Modalidad **VIRTUAL**

Derecho y Ciencias Políticas
UAI

DIPLOMATURA EN

Ciberdiplomacia y Seguridad Internacional del Ciberespacio

+54 9 11 21823616

Duración:

163 hs. (93 hs. de clases + 70 hs. de trabajos)

Días y horarios:

Del 23 de abril al 17 de diciembre. Jueves de 17:30 a 20:30 hs. (Examen: 10 de diciembre. Última fecha de entrega: 17 de diciembre)

Calendario

Abril	23	30			
Mayo	7	14	21	28	
Junio	4	11	18	25	
Julio	2	23	30		
Agosto	6	13	20	27	
Septiembre	3	10	17	24	
Octubre	1	8	15	22	29
Noviembre	5	12	19	26	
Diciembre	3	10	17		

Modalidad:

Virtual sincrónica (Zoom)

Aranceles (*):

(50 % de Bonificación sobre la matrícula por inscripción antes del 15/03/2026)

Matrícula: $100000.

Externos: Contado $864000 ó 9 cuotas de $120000.

Comunidad UAI: Contado $604000 o 9 cuotas de $84000.

Extranjeros no residentes en Argentina (**):
Matrícula: USD 70.
Arancel: Contado USD 600 o 9 cuotas de USD 80.

(*) En caso de elegir la opción de pago al contado, deberá avisarnos al momento de abonar la matrícula, o dentro del primer mes de cursado a uai.extensionrosario@uai.edu.ar ó al WhatsApp: +54 9 11 2182-3616. Transcurrido ese período la opción ya no será válida y deberá pagar obligatoriamente las cuotas mensuales según el valor establecido en cada capacitación

(**) Los aranceles de la actividad comprenden únicamente los conceptos de matrícula y cuota. Todo impuesto, tasa o contribución asociada a los pagos en dólares estadounidenses que pudiera ser aplicada por el país de origen, así como cualquier otra suma que se adicione en virtud de las tarifas vigentes en la entidad bancaria al momento de realizar la transacción, queda a exclusivo cargo del alumno.

Dirigido a:

- Estudiantes y egresados de carreras afines a Relaciones Internacionales y Ciencias Políticas
- Analistas e Investigadores relacionados a Ciberseguridad, Ciberdefensa y/o Inteligencia de Amenazas
- Profesionales y equipos que participen en gobernanza digital y en la administración multinivel de Internet (sector público, sector privado, academia y sociedad civil).
- Funcionarios/as y asesores/as en áreas de política exterior, defensa y seguridad, vinculados al diseño de políticas públicas y estrategias nacionales en materia de ciberseguridad/ciberdefensa.
- Perfiles con interés en negociación internacional, orientados a la participación en foros multilaterales cibernéticos y mecanismos de cooperación (ej., ámbitos multilaterales y regionales).
- Investigadores/as y operadores/as que trabajen sobre conflictos híbridos, desinformación y atribución de ciberataques, en entornos de análisis político-estratégico.

Objetivos:

Se espera que los/las participantes logren comprender el ciberespacio como dominio estratégico de la conflictividad internacional y su impacto en la seguridad internacional y la

política exterior. Que los destinatarios puedan desarrollar un enfoque integral que articule dimensiones técnicas, Luncos legales internacionales, dinámicas geopolíticas y herramientas de análisis estratégico, al igual que adquirir capacidades para la gobernanza digital y la práctica de ciber negociaciones internacionales, logrando analizar conflictos híbridos, desinformación y atribución política de ciberataques, lograr diseñar lineamientos de estrategia nacional de ciberseguridad, incluyendo protección de infraestructuras críticas y gestión de crisis; y aplicar estos aprendizajes en instancias prácticas de simulación, toma de decisiones bajo presión y producción de entregables profesionales. El grupo de disertantes está integrado por docente de amplia expertis en la rama y por alumnos a punto de recibirse en la facultad de derecho de la UIA, que integran el equipo de investigación sobre derecho del trabajo que coordina el Dr. de primer nivel, especialistas y profesores universitarios de reconocida trayectoria.

Enfoque general:

La actividad está orientada a comprender el ciberespacio como un dominio estratégico de la conflictividad internacional y a abordar la brecha de formación que existe entre lo técnico, lo legal, lo diplomático y lo geopolítico. Su propósito general es desarrollar capacidades para el análisis y la toma de decisiones en seguridad internacional aplicada al entorno digital, formando perfiles capaces de asesorar en gobernanza digital, investigar ciberdelitos y amenazas con encuadre jurídico internacional y participar en negociaciones multilaterales. La propuesta integra contenidos que van desde geopolítica, derecho internacional y ciberdiplomacia hasta conflictos híbridos y diseño de estrategias nacionales, culminando en instancias prácticas de simulación de crisis y negociación.

Contenidos:

Módulo I – Geopolítica del Ciberespacio, Infraestructura y Poder: ciberespacio como “quinto dominio”; geopolítica de la infraestructura (cables subLuninos, rutas de datos, IXP, 5G y

semiconductores); “balcanización”/splinternet; actores del sistema internacional digital (Estados, proxies, crimen organizado transnacional, hacktivismo y Big Tech) .

Módulo II – Derecho Internacional Público y Luncos Normativos Globales: aplicabilidad del Derecho Internacional y DIH; soberanía y no intervención en ciberoperaciones; debida diligencia estatal; tratados sobre cibercrimen (Budapest vs. nueva convención ONU); control de exportación de ciberarmas.

Módulo III – Ciberdiplomacia y Gobernanza de Internet: modelo multistakeholder y ecosistema de gobernanza (ICANN, IETF, ISOC, UIT); práctica de la ciberdiplomacia; “techplomacia”; cooperación internacional y medidas de fomento de la confianza (CBMs) y rol de organismos regionales.

Módulo IV – Conflictos Híbridos, Desinformación y Guerra Cognitiva: zona gris y guerra híbrida; operaciones de influencia y desinformación; atribución pública y negación plausible; ciberinteligencia estratégica; inteligencia de amenazas (CYBINT y OSINT).

Módulo V – Estrategia Nacional de Ciberseguridad, Políticas Públicas y Soberanía Nacional: diseño de estrategias nacionales (ENCS) y modelos comparados; protección de infraestructuras críticas; gestión de crisis a nivel nacional y comunicación política; responsabilidad penal individual y Estatuto de Roma.

Módulo VI – Economía Digital y Problemáticas Emergentes: geopolítica de criptomonedas y sanciones; IA y biometría y su regulación; armas autónomas letales (LAWS) y privacidad; ataques a la cadena de suministro.

Módulo VII – Taller de Simulación de Crisis: simulación de negociación internacional (OEWG ONU / OEA); war gaming político ante ciberataque a infraestructura crítica; elaboración del trabajo final integrador (policy brief / nota diplomática / propuesta de estrategia nacional).

Para acreditar la actividad se prevé una instancia de evaluación integradora, consistente en la presentación de un Trabajo Final Integrador

Directores:

FABIAN LAVALLEN RANEA - Docente y Director de las carreras de Ciencia Política y Relaciones Internacionales de la UAI, Doctor en Ciencia Política, Licenciado en Historia y en Relaciones Internacionales.

TOMÁS ILLUMINATI BALBIN - Analista de Ciberseguridad, Analista de Inteligencia de Amenazas. MSc in Cyber Security Candidate at The Open University (UK). Ciberseguridad, Ciberdefensa, Relaciones Internacionales, Inteligencia de Amenazas.

Dictantes:

ELOISA MENDER BINI - Doctora en Ciencias Jurídicas, Universidad Católica Argentina (UCA). Especialista en Sistemas Biométricos, Privacidad y Protección de Datos Personales (FernUni, Suiza). Sistemas Biométricos, Privacidad y Protección de Datos Personales.

OSCAR NISS - Licenciado en Administración Pública. Maestrando en Derecho Internacional. Ex Subsecretario de Ciberdefensa de Argentina. Ciberdefensa, Soberanía y Seguridad en el Ciberespacio

DANIEL SASIA - Ex CIO y CISO en Instituto de Ayuda Financiera (IAF), MBA en Dirección de Sistemas de Información. Transformación Digital Segura, Gobierno De Ti, Gestión De Riesgos, Cumplimiento Normativo Y Protección De Datos

DANIEL FEIPELER - Analista Programador Universitario. Docente Universitario. Ciberseguridad, Ciberdefensa y Seguridad de la Información

CARLOS E. SÁNCHEZ TORRES (MEXICO) - Licenciado en Ciencias de la Computación (UABC). Inteligencia Artificial, Ingeniería de Software y Ciencia de Datos

FACUNDO NAHUEL BRITOS - Licenciado en Relaciones Internacionales (UAI). Conflictos Militares Híbridos y Guerras Modernas.

LUNIANO DARÍO ROLDAN - Abogado, Mediador. Docente Universitario (UAI). Diplomado en Políticas Públicas y en Asesoría Política. Métodos Alternativos de Resolución de Conflictos.

IVAN ALEXANDER GAWEK - Ex oficial de inteligencia del Ejército Argentino y actual científico de datos, especializado en protección de Luncas y previsión de riesgos cibernéticos en JPMorgan. Protección de Luncas y previsión de riesgos en sector privado.

MATÍAS COSSO - Oficial de Estado Mayor Naval y Conjunto del Cuerpo de Comando de la Armada Argentina, egresado de la Escuela Naval Militar (Promoción CXXXVI). Conflictos Híbridos y Sistemas Complejos

Contacto:

uai.extensionrosario@uai.edu.ar

Envianos un mensaje en WhatsApp: +54 9 11 21823616