



UNIVERSIDAD NACIONAL
RAÚL SCALABRINI ORTIZ
SAN ISIDRO



ÁREA DE POSGRADO

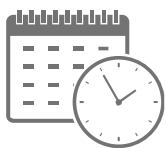
DIPLOMATURA LITIGACIÓN DE CIBERDELITOS Y EVIDENCIA DIGITAL

CONTACTO DIPLOMATURAS:
dip.juridicas@unsanisidro.edu.ar



OBJETIVOS

1. Proveer conocimientos técnico-jurídicos sobre litigación de ciberdelitos y evidencia digital, comprendiendo su marco legal y aplicación práctica en casos concretos.
2. Estudiar medios de obtención y uso de evidencia digital en el proceso penal, analizando técnicas para su recolección, preservación y admisibilidad judicial.
3. Adquirir técnicas de investigación en entornos digitales, capacitando en metodologías para rastrear actividades ilícitas e identificar responsables en plataformas tecnológicas.
4. Capacitar en técnicas de litigación y uso eficiente de pruebas digitales, desarrollando habilidades para la defensa de casos y manejo de información.
5. Analizar la intersección entre inteligencia artificial y derecho penal, explorando su uso en delitos y las implicaciones éticas y legales derivadas.
6. Fomentar la comprensión de legislación nacional e internacional sobre cibercrimen, estudiando el Convenio de Budapest para operar en casos de componentes transnacionales.
7. Promover el respeto a los derechos fundamentales en el ciberespacio, concientizando sobre la privacidad y su equilibrio con la persecución penal efectiva.
8. Desarrollar competencias en el manejo de criptoactivos en investigaciones penales, ofreciendo formación sobre su naturaleza, funcionamiento, rastreo e incautación judicial.
9. Facilitar la aplicación práctica mediante talleres y casos reales, fortaleciendo la capacidad para enfrentar desafíos en cibercrimen e inteligencia artificial generativa.



DETALLES ADMINISTRATIVOS

FECHA DE INICIO: 6 DE MAYO

FECHA DE FIN: 16 DE SEPTIEMBRE

DIAS Y HORARIOS: miércoles de 17 a 19:30 hs

MODALIDAD: virtual

REQUISITO DE INGRESO: Egresados de la carrera de Derecho y afines.

CARGA HORARIA TOTAL: 45HS sincrónicas + 10HS asincrónicas

CERTIFICACIÓN OTORGADA: de aprobación con resolución rectoral.



DIRECCIÓN

- **Dr. Rubén Chaia (Director)**

Vocal del Tribunal de Juicios y Apelaciones de Concepción del Uruguay. Abogado (UBA). Magíster en Derecho y Magistratura Judicial (Austral). Especialista en Derecho Penal (Austral). Profesor Universitario de Grado y Posgrado. Ha publicado gran cantidad de libros, artículos en revistas especializadas y disertado en numerosos certámenes jurídicos.

- **Dr. Sebastián D. Luján (Coordinador)**

Abogado especializado en Derecho Penal (UBA) con un enfoque particular en ciberdelitos, ciberseguridad e inteligencia artificial. Diplomado Internacional en Ciberdelitos y Evidencia Digital por la Universidad Austral y Universidad Abat Oliba (Barcelona). Secretario en el Juzgado de Garantías n.º 4 de San Isidro. Premio Poder Judicial en el eje gestión judicial. Profesor universitario en Derecho Procesal Penal y docente en programas de capacitación nacional sobre ciberseguridad y ciberdelitos en UNSAM. Investigador en OCEDIC (Universidad Austral) y expositor en temas de derecho y tecnología.

- **Nómina docente:**

Rubén Chaia, Nicolás Ceballos, Sebastián Luján, Lucas Moyano, Mariana Maldonado, Alejandro Musso, Alejandro Orlandini, Denis Banchemo, Williams Alfaro, Daniela Dupuy, Mario Adaro, Jonathan Polansky, Carlos Sueiro y Diego Lugo.



PROGRAMA

Presentación e Introducción al curso.

1. Descripción de cada bloque temático de la diplomatura.
2. Introducción a la litigación en entornos digitales.
3. Características de la evidencia digital. Complejidad del abordaje. Normas procesales. Principios que guían al proceso penal. Omisión de regulación de la prueba digital. Avances y retrocesos. ¿Reglas de evidencia digital?
4. Libertad probatoria. Injerencias. Privacidad e intimidad. Ausencia de reglas para la investigación y litigación. Uso de protocolos. Omisión. Cadena de Custodia. Planteos de Nulidad.
5. Análisis de fallos y casos prácticos.

DOCENTES: Dres. Rubén Chaia, Nicolás Ceballos y Dr. Sebastián Luján

Prueba Ilegal. Desbloqueo forzoso. ¿Autoincriminación forzada? ¿La víctima como insumo digital del proceso penal? Límites al uso del material secuestrado.

1. Características y complejidad en la Investigación y Litigación en delitos “tradicionales” y los llamados “ciberdelitos”.
2. Problemas en la Admisión de pruebas.
3. Prueba Ilegal Digital.
4. Prueba digital obtenida por particulares y agentes públicos. ¿Admisibilidad? Tratamiento en punto a las exclusiones probatorias.
5. Desbloqueo forzoso de celular. Uso de datos biométricos. ¿Es posible utilizar la fuerza? Variantes en función de las medidas que se intentan emplear.
6. Uso de nuevas tecnologías en el marco de delitos “tradicionales”. Problemas probatorios que acarrea en casos de amenazas, coacciones, abusos sexuales, homicidios, femicidios.
7. La víctima, su trato en la investigación en entornos digitales. ¿Existen límites a la investigación sobre la víctima?
8. Material digital secuestrado. Uso, destrucción, ¿acceso de las partes? Posible viralización, privacidad, intimidad, derecho a la imagen. Terceros involucrados.
9. Análisis de fallos y casos.

DOCENTE: Dr. Rubén Chaia

Evidencia digital y garantías constitucionales.

1. Legislación nacional e internacional aplicable (Convenio de Budapest, leyes locales).
2. Competencia territorial y material en la práctica cotidiana (casos con múltiples jurisdicciones).
3. Análisis de los tipos penales. Complejidad de encuadre. Grooming. MASI. Violación de correspondencia electrónica. Acceso ilegítimo. Publicaciones abusivas. Estafa.
4. Extracción de evidencia digital en dispositivos móviles y redes sociales. Problemas prácticos.
5. Requerimientos a plataformas y proveedores de Internet. Modelos. Usos.
6. Puesta en común de casos simulados y reales sobre estafas digitales
7. Análisis de fallos y casos.

DOCENTE: Dr. Lucas Moyano



PROGRAMA

Investigación en entornos digitales.

1. Borrado de datos del dispositivo. Omisión de aportar la clave de acceso al celular u ordenador. Ausencia de colaboración. ¿Presunción de culpabilidad del sospechado? Supuestos especiales: funcionario público, material provisto por el estado, ¿cuentas públicas o privadas?, reglas éticas.
2. Tratamiento de la admisión y exclusión de comunicaciones por WhatsApp, Instagram, Facebook y demás plataformas.
3. Las comunicaciones por WhatsApp: mensajes en grupos, aspectos probatorios, ¿secretos entre comunicantes?, límites.
4. Observación en el interior de la vivienda mediante dispositivos tecnológicos y a “simple vista”. Investigación de delitos con auxilio de tecnología v. privacidad. Uso de drones.
5. Fotos, videos, publicaciones, su impacto en la prueba de los hechos. Admisión y exclusión. Preparación del caso en orden a prueba.
6. Prueba digital inflamatoria, perturbadora, sobreabundante. Litigación. Juicios por Jurados y jueces técnicos. Posibilidades de objetar.
7. Análisis de casos y fallos.

DOCENTE: Dr. Rubén Chaia

Evidencia Digital. Secuestro. Prueba ilegal. Análisis comparado Código Procesal Federal y códigos procesales provinciales.

1. Regulación de la prueba digital en el Código Procesal Federal.
2. Regulación en los códigos provinciales.
3. Nulidad y exclusión de prueba material y digital, supuestos.
4. Utilización de nuevas tecnologías. Investigaciones especiales.
5. Ciberpatrullaje.
6. Agente delator, provocador y encubierto digital.
7. Análisis de casos y fallos.

DOCENTES: Dres. Mariana Maldonado y Nicolás Ceballos

Litigación en entornos digitales: IA como testigo experto. Testigos Legos. Interrogatorio y contrainterrogatorio.

1. Presentación clara de datos técnicos ante el juez/jurado: simplificación del lenguaje.
2. Contrainterrogatorio de peritos: preguntas clave sobre cadena de custodia, métodos de análisis, margen de error.
3. Exhibición de la evidencia digital. Uso del material en juicio, preparación y litigación.
4. Interrogatorio y contrainterrogatorio a testigos expertos. Posibilidades de Impugnación.
5. Interrogatorio y contrainterrogatorio a testigos legos. Posibilidades de Impugnación.
6. ¿La IA como testigo experto? ¿Es posible reemplazar a los peritos o expertos por IA?, ¿Podría declarar en juicio?.
7. Prueba inflamatoria. Exclusión. Estándar. Valoración de prueba por parte del jurado popular. Efecto CSI.
8. Prácticas de argumentación final (alegatos) con enfoque en evidencia digital.
9. Análisis de casos y fallos.

DOCENTES: Dres. Rubén Chaia y Sebastián Lujan



PROGRAMA

Litigación en entornos digitales.

1. La preparación del caso en el entorno digital. Cómo desarrollar una teoría del caso digital sólida. Evidencia Digital técnica. Casos concretos: malware y criptoactivos.
2. Redacción de requerimientos y resoluciones teniendo en cuenta aspectos técnicos complejos. Utilización de lenguaje claro.
3. Testigos Expertos. Sujetos procesales habilitados a exponer sobre materias informáticas no reglamentadas. Formas de interrogar.
4. La posible influencia al juez o jurado. Publicaciones en redes durante el juicio. Prejuicios digitales.
5. Medidas cautelares urgentes. Modelos y casos.
6. Análisis de casos y fallos.

DOCENTES: Dres. Alejandro Musso (Fiscal Especializado UFEIC) y Alejandro Orlandini (Secretario UFEIC)

Criptoactivos en la investigación penal.

1. Introducción a los criptoactivos.
2. Medidas cautelares. Procedimientos para congelar y secuestrar criptoactivos en el marco de un proceso penal.
3. Legislación y guías sobre incautación de criptoactivos.
4. Custodia segura de los activos (hardware wallets, software wallets, etc.) para evitar su fuga.
5. Análisis de casos y fallos.

DOCENTES: Dres. Denis Banchero y Sebastian Luján

Herramientas informáticas de investigación: Rastreo de IP, análisis de metadatos y móviles.

1. Rastreo de direcciones IP.
2. Análisis de metadatos en archivos (documentos, imágenes, correos electrónicos).
3. Forense de dispositivos móviles: extracción de información y cifrado.
4. Necesidad de orden judicial para el rastreo de IP, análisis de datos de geolocalización y otros rastros digitales. Exclusión y admisión.
5. Aplicación de valores hash a la evidencia digital. Concepto. Cifrado. Tipos de hash. Metodología para su correcta aplicación. Importancia de su uso en la práctica jurídica. Limitaciones.
6. ¿Cómo resguardar de forma simple y sencilla un archivo digital de posibles alteraciones o manipulaciones? Procedimientos y software aplicables sin conocimientos técnicos.
7. Pericia. Existe la posibilidad de reproducir los pasos y el método en juicio?, ¿Cómo garantizo la credibilidad del trabajo pericial?, ¿Qué puntos / temas / pasos son importantes tener en cuenta?.
8. Análisis de casos y fallos.

DOCENTE: Lic. Willams Alfaro



PROGRAMA

Resolución de casos prácticos (I): integrando lo aprendido.

1. Envío de casos con componentes de los temas dados.
2. Creación de equipos (fiscalía, defensa, peritos) y asignación de roles.
3. Presentación de estrategias procesales y litigiosas de cada parte.
4. Trabajo en grupos sobre temas complejos y conflictivos según programa y aquellos que sean propuestos por los cursantes, debate de posiciones.
5. Puesta en común. Debate. Conclusiones.

DOCENTES: Dres. Rubén Chaia y Sebastián Luján

Estándares globales y protocolos de actuación en ciberdelitos.

1. Recomendaciones de Interpol, Europol y convenios internacionales (e.g. Budapest).
2. Protocolos forenses estándar para manejo de evidencia digital.
3. Coordinación internacional en investigaciones transnacionales.
4. La investigación y cooperación internacional desde la práctica.
5. Análisis de casos y fallos.

DOCENTE: Dra. Daniela Dupuy

Inteligencia Artificial en la práctica jurídica. Uso de herramientas para investigar.

1. Introducción a las herramientas de I.A. generativa y LLMs ChatGPT, Gemini, Notebook LM, Copilot. Como aplicarlas de forma adecuada en la práctica jurídica en general y en la evidencia digital en particular.
2. Aplicación práctica. Análisis de documentación compleja. Elaboración de gráficos y diapositivas con IA para mejorar la comprensión y explicación de la evidencia digital.
3. Elaboración de prompts jurídicos. Principios básicos del Prompt Engineering. Uso de delimitadores y placeholders. Aplicación a casos concretos.
4. Qué es un chatbot aplicado a la práctica jurídica. Creación de chatbots con ChatGPT y Gemini para delimitar la información de entrada y lograr resultados óptimos.
5. Problemas éticos y legales: sesgos algorítmicos y privacidad.
6. Ejercicio Práctico: creación de un chatbot

DOCENTE: Dr. Sebastián Luján

Inteligencia Artificial en la práctica judicial. La constitucionalización de derechos digitales.

1. Blockchain. Qué es y cómo funciona en el poder judicial.
2. Innovación y Derecho digital. Algoritmos, datos e IA. IA y Derechos Humanos. Identidades digitales. Protección de datos. Ecosistemas Digitales a través de IA.
3. Neuroderechos. Datos y Ética.
4. Metaverso y su aplicación en el derecho.
5. La constitucionalización de derechos digitales.
6. Reputación on line y derecho a la imagen en internet. Responsabilidad de los buscadores.
7. Tecnologías informáticas aplicadas a la investigación.
8. Análisis de casos y fallos.

DOCENTE: Dr. Mario Adaro



PROGRAMA

Desarrollo de investigaciones complejas: deep web, dark web y criptografía avanzada.

1. Diferencia entre deep web y dark web; Tor y otros servicios de anonimato.
2. Cifrado extremo a extremo y el dilema de las puertas traseras (backdoors).
3. Redes sociales en la Deep Web. Su investigación penal. Caso Telegram. Jurisprudencia.
4. Obtención de metadatos. El derecho de defensa ante la utilización de algoritmos secretos.
5. Análisis de información contenida en dispositivos de almacenamiento digital. Aplicación de la "Plain View Doctrine".

DOCENTE: Dr. Jonathan A. Polansky

Inteligencia Artificial Generativa. Producción de Imágenes. Neuroderechos.

1. Imágenes de material de abuso sexual infantil (MASI) íntegramente creadas por IAG. Rostros de menores fusionados con cuerpos desnudos creados por IA.
2. Debido proceso. Posverdad y posprivacidad en la era de IA.
3. Aplicaciones asistidas por algoritmos de IA.
4. Prueba digital y técnicas de identificación de fake news y Deep fake. Protocolo IFLA para detección temprana.
5. Técnicas de detección de Deep fake y adquisición de prueba digital. Aplicaciones para detectar Deep fake.
6. Neuroderechos y neurodelitos.

Docente: Dr. Carlos Sueiro

Investigación en fuentes abiertas. Herramientas y métodos. IA aplicada.

1. Investigación en fuentes abiertas. Herramientas abiertas para desarrollar investigaciones.
2. IA generativa y creación de contenido falso: riesgos para la prueba digital.
3. Individualización de personas mediante información obtenida de redes sociales y plataformas de pago. La utilización de los métodos de KYC como herramienta para la investigación penal.
4. Responsabilidad penal por la difusión de deepfakes y la protección de la integridad de las personas.

DOCENTES: Dr. Alejandro Orlandini y Diego Lugo

Taller. Secuestro y Apertura Forense de Dispositivos Tecnológicos.

1. Secuestro de dispositivos tecnológicos. Requisitos legales para su validez. Violación de la cadena de custodia. Triage.
2. Procedimiento de incautación. Protocolos vigentes para resguardar la evidencia digital en la escena del hecho.
3. Herramientas forenses de extracción de datos: UFED. Demostración de su uso. Modificación y preservación de la evidencia digital.
4. Apertura telefónica mediante técnicas de fuerza bruta. Modalidad de análisis y resultados.
5. Explicabilidad de los modelos de extracción forense. ¿Cómo podemos explicar su funcionamiento en un juicio?
6. Posibles cuestionamientos a la evidencia digital. Exclusión probatoria.

DOCENTE: Lic. William Alfaro



PROGRAMA

Resolución de casos prácticos (II): simulación de audiencia con evidencia digital.

1. Trabajo en grupos sobre temas complejos y conflictivos según programa y aquellos que sean propuestos por los cursantes, debate de posiciones.
2. Asignación de roles (fiscalía, defensa, jueces, peritos) para casos de perfiles multifacéticos.
3. Puesta en común de estrategias de cada parte: admisión, impugnación, alegatos, introducción y exhibición de pruebas, objeciones.
4. Deliberación final y retroalimentación general del docente y de los participantes. Cierre del curso.

DOCENTES: Dres. Rubén Chaia y Sebastián Luján

Clases Asincrónicas y envío de material: Estará a disposición de los cursantes para ampliar la base de saberes.

1. **Carlos Andres Guzman.** Prueba digital. Prueba ilegal. Estado actual en la jurisprudencia de Colombia.
2. **Amir Nayi Abushih.** El rol del defensor en casos que involucran investigaciones internacionales con prueba digital. Estrategias. Análisis del caso “Panamá Papers”.
3. **Rafael Blanco.** Prueba digital. Prueba ilegal. Estado actual en la jurisprudencia de Chile.
4. **Jaime Arellano.** Admisión de prueba digital. Test. Control. Impugnación
5. **Javier Zaragosa Tejada.** Prueba digital. Prueba ilegal. Estado actual en la jurisprudencia de España y Europa.



ARANCEL

Matrícula de \$ 150.000 (may) + 3 cuotas (jun-ago) de \$ 100.000.

TOTAL: \$ 450.000

LAS CUOTAS SE ABONAN DEL 1 AL 10 DE CADA MES, PASADA ESA FECHA, SE COBRARÁ UN RECARGO DEL 10%.

*Los valores son estimados y podrán ser actualizados de acuerdo a la evolución del índice inflacionario 2026. El costo total de la Diplomatura podrá ser actualizado en función de los condicionamientos económicos del Programa. El medio de pago que se utiliza es a través del portal de la universidad, que remite a MercadoPago, donde se puede abonar con tarjeta de crédito, débito o dinero en cuenta; como así también cuenta con opciones de financiación propias.



INSCRIPCIÓN

PARA INSCRIBIRSE INGRESAR AQUÍ

UNA VEZ QUE COMPLETES EL FORMULARIO DE INSCRIPCIÓN TE ENVIAREMOS UN EMAIL CON EL LINK DE PAGO. CUANDO REALICES EL PAGO TU INSCRIPCIÓN ESTARÁ COMPLETA

SE DEBE CONTAR CON UN MÍNIMO DE PREINSCRIPTOS PARA SU APERTURA. EN EL CASO DE NO ABRIR, FINALIZADO EL PERÍODO DE INSCRIPCIÓN, EL ÁREA DE POSGRADO SE PONDRÁ EN CONTACTO CON LOS INSCRITOS VÍA MAIL



BENEFICIOS y CONVENIOS

- COMUNIDAD UNSO (alumnos, Ex-alumnos o personal de las instituciones con convenio).
- FEDERACIÓN ARGENTINA DE LA MAGISTRATURA Y LA FUNCIÓN JUDICIAL
- ASOCIACION DE MAGISTRADOS Y FUNCIONARIOS DE LA JUSTICIA NACIONAL
- REFLEJAR - JU.FE.JUS
- ASOCIACIÓN DE FISCALES Y FUNCIONARIOS DEL MINISTERIO PÚBLICO FISCAL DE LA NACIÓN
- MINISTERIO PÚBLICO DE LA PROVINCIA DE BUENOS AIRES
- ASOCIACIÓN DE MAGISTRADOS Y FUNCIONARIOS DE SAN MARTIN
- COLEGIO DE MAGISTRADOS Y FUNCIONARIOS DE LA PROVINCIA DE BUENOS AIRES
- CONSEJO DE LA MAGISTRATURA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES (CABA)
- COLEGIO DE MAGISTRADOS Y FUNCIONARIOS DE SAN ISIDRO
- COLEGIO DE ABOGADOS DE SAN MARTIN
- DEFENSORÍA DEL PUEBLO DE LA PROVINCIA DE BUENOS AIRES
- COLEGIO PUBLICO DE ABOGADOS DE LA CAPITAL FEDERAL (CPACF)

15% DE DESCUENTO

(sobre las cuotas de la diplomatura)

PARA ACCEDER A LOS BENEFICIOS DEBE ENVIAR CERTIFICADO VIA E-MAIL

CONTACTO:

dip.juridicas@unsanisisidro.edu.ar