esade

GUÍA DOCENTE - 2025-2026

Ciberseguridad

UGRA_011232

Departmentos	Datos, Analytics, Tecnología e Inteligencia Artificial, Departamento de Operaciones, Innovación y Data Sciences, Global Governance
Idiomas impartición	Inglés, Español
ECTS	5
Profesor/a responsable	Mara Eugenia Balestrini - mara.balestrini@esade.edu

Objetivos de la asignatura

Este curso explora las profundas implicaciones globales de la ciberseguridad, la inteligencia artificial (IA) y la infraestructura pública digital (IPD) en el ámbito de la gobernanza global. Desde los ciberataques entre Estados hasta la regulación de la IA generativa y la geopolítica de los datos, los estudiantes descubrirán cómo la tecnología está transformando la soberanía, la diplomacia, los derechos humanos y las dinámicas de poder.

Analizaremos críticamente las dimensiones legales y éticas de los desafíos tecnológicos globales—desde el ransomware y los sesgos algorítmicos hasta las tecnologías de vigilancia, los riesgos a la privacidad y la gobernanza de las identidades digitales. A través de estudios de caso, simulaciones reales y análisis de medios, los estudiantes también examinarán el rol de sistemas de IInfraestructura Púlica Digital (IPD) como Aadhaar (identidad digital) y UPI (sistema de pagos) en la India, la plataforma de gobierno digital de Estonia, PIX en Brasil, y LACNet como plataformas de desarrollo digital e influencia geopolítica.

Diseñado para estudiantes sin formación técnica previa, este curso ofrece alfabetización tecnológica básica junto con un análisis crítico y una perspectiva política global. Los estudiantes examinarán las principales amenazas y respuestas en materia de ciberseguridad desde enfoques legales, políticos e institucionales, y explorarán cómo los gobiernos, las organizaciones internacionales y los actores privados utilizan, regulan y gobiernan el ámbito digital. A través de estudios de caso globales y simulaciones, el curso abordará desafíos como el ciberdelito, la infraestructura pública digital, la soberanía digital y la gobernanza de tecnologías emergentes como la inteligencia artificial y blockchain.

Conocimientos previos

No se requieren conocimientos técnicos previos. Este curso está diseñado específicamente para estudiantes de relaciones internacionales, derecho, ciencias políticas u otras disciplinas sociales que deseen comprender el impacto global de la tecnología sin necesidad de formación en informática, programación o ingeniería.

Se valorará un interés por los temas de gobernanza, derechos humanos,

tecnología y asuntos internacionales, así como una actitud crítica y proactiva para participar en debates, simulaciones y análisis de casos.

Prerrequisitos

Sin prerrequisitos específicos.

Metodología

Este curso combina fundamentos teóricos con un enfoque práctico y experiencial. Las sesiones son interactivas y fomentan el pensamiento crítico mediante debates, simulaciones, ejercicios de rol y análisis de casos reales. Los conceptos clave se presentan a través de clases accesibles, contenido multimedia y lecturas académicas y periodísticas.

Los estudiantes trabajarán de forma individual y en grupos para reflexionar sobre los desafíos de la gobernanza tecnológica global, aplicando enfoques legales, éticos y geopolíticos. Las simulaciones colaborativas—como escenarios de crisis cibernética—permiten una inmersión en la dinámica compleja de actores y en los procesos de toma de decisiones.

La participación activa es esencial en el proceso de aprendizaje, complementada con reflexiones semanales, pruebas breves y un proyecto final en grupo que integra los contenidos del curso con aplicaciones prácticas reales.

Bibliografía

Bruce Schneier, Click Here to Kill Everybody (Libro)
, The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats (Libro)

Sarosh Nagar & David Eaves, Interactions Between Artificial Intelligence and Digital Public Infrastructure: Concepts, Benefits, and Challenges (Artículo)
, Charting the International Governance of the AI–Cyber Nexus, Paris Peace Forum report, 2025 (Artículo electrónico)

Ifeanyi Kingsley Kwentoa, Cybersecurity in Digital Sovereignty: Protecting National Digital Ecosystems against Foreign Cyber Infiltration in the Age of Decentralized Technology (Artículo)

OECD, 2024, Digital Public Infrastructure for Digital Governments (Documento)

Justin Sherman, Finding security in digital public infrastructure (Blog)

Swati Srivastava, Justin Bullock, AI, Global Governance, and Digital Sovereignty (Artículo)

Contenido

#	Módulo
1	Ciberseguridad y Gobernanza Global Introducción a los conceptos fundamentales de la ciberseguridad y su relevancia en el contexto internacional. Se abordarán las principales amenazas digitales (malware, ransomware, phishing, ataques DDoS), los principios del triángulo CIA (confidencialidad, integridad, disponibilidad) y las buenas prácticas de ciberhigiene. Además, se discutirá el rol de la ciberseguridad en la gobernanza global desde perspectivas técnicas, jurídicas y geopolíticas.
2	Ciberseguridad y Política Internacional Este módulo examina cómo la ciberseguridad se entrelaza con la política internacional y los conflictos entre Estados. Se analizarán ciberataques patrocinados por gobiernos, conflictos híbridos, diplomacia cibernética y los

#	Módulo
2	actores clave en la geopolítica digital (EE.UU., China, Rusia, UE, OTAN). También se debatirá la necesidad de normas internacionales para el comportamiento responsable en el ciberespacio.
3	Soberanía Digital y Geopolítica Se analizará el concepto de soberanía digital y cómo los Estados buscan controlar datos, infraestructura y plataformas digitales. Se discutirán estrategias de localización de datos, censura, independencia tecnológica y los modelos de gobernanza de Internet impulsados por diferentes bloques geopolíticos (EE.UU., China, UE, Rusia).
4	Vigilancia, Privacidad y Derechos Digitales Un análisis crítico de la tensión entre vigilancia privada y estatal y protección de los derechos fundamentales. Se estudiarán marcos legales como el GDPR, la legislación sobre derechos humanos y casos emblemáticos como Pegasus, las revelaciones de Snowden, Cambridge Analytica y el Acta de IA de la UE. El objetivo es comprender los desafíos éticos y jurídicos de la sociedad digital.
5	Ciberguerra y Guerra de Información Este módulo aborda las nuevas formas de conflicto en la era digital. Se discutirán los retos de atribución, los ataques a infraestructuras críticas y la difusión de desinformación en contextos electorales o bélicos. Casos como la guerra en Ucrania servirán para analizar la frontera difusa entre guerra y paz en el ciberespacio.
6	Ciberseguridad en la Era de la Inteligencia Artificial Se examinará cómo la IA está transformando tanto las amenazas como las defensas en ciberseguridad. Se discutirán ataques potenciados por IA (deepfakes, malware generativo), el uso de IA para la detección de amenazas, los sesgos algorítmicos y los desafíos de gobernanza de tecnologías de doble uso.
7	Tecnologías Emergentes y Riesgos Cibernéticos Un repaso de las tecnologías emergentes —como IoT, blockchain, computación cuántica— y su impacto en la seguridad digital. Se analizarán también los riesgos éticos y estructurales que plantean y las respuestas regulatorias posibles.
8	Digitalización y Desarrollo Global Exploración del papel de la infraestructura pública digital (IPD) en procesos de desarrollo. Casos como India Stack, Estonia X-Road, PIX en Brasil y LACNet servirán para analizar cómo las tecnologías digitales pueden impulsar (o limitar) la inclusión, la eficiencia y la soberanía digital.
9	Simulación de Crisis Cibernética Global En esta sesión, los estudiantes participarán en una simulación de crisis cibernética global que integrará los aprendizajes del curso. Asumirán el rol de actores clave —gobiernos, organismos internacionales, empresas tecnológicas y sociedad civil— y deberán responder a un incidente crítico que amenaza la infraestructura digital internacional. Durante la simulación, se negociarán respuestas legales, regulatorias y diplomáticas bajo presión, considerando dilemas éticos, conflictos de interés y tensiones geopolíticas. Los estudiantes propondrán políticas, marcos regulatorios o soluciones tecnológicas para desafíos reales de gobernanza digital. Se reservará un espacio para reflexionar colectivamente sobre los conceptos clave del curso y discutir las tendencias emergentes en ciberseguridad, inteligencia artificial y gobernanza global.
10	Tecnología Ciudadana e Innovación Democrática Exploraremos plataformas tecnológicas impulsadas por la ciudadanía para la transparencia, la participación política y la defensa de derechos. Se estudiarán colectivos como Guardian Project, EFF o Civic Tech Labs como ejemplos de innovación democrática desde la sociedad civil.

Evaluación

Herramienta	Sistema de evaluación	Categoría	%
Análisis y discusión de temas en clase	Participación activa	Convocatoria Ordinaria	20.00%
Exámenes escritos y/o orales	Examen - Ensayo	Convocatoria Ordinaria	40.00%
Trabajo en equipo	Presentación grupal final	Convocatoria Ordinaria	40.00%

PROGRAMAS

GDL20-Double Degree in Law and Global Governance, Economics and Legal Order (Undergraduates: Law)
GDL20 Curso 4 (Obligatoria)

GEL19-Grado en Gobernanza Global, Economía y Orden Legal (Undergraduates: Law)
GEL19 Curso 3 (Obligatoria)

GEL23-Bachelor of Global Governance, Economics and Legal Order (Undergraduates: Law)
GEL23 Curso 3 (Obligatoria)