COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2022 - 2023

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
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
Créditos	3,0 ECTS
Carácter	Optativa (Grado)
Departamento / Área	Departamento de Sociología y Trabajo Social
Responsable	Mikel Rufián Albarrán
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 y la transformación digital. 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	Mikel Rufián Albarrán
Departamento / Área	Departamento de Sociología y Trabajo Social
Correo electrónico	mrufian@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 (entorno **VUCA** y **BANI)**, un término compuesto por las iniciales de las palabras inglesas Brittle (quebradizo), Anxious (que genera ansiedad), Non-linear (no lineal) e Incomprehensible (incomprensible). Un entorno político, social y económico que, facilitado y potenciado por el Ciberespacio, Internet 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.

Prerequisitos

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
CG03	Capacidad de organización y planificación en su trabajo como criminólogo	
	RA1	Planifica su trabajo personal de una manera viable y sistemática
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
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
	RA3	Escribe con corrección
	RA4	Presenta documentos estructurados y ordenados
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
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
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, Redes sociales y control social

2. La sociedad red

3. Los conflictos en red

6. Redes sociales en el siglo XXI

7. Impactos individuales y sociales de las redes

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, utopías y distopías

2. Ciberespacio, Internet y Metaverso

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. El panopticón digital

5. Alfabetización mediática y digital

6. 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

• 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

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/grupales	Un ensayo individual y un trabajo grupal en los que se valorará: • Capacidad de aplicar pensamiento crítico • Capacidad de síntesis • Presentación formal • Creatividad • Comunicación escrita y verbal	40

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	Penúltima semana lectiva, con presentación oral en clase
Trabajo individual	Todo el periodo	Último día lectivo

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica
Control social (por orden de importancia)

- José R. Agustina Sanllehi, Irene Montiel Juan, Manuel Gámez Guadix (2020). **Cibercriminología y Victimización Online.** Sintesis.
- Lucas Sztandarowski (2021) **La verdadera cibercriminalidad: Manual jurídico del cibercrímen, ensayo de cibercriminología.** Cyberdéfenseur.
- de Ravi R., Shargunam S., Mallika Pandeeswari R. (2022) **Prevención de la ciberdelincuencia y examen crítico de la ciberley: Prevención de la ciberdelincuencia.** Ediciones Nuestro Conocimiento.
- Alicia Gil Gil, Roberto Hernández Berlinches (2019). **Ciberdelincuencia**. Editorial Dykinson, S.L
- Melossi, Darío (2018). Controlar el delito, controlar la sociedad: Teorías y debates sobre la cuestión criminal, del siglo XVIII al siglo XXI (Nueva Criminología). Polity Press, Cambridge, Reino Unido
- Garland, David (2001). The culture of control. Crime and social order in contemporary society. The University of Chicago Press.
- Beck, Ullrich (2002). La sociedad del riesgo global. Madrid: Siglo XXi de España
- García, Sergio y Ávila Débora (2015). Enclaves de riesgo: Gobierno neoliberal, desigualdad y control social. Traficantes de Sueños.
- Castillo Moro, Manuel (2015). Miedo, control social y política criminal. Tesis doctoral.
- Bauman, Zygmunt (2003). Modernidad líquida. Buenos Aires: Fondo de cultura económica.
- Bauman, Zygmunt (2007). Miedo líquido. La sociedad contemporánea y sus temores. Paidós. Innerarity,
- Daniel (2013). Un mundo de todos y de nadie. Piratas, riesgos y redes en el nuevo desorden global. Paidós.
- Marina, José Antonio (2006). Anatomía del miedo. Un tratado sobre la valentía. Anagrama.

Seguridad y redes

- Castells, Manuel (1999). La era de la información: economía, sociedad y cultura. Madrid: Alianza
- Castells, Manuel (2011). La sociedad red: una visión global. Madrid: Alianza
- Castells, Manuel. Comunicación y poder.
- Arquilla, John y Ronfeldt, David (2002). Redes y guerras en red. El futuro del terrorismo, el crimen organizado y el activismo político. Alianza Editorial

Seguridad y control social en un mundo digital

- VV.AA. (2016). Media and information literacy: reinforcing human rights, countering radicalization and extremism. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000246371
- Morozov, Eugeny (2015). La locura del solucionismo tecnológico. KATZ-CLAVE INTELECTUAL
- Morozov, Eugeny (2012). The net The Net Delusion: How Not to Liberate the World. Penguin Books LTD.
- Stalman, Andy (2016). Humanoffon: ¿Está internet cambiándonos como seres humanos? Deusto
- Lanier, Jaron (2018). Diez razones para borrar tus redes sociales de inmediato. Debate Revista Telos. Fundación Telefónica. https://telos.fundaciontelefonica.com/

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/

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/