

Modalidad **VIRTUAL**



DIPLOMATURA UNIVERSITARIA EN

Cibercrimen

**"Prevención, investigación y análisis de
delitos en entornos digitales"**



+54 9 11 21823616

Duración:

100 hs. (72 hs. sincrónicas y 28 hs. asincrónicas)

Días y horarios (*):

Del 8 de abril al 23 de septiembre (**)

Martes de 19:00 a 22:00 hs.

* Encuentros optativos de supervisión y/o práctica (sábado de 10 a 12 hs.).

- Nota: Si bien se intentará mantener las fechas de los encuentros virtuales en directo obligatorios y optativos, las mismas pueden variar hacia el segundo cuatrimestre según circunstancias externas.

** Evaluación final integrativa: al finalizar la cursada.

Calendario:

| | | | | | |
|-------------------|---|----|----|----|----|
| Abril | 8 | 15 | 22 | 29 | |
| Mayo | 6 | 13 | 20 | 27 | |
| Junio | 3 | 10 | 17 | 24 | |
| Julio | 1 | 8 | 15 | 22 | 29 |
| Agosto | 5 | 12 | 19 | 26 | |
| Septiembre | 2 | 9 | 16 | 23 | |

Modalidad:

Virtual.

- La modalidad es online, vía ZOOM, en forma sincrónica.
- Las clases quedan grabadas para que puedan verla quienes no han podido asistir a los encuentros.
- Para obtener el certificado de la diplomatura, se requiere aprobar el examen final y cumplir con el 60% de la asistencia online.

Aranceles (*):

Matrícula: \$20000.

Externos: Contado \$240000 ó 6 cuotas de \$50000.

Comunidad UAI y miembros del Círculo Argentino de Seguridad: Contado \$200000 ó 6 cuotas de \$45000.

Extranjeros no residentes en Argentina (**):

Matrícula: USD 20.

Arancel: Contado USD 400 ó 6 cuotas de USD 70.

Arancel Alternativo en Pesos: Contado \$400000 ó 6 cuotas de \$80000

(*) 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 esta 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:

Miembros de fuerzas armadas o de seguridad. Miembros de empresas privadas. Analistas que ejerzan cargos de asesoramiento en fuerzas armadas, de seguridad y empresas privadas. Profesionales de las distintas áreas estatales o privadas que se desempeñen o pretendan desarrollar la actividad de analistas o asesores.

Objetivos:

Objetivo General:

- Formar profesionales capacitados para prevenir, investigar y analizar delitos en el ámbito digital, integrando conocimientos técnicos, legales y éticos para garantizar una respuesta efectiva ante el cibercrimen.

Objetivos Específicos:

1. Comprender las características y dinámicas del cibercrimen en el contexto actual.
2. Desarrollar habilidades técnicas para investigar y analizar delitos digitales.
3. Aplicar normativas legales nacionales e internacionales en la gestión de casos de cibercrimen.
4. Promover prácticas éticas en la prevención y resolución de delitos cibernéticos.
5. Diseñar estrategias de ciberseguridad para la protección de sistemas y datos sensibles.

Enfoque general:

Esta Diplomatura Universitaria en Cibercrimen ofrece una formación integral y práctica, orientada a dotar a los participantes de herramientas técnicas, legales y analíticas para abordar el fenómeno delictivo en el entorno digital. Con un enfoque interdisciplinario, este programa prepara a los profesionales para enfrentar los desafíos del ciberespacio, respetando principios éticos y promoviendo la seguridad digital.

Contenidos:

MÓDULO I: Fundamentos del Cibercrimen y el Uso Responsable de Internet

- Evolución de Internet: De la Web 2.0 a la Web 3.0.
- Conceptos de Ciberdelitos: Cyberbullying, Grooming, Sexting, Sextorsión, Sharenting, Tecnoadicciones, Retos Virales.
- Legislación Vigente: Delitos informáticos en Argentina, regulación internacional y normas específicas como la Ley 26.904 (Grooming).

MÓDULO II: Ciberinteligencia y OSINT (Open Source Intelligence)

- Introducción a la Ciberinteligencia: OSINT, HUMINT, CYBINT, SOCMINT.
- Ciclo de inteligencia: Credibilidad vs. Fiabilidad, herramientas como Maltego y OSRFramework.
- Deep & Dark Web: Uso de Tor, I2P, Freenet; anonimato digital y herramientas de búsqueda avanzada.

MÓDULO III: Seguridad de la Información y Protección de Datos

- Bases de la Seguridad Informática: Vulnerabilidades, amenazas físicas y lógicas, políticas de seguridad.
- Ciberinfraestructura Crítica: Riesgos, actores de ciberataques y normativas argentinas.
- Privacidad y Protección de Datos: Ley 25.326 de Protección de Datos Personales y casos internacionales.

MÓDULO IV: Peritaje Informático y Evidencia Digital

- Obtención y análisis de evidencias digitales: Introducción a la informática forense.
- Software y Hardware Forense: Autopsy, Magnet, Tableau, UFED; recuperación de datos en dispositivos móviles.
- Evidencia Digital: Procesamiento, gestión y errores comunes en la preservación.

MÓDULO V: Delitos Informáticos y Crimen Organizado Digital

- Crimen Organizado Digital: Lavado de dinero, financiamiento del terrorismo y delitos financieros.
- Delitos en Redes Sociales: Phishing, Pharming, Fake News, Robo de Identidad.
- Ciberterrorismo y Ciberguerra: Formas de ataque, actores relevantes y ejemplos históricos.

MÓDULO VI: Blockchain, Criptomonedas y Criptoactivos

- Introducción al Blockchain: Características, tipos y aplicaciones.
- Criptomonedas: Bitcoin, Ethereum, Altcoins y estafas comunes (ransomware, esquemas piramidales).
- Marco legal y riesgos asociados: Estafas, delitos financieros y protección del usuario.

MÓDULO VII: Robótica, Drones y Ciberseguridad

- Introducción a la Robótica: Sistemas autónomos y su relación con la ciberseguridad.
- Vehículos aéreos no tripulados: Clasificación, legislación argentina (ANAC N°880-E/19) y amenazas como GPS Spoofing y SkyJack.
- Manejo Forense de Imágenes y Videos obtenidos con Drones.

MÓDULO VIII: Big Data y su Impacto en la Seguridad

- Introducción al Big Data: Tipos de datos, tecnologías para análisis y las '7V'.
- Usos en Seguridad: Aplicaciones en turismo, salud, telecomunicaciones y gobernanza.
- Mal Uso del Big Data: Caso Cambridge Analytica y dilemas éticos.

MÓDULO IX: Inteligencia Artificial y Malware (6 horas)

- Historia y Evolución de la IA: Tipos de procesamiento y aplicaciones en ciberseguridad.
- Malware: Virus, Troyanos, Ransomware y Spyware; técnicas de ataque como DDoS y spoofing.

MÓDULO X: Ciber Delitos Avanzados y Legislación Internacional (6 horas)

- Pornografía Infantil y Grooming: Definición, simbología y legislación nacional e internacional.
- Normativa Internacional: Convención de Budapest sobre Ciberdelincuencia.
- Legislación Argentina: Leyes clave como 26.388 (delitos informáticos), 26.653 (accesibilidad web) y normas provinciales.

Evaluación:

Evaluación final integrativa.

Beneficios:

1. Formación Especializada: Obtendrás competencias avanzadas en la investigación de delitos digitales.
2. Enfoque Integral: Abordarás el cibercrimen desde una perspectiva técnica, legal y ética.
3. Certificación Universitaria: Diploma avalado por una institución reconocida.
4. Networking Profesional: Conexión con especialistas y colegas en cibercrimen y ciberseguridad.
5. Preparación para el Futuro: Capacitación en un área de alta demanda y constante crecimiento.

Cuerpo docente:

NELSON DARIO NOVAL

Director Académico de la Diplomatura Superior Internacional en Cibercrimen - UAI
Director Nacional de Cibercrimen del Círculo Argentino de Seguridad
Director Académico del Programa "ALERTAS NIÑOS"
Director Académico de la Red Internacional de Seguridad
Prof. Titular en Nivel Terciario Prov. Bs. As.

Contacto:



uai.extensionrosariouai.edu.ar



Envíanos un mensaje en WhatsApp: +54 9 11 21823616