GUÍA DOCENTE
2026 - 2027

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Seguridad y Redes
Código	E000008018
Título	Grado en Criminología por la Universidad Pontificia Comillas [GCRIMI 14]
Impartido en	Grado en Criminología y Grado en Trabajo Social [Quinto Curso] Grado en Psicología y Grado en Criminología [Quinto Curso]
Nivel	Reglada Grado Europeo
Cuatrimestre	Semestral
Créditos	3,0 ECTS
Carácter	Optativa (Grado)
Departamento / Área	Departamento de Sociología y Trabajo Social
Responsable	Markel Pascual Blanco
Horario	Lunes, 12:40h - 14:30h
Descriptor	La asignatura proporcionará a los alumnos una visión sobre la realidad social actual en el Ciberespacio, configurada por el desarrollo tecnológico, la transformación digital y la polarización global. La denominada sociedad red actual, al margen de su contribución al desarrollo de las sociedades, genera nuevos riesgos, amenazas y oportunidades, nuevas formas de control social, nuevas tipologías delictivas y formas de victimización online. Internet, las redes sociales, las Apps y el desarrollo tecnológico generan elevados impactos que precisan vigilancia, detección y análisis. De esta forma, los contenidos de la asignatura desarrollarán las capacidades de los alumnos para la investigación digital (Ciberseguridad, fuentes abiertas y Deep Web), la comprensión de la evolución de la cibercriminalidad, delincuencia tecnológica y las vías para, como investigadores, protegerse de los riesgos derivados de las nuevas tecnologías.

Datos del profesorado	
Profesor	
Nombre	Markel Pascual Blanco
Departamento / Área	Departamento de Sociología y Trabajo Social
Correo electrónico	mpascual@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Aportación al perfil profesional de la titulación

La asignatura aporta a los estudiantes que finalizan su formación en el doble grado, una visión global sobre los impactos en la seguridad producidos en el Ciberespacio por Internet, las redes sociales, las Apps y las nuevas tecnologías. Bajo esta visión, la aproximación sociológica criminológica es fundamental, siendo preciso realizar una aproximación rigurosa a la realidad social en que vivimos, en una sociedad en red caracterizada por la volatilidad, la incertidumbre, la complejidad y la ambigüedad. Un entorno político, social y económico que, facilitado y potenciado por el Ciberespacio, Inteligencia Artificial y las nuevas comunicaciones, así como avanzados desarrollos tecnológicos, están generando nuevas formas de control social, influyendo en las tipologías delictivas “Cibercriminalidad”, afectando a la

victimización de colectivos, o generando nuevos procesos de desigualdad.

La asignatura pretende potenciar en los alumnos la capacidad de análisis, conjugando el pensamiento crítico con la creatividad, a través de la exposición de casos prácticos, debates y simulaciones. Igualmente, pretende dotar a los alumnos de una base de conocimiento sobre la magnitud del proceso de cambio tecnológico al que asistimos y su impacto en los sistemas de control social y en los fenómenos vinculados a la seguridad. De la misma forma, la asignatura tiene como objetivo dotar a los alumnos de herramientas para la comprensión y el análisis del Ciberespacio, Internet y las redes sociales en la criminología y seguridad: Ciberseguridad, obtención de información, análisis de la información, Ciberinteligencia, seguridad en la utilización de Internet, Apps y redes sociales, apoyos tecnológicos.

Prerrequisitos

Ninguno

Competencias - Objetivos

Competencias

GENERALES

CG01	Capacidad de búsqueda y gestión de información en el área de la Criminología	
	RA1	Conoce y emplea con eficiencia las fuentes de información en el campo de la criminología
	RA2	Elabora la información fundamental de los artículos científicos consultados y cita apropiadamente las fuentes consultadas
CG02	Capacidad de análisis y síntesis de datos e informaciones relevantes en el ámbito profesional de la Criminología	
	RA1	Describe, relaciona e interpreta situaciones y planteamientos sencillos
	RA2	Selecciona los elementos más significativos y sus relaciones en textos complejos
	RA3	Identifica las carencias de información y establece relaciones con los elementos externos a la situación planteada
CG03	Capacidad de organización y planificación en su trabajo como criminólogo	
	RA1	Planifica su trabajo personal de una manera viable y sistemática
	RA2	Se integra y participa en el desarrollo organizado de un trabajo en grupo
CG04	Capacidad para utilizar las Tecnologías de la Información y la Comunicación en el desarrollo de su profesión como criminólogo	
	RA1	Utiliza recursos informáticos adecuados para un trabajo académico general
	RA2	Conoce y utiliza correctamente recursos informáticos para la práctica general de su profesión
	RA3	Conoce y utiliza algunos recursos informáticos básicos para investigación en su ámbito de estudio

CG05	Capacidad para comunicarse de forma oral y escrita correctamente en el desempeño de su trabajo criminológico	
	RA1	Expresa sus ideas de forma estructurada, inteligible y convincente
	RA2	Interviene ante un grupo con cierta seguridad y soltura
	RA3	Escribe con corrección
	RA4	Presenta documentos estructurados y ordenados
	RA5	Elabora, cuida y consolida un estilo personal de comunicación, tanto oral como escrita, y valora la creatividad en estos ámbitos
CG07	Capacidad para el razonamiento crítico y la autocrítica en el ejercicio de su profesión como criminólogo	
	RA1	Se muestra abierto e interesado por nuevas informaciones no contempladas
	RA2	Cambia y adapta sus planteamientos iniciales a la luz de nuevas informaciones
	RA3	Muestra curiosidad por las temáticas tratadas más allá de la calificación
	RA4	Establece relaciones y elabora síntesis propias sobre los contenidos trabajados
CG08	Capacidad para tomar decisiones de forma autónoma y fundamentada sobre problemas profesionales del ámbito de la Criminología	
	RA1	Realiza sus trabajos y su actividad necesitando sólo unas indicaciones iniciales y un seguimiento básico
	RA2	Busca y encuentra recursos adecuados para sostener sus actuaciones y realizar sus trabajos
ESPECÍFICAS		
CE20	Proporcionar información actualizada sobre el impacto de las nuevas tecnologías en la sociedad contemporánea y su impacto sobre la conducta delictiva, las posibilidades que ofrecen de cara a la persecución y reducción del delito, y sus implicaciones en términos de control social	
	RA1	Identificar los puntos de riesgo básicos en redes y sistemas informáticos
	RA2	Seleccionar estrategias de prevención a ataques informáticos

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos
Seguridad y Redes
1. Introducción a la ciberseguridad 2. Ciberseguridad y su relación con la Criminología, psicología y sociología

1. Ciberespacio
2. La sociedad red
3. Fraude

3. Impactos individuales y sociales

Ciberinteligencia: La inteligencia en Ciberseguridad

1. Concepto, alcance y contenidos

2. El ciclo de inteligencia y otros marcos en Ciberinteligencia

3. Cibercrimen. Concepto y tipologías

4. Habilidades para la investigación en el Ciberespacio: Internet y redes sociales

5. Investigación en Social Media / Redes sociales

6. Deep Web, Dark Web y Darknet

7. OPSEC. Seguridad operacional del investigador en el Ciberespacio: Internet y Redes Sociales. Anónimato

8. Aplicaciones prácticas: delitos de odio, radicalización online, impactos en inmigración, desinformación, noticias falsas - fake news,

El futuro de un mundo digital

1. Mundo digital. Tendencias.

2. Ciberespacio, Internet e Inteligencia Artificial

3. Nuevas tecnologías disruptivas

    a. Tendencias tecnológicas

    b. Oportunidades, generales y en materia de Cibercriminología y trabajo social

    c. Nuevos riesgos, amenazas y Oportunidades

    d. Derecho Digital y Nuevas Tecnologías

    e. Ética

4. Presente y futuro del delito y del crimen organizado

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Metodología Presencial: Actividades

- Trabajos de análisis y presentaciones en el aula
- Debate grupal
- Brainstorming grupal
- Estudio de casos (reales o supuestos)
- Simulaciones
- Evaluaciones formativas

Metodología No presencial: Actividades

- Trabajos en equipo e individual
- Lectura y comprensión de materiales y textos complementario

RESUMEN HORAS DE TRABAJO DEL ALUMNO

HORAS PRESENCIALES		
Lecciones magistrales	Trabajos individuales/grupales	Ejercicios prácticos/Seminarios
20.00	2.00	8.00
HORAS NO PRESENCIALES		
Estudio personal y documentación	Trabajos individuales/grupales	Ejercicios prácticos/Seminarios
40.00	10.00	10.00
		CRÉDITOS ECTS: 3,0 (90,00 horas)

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

El uso de IA para crear trabajos completos o partes relevantes, sin citar la fuente o la herramienta o sin estar permitido expresamente en la descripción del trabajo, será considerado plagio y regulado conforme al Reglamento General de la Universidad.

Actividades de evaluación	Criterios de evaluación	Peso

Exámenes	• Comprensión de conceptos • Capacidad de razonamiento y argumentación • Capacidad de síntesis • Calidad de comunicación escrita	60
Trabajos individuales	Un trabajo individual en el que valorará: • Capacidad de aplicar pensamiento crítico • Capacidad de síntesis • Presentación formal • Creatividad • Comunicación escrita. • Aplicación de conceptos teóricos.	20
Trabajos grupales realizado en clase/casa.	Se realizarán prácticas grupales donde se valoran, entre otros aspectos: • Capacidad de trabajar en grupo. • Puesta a puntos de los conocimientos teóricos/prácticos. • Defensa escrita y oral. • Capacidad de redacción.	20

Calificaciones

1. Para superar la asignatura la media ponderará deberá ser igual o superior a cinco puntos. Para que esta media pueda realizarse, deberá también aprobarse el examen final de la asignatura con una calificación igual o superior a cinco. Por otra parte, la no realización del resto de las actividades de evaluación contempladas en los apartados de prácticas (trabajo individual o prácticas realizadas grupalmente en clases), en las fechas y en los formatos que se señalen, significará cero puntos en el apartado correspondiente a la calificación de cada actividad.
2. Los criterios de calificación serán los mismos en la convocatoria ordinaria y extraordinaria, es decir, entre otros aspectos indicados, debe aprobarse el examen final de la asignatura. En la convocatoria extraordinaria no se podrán presentar los trabajos prácticos realizados en el aula de forma grupal que no se hubieran presentado a lo largo del curso en las fechas indicadas por el profesor, pues estas actividades de evaluación forman parte del seguimiento continuo de la asignatura y de la asistencia a las clases.
3. Estos criterios se aplicarán en las convocatorias 1ª y 2ª. En las convocatorias siguientes, los alumnos y los alumnos que ya hayan cursado previamente la asignatura y que tengan la escolaridad cubierta únicamente tendrán que presentarse al examen escrito, que en su caso constituir el 100% de su calificación.
4. La inasistencia comprobada e injustificada a más de un tercio de las horas lectivas impartidas en cada asignatura, contabilizadas en el período comprendido desde el primer día de clase hasta quince días antes del inicio del período de exámenes, puede tener como consecuencia la imposibilidad de presentarse a examen en la convocatoria ordinaria del mismo curso académico (artículo 93.1 del Reglamento General). En el supuesto de que se aplicará esta consecuencia, la pérdida de convocatoria se podrá extender a la convocatoria extraordinaria.
5. El incurrir en una falta académica grave, como es el plagio de materiales previamente publicados o el copiar en su examen u otra actividad evaluada, o no respetar las normas de convivencia básicas puede llevar a la apertura de un expediente sancionador y la pérdida de dos convocatorias.
6. El uso de IA para crear trabajos completos o partes relevantes, sin citar la fuente o la herramienta o sin estar permitido expresamente en la descripción del trabajo, será considerado plagio y regulado conforme al Reglamento General de la Universidad."

PLAN DE TRABAJO Y CRONOGRAMA

Actividades	Fecha de realización	Fecha de entrega
Actividades presenciales	Semanal, en cada sesión	
Lectura y comprensión de apuntes y lecturas	Semanal	
Trabajos grupales	Desde la primera semana	
Trabajo individual	Todo el periodo	

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Bibliografía básica

- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd ed.). Academic Press.
- Cressey, D. R. (1973). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Patterson Smith.
- Gralla, P. (2019). *How the Internet Works* (9th ed.). Que Publishing.
- Hadnagy, C. (2021). *Social Engineering: The Science of Human Hacking* (2nd ed.). Wiley.
- Heuer, R. J. (1999). *Psychology of Intelligence Analysis*. Center for the Study of Intelligence.
- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.
- Mitnick, K., Simon, W., & Wozniak, S. (2011). *The Art of Deception*. Wiley.
- Pherson, K., & Heuer, R. J. (2019). *Structured Analytic Techniques for Intelligence Analysis* (3rd ed.). CQ Press.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.
- Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
- Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
- Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). Sage Publications.

Ciberseguridad y redes

- Easttom, C. (2022). *Network Defense and Countermeasures* (4th ed.). Pearson.
- Goodrich, M., & Tamassia, R. (2014). *Introduction to Computer Security*. Pearson.
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton.

Fraude e investigación

- ACFE (Association of Certified Fraud Examiners). (última edición disponible). *Report to the Nations*.
- Bologna, G. J., Lindquist, R. J., & Wells, J. T. (2013). *The Accountant's Handbook of Fraud and Commercial Crime*. Wiley.
- Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection* (5th ed.). Wiley.

Inteligencia y análisis criminal

- Clark, R. M. (2020). *Intelligence Analysis: A Target-Centric Approach* (6th ed.). CQ Press.
- Ratcliffe, J. H. (2016). *Intelligence-Led Policing* (2nd ed.). Routledge.

Ética, regulación y gobernanza

- Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.
- Johnson, D. G. (2021). *Computer Ethics* (5th ed.). Pearson.

Recursos institucionales recomendados

- Instituto Nacional de Ciberseguridad (INCIBE). Guías y publicaciones técnicas.
- Centro Criptológico Nacional (CCN-CERT). Guías CCN-STIC.
- Agencia de la Unión Europea para la Ciberseguridad (ENISA). *Threat Landscape Reports*.
- Europol. *Internet Organised Crime Threat Assessment (IOCTA)*.
- National Institute of Standards and Technology (NIST). *Cybersecurity Framework*.
- Interpol. Publicaciones sobre cibercrimen y fraude digital.

Bibliografía Complementaria

Recursos abiertos y disponibles

Webs y documentos oficiales:

- Ministerio del Interior (ESPAÑA) : https://www.interior.gob.es/opencms/ca/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones/publicaciones-descargables/publicaciones-periodicas-anuarios-y-revistas/informe-sobre-la-cibercriminalidad-en-espana/
- INCIBE (ESPAÑA): https://www.incibe.es/
- CCN-CERT (ESPAÑA): https://www.ccn-cert.cni.es/
- OSI (ESPAÑA): https://www.osi.es/es
- OEA (Organización de los Estados Americanos) : https://www.oas.org/es/
- WORLD ECONOMIC FORUM: https://es.weforum.org/agenda/2022/02/informe-de-riesgos-globales-2022-lo-que-debes-saber/
- INTERPOL: https://www.interpol.int/es
- EUROPOL: https://www.europol.europa.eu/about-europol:es
- FBI: https://www.fbi.gov/news/espanol
- United Nations: https://www.un.org/