Modalidad **VIRTUAL**

DIPLOMATURA EN

Delitos Informáticos y análisis del rastro forense digital

Derecho y Ciencias Políticas

+54 9 11 2660 3030 / +54 9 11 5594 9903

Duración: 120 horas.

Días y horarios:

Del 05 de junio al 18 de diciembre de 2024.
Miércoles de 18:00 a 21:00 Hs.

Modalidad y localización: Virtual.

Aranceles:

Externos:
Matrícula: $ 50.000.-
Contado: $504.000.- u 8 cuotas de $75.000.-

Comunidad UAI:
Matrícula: $ 50.000.-
Contado: $352.000.- u 8 cuotas de $52.800.-

Operadores de justicia, agentes de la administración pública:
Matrícula: $ 50.000.-
Contado: $403.200.- u 8 cuotas de $60.500.-

Extranjeros no residentes en Argentina*:
Matrícula: USD 60.-
Contado: USD 600.- u 8 cuotas de USD 100.-

(*) 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.

Reglamento interno

Artículo 35: Modificación de los aranceles: La Universidad se reserva el derecho de modificar los aranceles de acuerdo a los incrementos que se produzcan en su estructura de costos y/o nuevos impuestos o contribuciones que pudieran afectar a la actividad con los límites que, en su caso, pudieran fijar las autoridades nacionales. Los aranceles especiales y gastos administrativos que fueran expresados en el presente Reglamento en valores constantes en pesos, sufrirán idéntico ajuste al que se determine para los aranceles de las carreras respectivas.

Dirigido a:

La informática forense y la comprensión de los delitos informáticos son esenciales para los estudiantes y profesionales involucrados en disciplinas relacionadas con las ciencias sociales y jurídicas. Abogados, antropólogos, educadores, trabajadores sociales, politólogos, sociólogos, agentes de seguridad, operadores de justicia, funcionarios públicos y cualquier persona interesada en la temática se encuentran inmersos en un entorno donde la delincuencia digital plantea desafíos constantes.

Objetivos:

• Comprensión Integral de los Delitos Informáticos: Explorar los principios conceptuales esenciales para entender la naturaleza y dinámica de los delitos informáticos desde una perspectiva interdisciplinaria.
• Evolución de las Teorías Criminológicas en el Contexto Digital: Analizar la historia y el desarrollo de las teorías criminológicas actuales, aplicadas específicamente al ámbito de los delitos informáticos y el cibercrimen.
• Importancia de la Criminología en la Prevención Cibernética Empresarial: Reconocer la relevancia de la criminología en entornos empresariales para prevenir y abordar los delitos informáticos, enfocándose en estrategias y tácticas específicas.
• Estrategias Internacionales de Prevención de Cibercrimen: Caracterizar y adaptar estrategias y tácticas de prevención de cibercrimen implementadas a nivel internacional, centrándose en su aplicabilidad en distintos contextos digitales.
• Examen Crítico de las respuestas a Nivel Institucional: Reflexionar críticamente sobre las respuestas institucionales al cibercrimen, incluyendo un análisis desde perspectivas de género y consideraciones específicas de la criminología digital.
• Abordaje Psicológico y Comportamental del Cibercrimen: Analizar en profundidad la psicología y el análisis conductual asociados con el cibercrimen, su relevancia en investigaciones y análisis periciales en entornos digitales.
• Perspectivas Emergentes en Cibercriminología: Explorar nuevos enfoques y tendencias en el estudio del cibercrimen, incluyendo la implementación de perspectivas de género y corrientes innovadoras para comprender y prevenir los delitos informáticos en la actualidad.

Enfoque general:

La informática forense y la investigación de delitos informáticos son elementos cruciales en el ámbito de la seguridad digital y la prevención de actividades delictivas en entornos tecnológicos. Estos campos son esenciales para comprender y abordar los desafíos emergentes en la era digital, donde la criminalidad adopta nuevas formas y se manifiesta de manera inesperada. A medida que la sociedad experimenta avances tecnológicos, los delitos informáticos evolucionan, presentando facetas cada vez más complejas y sofisticadas. Frecuentemente, la respuesta de las políticas de seguridad y prevención de delitos se ve rebasada por la rapidez de estos cambios. Es crucial replantear los enfoques tradicionales y explorar nuevas estrategias para entender, prevenir y enfrentar estos fenómenos delictivos.

Contenidos:

1. Ley de Delitos Informáticos en Argentina.
2. Estudio detallado de la legislación vigente en materia de delitos informáticos en Argentina, analizando su alcance, aplicabilidad y casos relevantes.
3. Convenio de Budapest y su Impacto en la Legislación sobre Delitos Informáticos.
4. Análisis del Convenio de Budapest sobre ciberdelincuencia y su influencia en la legislación internacional sobre delitos informáticos, así como su aplicación en contextos nacionales.

5. Desafíos de la Ciberseguridad en la Prevención de Delitos Informáticos.
6. Evaluación de los retos y estrategias en ciberseguridad para prevenir y enfrentar los delitos informáticos en entornos tecnológicos.
7. Legislación y Delitos Informáticos.
8. Estudio detallado de la legislación actual en delitos informáticos y su aplicación en la investigación y enjuiciamiento.
9. Pericias Informáticas en casos sensibles.
10. Importancia de las pericias informáticas en la investigación de casos delicados como la pornografía infantil y el grooming en el ciberespacio.
11. Investigación Criminal y Ciberespacio.
12. Métodos específicos para llevar a cabo investigaciones criminales en el ámbito digital y en cibercrimen.
13. Criminología Empresarial y Ciberdelincuencia Corporativa.
14. Enfoque de la criminología aplicada a entornos corporativos, destacando riesgos y medidas de prevención en el ámbito empresarial.
15. Estadísticas Criminales y Medios Digitales.
16. Análisis de la estadística criminal y su relación con la percepción pública de la delincuencia digital en medios de comunicación.
17. Control Social y Policía en el Ciberespacio.
18. Relación entre el control social, las fuerzas policiales y la ciberdelincuencia, con énfasis en América Latina.
19. Enfoque de Género y Ciberdelitos.
20. Estudio del género en la criminología digital, con análisis de casos específicos relacionados con delitos informáticos.
21. Abordaje de la delincuencia juvenil y estrategias de protección adaptadas al entorno digital.
22. Evaluación del riesgo de comportamiento delictivo en el ciberespacio y detección de delitos informáticos.
23. Metodologías de Investigación en Cibercrimen.
24. Proyecto Final: Investigación en Delitos Informáticos y Cibercrimen.

Calenario de encuentros:

Clase 1: Tema: ***Ley de Delitos Informáticos en Argentina.***
Clase 2: Tema: ***Estudio detallado de la legislación vigente en materia de delitos informáticos en Argentina, analizando su alcance, aplicabilidad y casos relevantes.***
Clase 3: Tema: ***Convenio de Budapest y su Impacto en la Legislación sobre Delitos Informáticos.***
Clase 4: Tema: ***Desafíos de la Ciberseguridad en la Prevención de Delitos Informáticos.***
Clase 5: Tema: ***Evaluación de los retos y estrategias en ciberseguridad para prevenir y enfrentar los delitos informáticos en entornos tecnológicos.***
Clase 6: Tema: ***Estudio detallado de la legislación actual en delitos informáticos y su aplicación en la investigación y enjuiciamiento.***

Clase 7: Tema: *Pericias Informáticas en Casos Sensibles.*
Clase 8: Tema: *Importancia de las pericias informáticas en la investigación de casos delicados como Material de Abuso Sexual Infantil (M.A.S.I),y grooming en el ciberespacio.*
Clase 9: Tema: *Investigación Criminal y Ciberespacio.*
Clase 10: Tema: *Métodos específicos para llevar a cabo investigaciones criminales en el ámbito digital y en cibercrimen.*
Clase 11: Tema: *Ciberdelincuencia Corporativa.*
Clase 12: . **Tema:** *Phishing aplicado en el ámbito empresarial.*
Clase 13: Tema: *Estadísticas Criminales y Medios Digitales.*
Clase 14:
Clase 15: Tema: *Control Social y Policía en el Ciberespacio.*
Clase 16: Tema: *Enfoque de Género en Ciberdelitos.*
Clase 17: Tema: *Abordaje estrategias de protección adaptadas al entorno digital.*
Clase 18: Tema: *Evaluación del riesgo de comportamiento delictivo en el ciberespacio y detección de delitos informáticos.*
Clase 19: Tema: *Metodologías de Investigación en Cibercrimen.*
Clase 20: Tema: *Cadena de custodia, protocolos de actuación. Sistema PURI. Protocolo Provincia de Buenos Aires. Protocolos. RES 234/16.*
Clase 21: Tema: *Hurto, fraude y daño informático.*
Clase 22: Tema: *Delitos informáticos en el ámbito financiero y económico.*
Clase 23: . **Tema:** *Ciberacoso (Grooming).*
Clase 24: Tema: *La prueba pericial, técnicas OSINT.*
Clase 25: Tema: *Dep Weeb y Dark Web.*
Clase 26: . **Tema:** *Delitos informáticos. Espionaje.*
Clase 27: 13/11/2024 de 18:00 a 21:00 Hs. **Tema:** *El uso de la IA en el tratamiento de los datos y la big data.*
Clase 28: Tema: *El uso de las TIC`s. Las redes sociales.*
Clase 29: Tema: *Acceso no autorizado a servicios y sistemas informáticos.*
Clase 30: . **Tema:** *Malware, virus, gusanos, troyanos, hijackers, keyloggers, hoax, jokes, spyware, adware, phishing, zombies.*
Clase 31: Tema: *Criptomonedas y su uso en los delitos informáticos. Blockchain.*
Clase 32: . **Tema:** *Proyecto Final: Investigación en Delitos Informáticos y Cibercrimen.*

Directores:

Mg. Carlos Avendaño. Docente UAI. Maestría en Ciencias. **Área de especialidad:** Criminología.

Esp. Rubén Marcelo Romero. Técnico en Seguridad Pública. **Área de especialidad:** Informática Forense. *Es técnico en seguridad pública, técnico en seguridad industrial, estudiante avanzado de derecho, Perito informático, diplomado en Criminalística; Diplomado en informática forense, miembro ad honorem en IRAM para la traducción de las ISO sobre informática Forense, experto en informática forense por distintas universidades, experto en Osint en distintas universidades, autor y coautor de varios libros sobre la temática del cibercrimen, director de la asociación argentina de lucha contra el cibercrimen.*

Docentes invitados: (por órden alfabético)

- **Mg. Carlos Avendaño.** Maestría en Ciencias. **Área de especialidad:** Criminología.
- **Esp. Romero Rubén Marcelo.** Diplomado en Criminología, Criminalística, Perito Informático, Esp. en Osint. **Área de especialidad:**Informática Forense.
- **Esp. Carlos Lujan Maldonado Ramírez.** Auditor de Seguridad en Sistema de Redes. **Área de especialidad:** Cibercrimen, Redes, secuestro de Evidencia Digital.
- **Esp. Cintia Anahí Bustos.** Analista en Sistemas. **Área de especialidad:** Delitos Informáticos, Programación.
- **Abg. Javier Bura Peralta.** Abogado especialista en Cibercrimen. **Área de especialidad:** Informática Forense, Perito Informático de la Fiscalía de CABA.
- **Esp. Giovanna Litza Avalos Apaza.** Técnica en Criminalística C/ Esp. en Laboratorio Químico, Esp. Cibercrimen. **Área de especialidad:** Técnica en Criminalista Esp. Cibercrimen Esp. Evidencia digital.
- **Lic. Javier Ezequiel Come.** Lic. Redes y Sistemas. **Área de especialidad:** Informática Forense, Perito Informático de la Fiscalía de CABA.
- **Abg. Nicole Lisette Dwek. Abogada. Área de especialidad:** Informática Forense, Investigadora Informático de la Fiscalía de CABA.

Contacto:

uai.extension@uai.edu.ar

E-MAIL

Envianos un mensaje en WhatsApp:

+ 54 9 11 5594 9903

+ 54 9 11 2660 3030