tecnológica . Dykinson.
9. Miró Llinares, F., & Felson, M. (2012). El cibercrimen : fenomenología y criminología de la delincuencia en el ciberespacio . Marcial Pons.
10. Montero Romero, F., Mababu Mukiur, R., Rubio Sánchez, J., & Ruiz Sánchez, G. (2020). Manual básico de ciberseguridad y protección de datos . Exit.
11. Guía práctica de ciberseguridad (1a ed.). (2019). Thomson Reuters Aranzadi.
12. Lázaro Domínguez, F. (2013). Introducción a la informática forense . Ra-Ma.
13. Panek, C. (2020). Security fundamentals (1st edition). Sybex. https://granatensis.ugr.es/permalink/34CBUA_UGR/1p2iirq/alma991014340755504990
14. P. Treu, Cyber Security for Beginners: A Complete Guide to Getting Started in Cybersecurity and Ethical Hacking, Tony Tor, 2020.
15. P. K. Roy, A. K. Tripathy, Cybercrime in Social Media: Theory and Solutions, CRC Press, 2023.
16. T. J. Holt, A. M. Bossler, K. C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, 3er Ed., Routledge, 2022.

BIBLIOGRAFÍA COMPLEMENTARIA

1. A. Gil y Gil, R. Hernández Berlinches, S. Cámara Arroyo, Cibercriminalidad, Dykinson, 2019.
2. O. Lira Arteaga, Ciberdelitos : perspectivas para su persecución . Tirant lo Blanch, 2019.
3. UOC, Los ciberdelitos en el ordenamiento español. Universitat Oberta de Catalunya, 2019.
4. F. Pérez Bes, Ciberseguridad . Lefebvre-El Derecho, 2021.
5. S: Moskowitz, Cybercrime and business : strategies for global corporate security . Butterworth-Heinemann, 2017.
6. F. Pérez Bes, Ciberseguridad . Lefebvre-El Derecho, 2021.
7. D. Arroyo Guardeño, V. Gayoso Martínez, L. Hernández Encinas, Ciberseguridad . CSIC, 2020.
8. Ciberseguridad: un enfoque desde la ciencia de datos. Editorial Universidad Icesi, 2018. https://granatensis.ugr.es/permalink/34CBUA_UGR/1p2iirq/alma991014238948304990.
9. C. Mallada Fernández, Nuevos retos de la ciberseguridad en un contexto cambiante . Thomson Reuters Aranzadi, 2019.
10. D. Canals Ametller, Ciberseguridad : un nuevo reto para el Estado y los Gobiernos Locales . Wolters Kluwer, 2021.
11. P. Vila Avendaño, Técnicas de análisis forense informático para peritos judiciales profesionales . 0xWORD, 2018.

ENLACES RECOMENDADOS

Plataforma docente: https://prado.ugr.es
Página web del Departamento: https://lsi.ugr.es/docencia/grados/grado-criminologia/seguridad-redes-y-telecomunicaciones.
El material docente de cada tema y/o práctica en Prado contiene los enlaces a recursos docentes/didácticas relativos a los ítems afectados.

METODOLOGÍA DOCENTE

- MD01 - Metodología expositivo-participativa de los contenidos
- MD02 - Presentaciones en PowerPoint
- MD03 - Lecturas Especializadas
- MD04 - Uso de materiales audiovisuales
- MD05 - Utilización de plataformas virtuales
- MD06 - Uso de Bases de Datos

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

La evaluación en la convocatoria ordinaria será continua, donde se valoran las actividades obligatorias:

1. 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 35% de peso a la calificación final.
2. Prácticas: Para cada una de las prácticas, que se realizan individualmente 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 35% a la calificación final si se realizan todos los supuestos.
3. Trabajo grupal tutorizado: durante el semestre se realizará un trabajo grupal sobre un ciberdelito y su prevención mediante tecnología, que será tutorizado y se evaluará mediante rúbrica. Dicho trabajo se expondrá en clase. Esta parte contribuye con 30% a la calificación final: 10% para el trabajo y 15% la presentación del mismo. Para la realización del trabajo no se permite la utilización de herramientas de IA (su uso anulará el resultado de esta actividad). Se pasará un test a cada estudiante sobre el trabajo realizado que supone el 10% de la calificación.

La calificación final es la suma de las calificaciones de teoría, prácticas y el trabajo grupal. 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:

1. 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.
2. La calificación final de la asignatura es la suma de las calificaciones de cada una de las actividades descritas anteriormente.
3. Para superar la Asignatura es necesario obtener un mínimo de 5 puntos en la calificación final.
4. 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.

EVALUACIÓN EXTRAORDINARIA

Se compone de los siguientes instrumentos:

- 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.

Si el estudiante superó alguna de las partes (teoría o prácticas) en la Convocatoria Ordinaria, solo deberá realizar la parte no superada.

EVALUACIÓN ÚNICA FINAL

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.

INFORMACIÓN ADICIONAL

En todas las actividades se tendrá especial cuidado en adjuntar, en virtud del Art. 15 de la Normativa, una declaración explícita de autoría.