IUSE

ANEXO I

TECNICATURA UNIVERSITARIA EN INFORMÁTICA FORENSE

1. Identificación de la carrera

1.1 Denominación de la carrera: Tecnicatura Universitaria en Informática Forense.

1.2 Título a otorgar: Técnico/a Universitario/a en Informática forense.

1.3 Duración de la carrera: dos (2) años y medio (cinco cuatrimestres).

1.4 Carga horaria total: mil cuatrocientas cuarenta (1.440) horas reloj.

1.5 Ubicación de la estructura: Secretaría Académica.

1.6 Modalidad: Presencial.

2. Características de la carrera

2.1 El nivel de la carrera: pregrado.

2.2 Titulación: Técnico/a Universitario/a en Informática Forense.

2.3 Objetivos de la carrera

Objetivo General

Formar profesionales forenses especializados en el tratamiento de evidencia digital, capacitados para intervenir en la identificación, recolección, análisis y presentación documentada de evidencia digital en investigaciones judiciales y policiales; garantizando la cadena de custodia y aplicando criterios científicos, tecnológicos y jurídicos en concordancia con las normas nacionales e internacionales vigentes.

Objetivos Específicos

- Promover el desarrollo de habilidades técnicas especializadas para la identificación, preservación y recolección de evidencia digital en diversos entornos y contextos forenses.

- Capacitar en el manejo y aplicación de herramientas forenses digitales, de software y hardware, tanto de código abierto como licenciadas, aplicadas a la investigación criminal y su análisis forense.
- Transmitir conocimientos sólidos y actualizados en derecho penal, procesal penal y normativa vigente aplicable a la evidencia digital y a los delitos informáticos.
- Desarrollar y consolidar competencias para la redacción de informes técnicos forenses que garanticen claridad, exactitud y reconocimiento jurídico pleno.
- Desarrollar la capacidad de argumentar con fundamentos técnicos, científicos y jurídicos en diversos contextos, aplicando estrategias discursivas adecuadas a la defensa del informe pericial, garantizando precisión terminológica, claridad expositiva y coherencia argumental.
- Fortalecer las competencias comunicacionales necesarias para la exposición oral del informe pericial ante magistrados, fiscales, defensores y otros peritos.
- Impulsar la capacidad de trabajo interdisciplinario colaborativo con peritos, fiscales, jueces y otras fuerzas o cuerpos de seguridad.
- Transmitir e inculcar criterios éticos y principios de responsabilidad en el tratamiento, manejo y protección de información sensible y datos personales.
- Proporcionar una formación profesional integral que habilite al egresado a desempeñarse eficazmente como auxiliar de la justicia o perito de parte en investigaciones judiciales, así como en funciones técnicas.

2.4 Perfil del egresado

El egresado de la *Tecnicatura Universitaria en Informática Forense* será un profesional con conocimientos, actitudes y habilidades que le permitirán:

- Intervenir en casos que involucren evidencia digital, asegurando su identificación, documentación, recolección y preservación, conforme a la normativa vigente, resguardando la cadena de custodia.

- Actuar en procedimientos judiciales y policiales (allanamientos, secuestros, pericias, incidentes de ciberseguridad), asegurando la validez probatoria de la evidencia digital involucrada.
- Dominar las metodologías y herramientas especializadas para la adquisición y análisis forense de discos rígidos, dispositivos móviles, redes y entornos virtuales.
- Elaborar informes técnicamente fundados y sostener sus conclusiones mediante una argumentación clara, coherente y ajustada al lenguaje jurídico.
- Comprender y aplicar la legislación penal y procesal vigente relacionada con evidencia digital, delitos informáticos y protección de datos.
- Colaborar e integrar equipos interdisciplinarios en investigaciones criminales complejas, que requieran procesamiento y análisis de evidencia digital.
- Desarrollar capacidades de investigación aplicada, utilizando metodología científica y técnicas de análisis.
- Asumir un compromiso ético responsable en el manejo de información sensible, equilibrando la preservación de evidencia con la protección de derechos individuales, dentro del marco legal vigente.

2.5 Alcances del título:

La *Tecnicatura Universitaria en Informática Forense* habilitará al egresado para:

- Realizar la primera intervención forense en hechos que involucren evidencia digital, identificando potenciales fuentes de prueba y aplicando protocolos de seguridad para la preservación inicial de dispositivos y datos.
- Desempeñarse como auxiliar de la justicia o en el ámbito privado, en tareas vinculadas con la obtención, aseguramiento, adquisición y análisis preliminar de evidencia digital, utilizando herramientas y técnicas forenses en distintos sistemas y soportes.

- Aplicar procedimientos técnicos que garanticen la integridad, autenticidad y trazabilidad de la evidencia recolectada, resguardando la cadena de custodia.
- Reunir, organizar y documentar registros informáticos con validez judicial, conforme a criterios técnicos y legales vigentes.
- Elaborar informes técnicos forenses debidamente fundamentados, en concordancia con el marco jurídico aplicable.
- Actuar como perito oficial o de parte en procesos judiciales, produciendo dictámenes técnicos y participando en audiencias y juicios para sostener la validez científica de los análisis realizados.
- Asesorar en el cumplimiento de normativas vinculadas con la seguridad de la información y la protección de datos personales en el tratamiento de evidencia sensible.
- Integrar equipos interdisciplinarios e intervenir en investigaciones vinculadas con delitos o incidentes informáticos.

2.6 Requisitos de ingreso en la carrera:

Podrán ingresar a la carrera de *Tecnicatura Universitaria en Informática Forense* los graduados del nivel medio o polimodal con título de instituciones reconocidas oficialmente, que hayan presentado la documentación requerida por la normativa vigente para la educación superior universitaria.

Los mayores de veinticinco (25) años que no hayan aprobado el nivel medio o el ciclo polimodal de enseñanza, podrán postularse como aspirantes a la carrera, siempre que cumplan los requisitos que a tal efecto determina el Artículo 7 de la Ley de Educación Superior N°24521.

ANEXO II

Asignaturas y carga horaria

3. Organización del plan de estudios

3.1 Organización general

La carrera se estructurará en cinco (5) cuatrimestres. Además, para obtener el título de *Técnico/a Universitario/a en Informática Forense*, el/la estudiante deberá acreditar dos (2) niveles de idioma inglés.

N°	Espacio curricular	Carga Horaria Semanal	Carga horaria Total	Régimen	Modalidad
PRIMER AÑO		**1° Cuatrimestre**			
1	Sociología y conocimiento científico	4	64	Cuatrimestral	Presencial
2	Principios de la informática forense	4	64	Cuatrimestral	Presencial
3	Criminalística	4	64	Cuatrimestral	Presencial
4	Fundamentos de ciberseguridad y cibercrimen	4	64	Cuatrimestral	Presencial
		16	**256**		
PRIMER AÑO		**2° Cuatrimestre**			
5	Derecho constitucional y derechos humanos	4	64	Cuatrimestral	Presencial
6	Seguridad informática y seguridad de la información	4	64	Cuatrimestral	Presencial
7	Informática forense I	4	64	Cuatrimestral	Presencial
8	Tecnología aplicada a la investigación	5	80	Cuatrimestral	Presencial
		17	**272**		
SEGUNDO AÑO		**1° Cuatrimestre**			
9	Fundamentos de programación	3	48	Cuatrimestral	Presencial
10	Elementos de derecho penal y contravencional	4	32	Bimestral	Presencial
11	Elementos de derecho procesal penal y contravencional	4	32	Bimestral	Presencial

12	Adquisición de evidencia digital	4	64	Cuatrimestral	Presencial
13	Resguardo de evidencia digital	4	64	Cuatrimestral	Presencial
14	Informática forense II	4	64	Cuatrimestral	Presencial
		19	**304**		
SEGUNDO AÑO		**2° Cuatrimestre**			
15	Privacidad de la información digital	4	64	Cuatrimestral	Presencial
16	Criptografía	3	48	Cuatrimestral	Presencial
17	Evidencia digital en la nube y en otros entornos virtuales	3	48	Cuatrimestral	Presencial
18	Análisis forense de dispositivos móviles	4	64	Cuatrimestral	Presencial
19	Rol del perito y producción de informes periciales	4	32	Bimestral	Presencial
20	Ética profesional	3	48	Cuatrimestral	Presencial
		21	**304**		
TERCER AÑO		**1° Cuatrimestre**			
21	Técnicas avanzadas en forensia digital	4	64	Cuatrimestral	Presencial
22	Investigaciones complejas en entornos digitales	4	64	Cuatrimestral	Presencial
23	Taller de argumentación oral	3	48	Cuatrimestral	Presencial
24	Taller de redacción de informes técnicos informático forenses	3	48	Cuatrimestral	Presencial
25	Taller integrador de prácticas en informática forense	5	80	Cuatrimestral	Presencial
		19	**304**		
CARGA HORARIA TOTAL			**1440**		
Otros requisitos				**Observaciones**	
1	Inglés I		0	El/la estudiante deberá acreditar dos (2) niveles de idioma inglés.	
2	Inglés II		0		

**Las cargas horarias están expresadas en horas reloj.*

ANEXO III

Contenidos Mínimos

4.0 Contenidos mínimos

1. Sociología y conocimiento científico

La ciencia moderna: surgimiento y características. Historia del conocimiento científico: inductivismo, falsacionismo, positivismo y consenso de las ciencias exactas y aplicadas. Kuhn y las revoluciones científicas. El postempirismo. La reconsideración del objeto en las ciencias sociales y humanas. Conceptos fundamentales de la Sociología. La cultura. Campos de la sociología. La sociedad. La persona. La socialización y sus etapas. Los grupos sociales. Clasificación. La estratificación social, naturaleza y funciones. Movilidad social. Estratificación social y desigualdad de género. Estratificación étnica y racial. La dinámica social. Cambio social y desarrollo humano.

2. Principios de la informática forense

Definición, alcance y evolución de la informática forense. Concepto, naturaleza y características jurídicas de la evidencia digital. Tipos y clasificación de la evidencia digital. Etapas de la informática forense. Principales ciencias forenses y particularidades. Principios de la disciplina forense informática y buenas prácticas internacionales (ISO/IEC 27037 – NIST). Disciplinas forenses vinculadas a la informática forense. Arquitectura informática y periféricos esenciales. Elementos tecnológicos con información almacenada en formato digital. Registros activos y volátiles. Aspectos técnicos generales para la preservación de la evidencia digital.

3. Criminalística

La ciencia criminalística. Historia y evolución. Precursores. El método científico. El perito, rol y funciones. Concepto. Clases. Medios de prueba. La Criminalística de Campo. Conceptos generales. Protocolos de actuación: Pautas y precauciones generales para la manipulación e identificación de los indicios. El lugar del hecho: la inspección ocular. Registro de la escena del crimen. Hallazgo, levantamiento, conservación y clasificación de evidencias. Criminalística de laboratorio. Tipos de peritajes. Balística forense; Accidentología vial;

Identidad humana: Papiloscopía, Sistemas de identificación; Documentología. Peritajes documentológicos: tipos de documentos. Falsificación y adulteración. Peritaje caligráfico. Peritajes mecanográficos, Principios scopométricos. Seguridad documental. Papel moneda nacional y extranjera. Las Ciencias Forenses: Medicina Legal; Criminología. El criminalista, desempeño profesional, relaciones con otros actores del campo. Normativa que encuadra su desempeño.

4. Fundamentos de la ciberseguridad y cibercrimen

Concepto y evolución de la ciberseguridad. Activos de información y vulnerabilidades. Incidentes de ciberseguridad. Políticas y estándares internacionales asociados a la ciberseguridad. Vectores de ataque informático y riesgos asociados. Fundamentos del cibercrimen. Relación entre ciberseguridad, investigación y forensia digital. Delitos informáticos y en tratados internacionales (Convenio de Budapest). Clasificación del cibercrimen. Normativa asociada a la protección de datos personales.

5. Derecho constitucional y derechos humanos

El Derecho Constitucional: concepto y contenido. Constitucionalismo. Las constituciones: Tipos y clasificación. Antecedentes y fuentes de la Constitución Nacional. Contenido y método: parte dogmática y parte orgánica. Las cláusulas constitucionales: su operatividad. Control de constitucionalidad: concepto. Sistemas difuso y concentrado. La forma representativa, republicana y federal. Formas de Estado y formas de gobierno. Garantías constitucionales. Principios de legalidad y reserva. Debido proceso. Mecanismos de Garantía: Habeas Corpus. Amparo. Distribución de competencias entre Estado nacional y Estados locales. El Estado argentino: elementos. El principio de supremacía de la Constitución Nacional: jerarquía de las normas. Los tratados con jerarquía constitucional. Las formas semi directas de la democracia en la Constitución Nacional. Situaciones de emergencia. Organización del Estado a nivel Federal y nivel Provincial. Órganos del Estado a nivel federal. El Poder Legislativo: Atribuciones, estructura y composición. Organización y funcionamiento. Formación y sanción de las leyes. El Poder Ejecutivo: Atribuciones. Estructura. Órganos de control: Auditoría General de la Nación y Defensor del Pueblo. El Poder Judicial. Estructura. La Corte Suprema de Justicia de la Nación. Los tribunales inferiores. El Ministerio Público Fiscal: Misiones y funciones. Constitución de la CABA:

estatus jurídico de la Capital Federal y la Ciudad Autónoma. La organización del poder Judicial en la Ciudad de Buenos Aires. Derechos, garantías y políticas especiales. Gobierno de la Ciudad: Estructura. Derechos políticos y participación ciudadana. Poder Legislativo, Poder Ejecutivo y Poder Judicial: Atribuciones y Estructura. Los Derechos Humanos. Desarrollo histórico en el ámbito internacional y en el país. Declaraciones internacionales. Principios que emanan de la Constitución Nacional respecto de los Derechos Humanos. Incorporación de los pactos internacionales a la Constitución Nacional. Sistema Interamericano de Derechos Humanos. Principio de Jurisdicción Universal. Corte Penal Internacional. Derecho a la integridad de las personas: Reglas mínimas que pautan el trato que se le dispensa a la persona privada de libertad. Conjunto de principios para la protección de personas sometidas a cualquier forma de detención o prisión. Los estándares internacionales en materia de actividad policial. Responsabilidad de los funcionarios. Principios Básicos sobre el Empleo de la Fuerza y de Armas de Fuego por los Funcionarios Encargados de Hacer Cumplir la Ley (ONU) Código de conducta para funcionarios encargados de hacer cumplir la ley (ONU). Estudio de casos.

6. Seguridad informática y de la información

Definición. Diferencia entre seguridad informática y seguridad de la información. Características. Clasificación de datos y de información. Características del delito informático. Los sujetos pasivos del delito. Extraterritorialidad. La disociación temporal. Cooperación conjunta contra este tipo de delito. Análisis del marco normativo. Principios de la seguridad informática. Políticas, planes y procedimientos de seguridad. La importancia del factor humano en la seguridad. Estandarización y certificación en seguridad informática. Vulnerabilidades en los sistemas informáticos. Amenazas a la seguridad informática. Virus informáticos y otros códigos dañinos. Ciberterrorismo y espionaje en las redes de ordenadores. Fundamentos de la criptografía. Firma electrónica. Herramientas para la seguridad en redes de ordenadores. Seguridad en redes privadas virtuales. Seguridad en las redes inalámbricas. Desarrollo seguro de aplicaciones en internet. La lucha contra el spam. Delitos informáticos. Ingeniería social. Respuesta a incidentes de seguridad y planes para la continuidad del negocio.

7. Informática forense I

Definición y evolución de la informática forense. Campo de aplicación en el ámbito policial, judicial y pericial. Aspectos técnicos, legales y estratégicos de la disciplina. Alcances y limitaciones de la informática forense en el contexto de la investigación digital. Procesos generales en los que interviene la disciplina: identificación, recolección, preservación, análisis y presentación de resultados. Registros activos y volátiles: importancia en los procedimientos forenses. Técnicas de documentación y registro de actuaciones. Preservación y adquisición avanzada Bloqueo contra escritura en medios digitales: dispositivos de hardware y técnicas de software; limitaciones y riesgos. Creación de imágenes forenses avanzadas y flujos de trabajo estandarizados. Triage informático: objetivos, metodología, consideraciones legales, riesgos y limitaciones. Software utilizado en informática forense: aplicaciones *open source* y licenciadas. Utilización de entornos de práctica.

8. Tecnología aplicada a la investigación

Tecnología aplicada a la investigación. Definición y evolución de las tecnologías aplicadas a la investigación criminal y la importancia en la resolución de casos. Tecnologías para la obtención de imágenes, audios y videovigilancia. Tecnologías de reconocimiento facial y biometría. Análisis y mejoramiento de imágenes. Metadatos. Criptografía y criptoactivos. Sistemas de vigilancia por geoposicionamiento satelital. Tecnologías de análisis de información digital. La importancia de las telecomunicaciones.

9. Fundamentos de programación

Algoritmos y lógica de programación. Lenguajes de programación: tipos y entornos de desarrollo. Variables, tipos de datos y estructuras básicas. Estrategias de resolución de problemas y diseño de algoritmos. Uso de procedimientos, funciones y scripts. Fundamentos de la programación aplicados a la informática forense: automatización de tareas y procesamiento de datos. Análisis de datos digitales: filtrado, clasificación y correlación de información. Manejo de archivos y metadatos. Buenas prácticas de programación en entornos forenses. Manejo de repositorios en Github.

10. Elementos de derecho penal y contravencional

Derecho Penal y Derecho Contravencional, concepto. Garantías constitucionales. Teorías de justificación de las penas. La teoría del delito, concepto. Estratos que componen la teoría del delito: acción, tipicidad, antijuridicidad y culpabilidad. Delitos de omisión, concepto. Punibilidad. Tentativa y consumación, desistimiento. Autoría y participación. Concurso de delitos, concepto y tipos: ideal, real y aparente. Diferencias entre el derecho penal y el derecho contravencional. Delitos y contravenciones en particular, su regulación en el Código Penal y en el Código Contravencional, definición, elementos y características.

11. Elementos de derecho procesal penal y contravencional

Derecho Procesal Penal: concepto, objeto, funciones. Principios y garantías constitucionales: debido proceso, juicio previo, defensa en juicio, principio de inocencia, garantía de juez natural, la duración razonable del proceso, la garantía de no estar obligado a declarar contra sí mismo, la prohibición de persecución penal múltiple, la protección del domicilio, comunicaciones y papeles privados, exclusión de la prueba obtenida por medios ilícitos, principio de congruencia, sistema acusatorio, el derecho al recurso. Acción penal, concepto y tipos. Jurisdicción y competencia, nociones. Sistemas procesales: acusatorio, inquisitivo y mixto. Etapas del proceso. Actos procesales, nociones. Sujetos del proceso. Investigación penal preparatoria: formas de inicio, prueba (concepto, medios de prueba). El imputado en el proceso, restricciones a la libertad, medidas precautorias y cautelares. Etapa intermedia, concepto. Juicio oral y público; juicio por jurados: concepto; salidas alternativas de resolución de conflictos: concepto. Régimen procesal contravencional: principios generales, estructura y características propias. Diferencias con el régimen procesal penal.

12. Adquisición de evidencia digital

Definición y alcance de la adquisición de evidencia digital. Diferencia entre preservación, resguardo y adquisición. Estándares y buenas prácticas internacionales (ISO/IEC 27037 – NIST). Procedimiento de bloqueo contra escritura en unidades de disco. Métodos para preservar la integridad de las evidencias. Principios técnicos de duplicación forense: imagen bit a bit, hash y verificación de integridad. Tipologías de adquisición. Dispositivos comunes en la adquisición: discos rígidos, memorias externas, dispositivos móviles y entornos

virtuales. Herramientas de adquisición forense: software open source y licenciado. Documentación y registro de la adquisición: actas, formularios de cadena de custodia y reportes técnicos. Riesgos y limitaciones de la adquisición de datos en entornos digitales. Implicancias de una adquisición deficiente.

13. Resguardo de evidencia digital

Resguardo de la evidencia digital. Documentación de la escena. Procesos para garantizar la integridad, autenticidad y disponibilidad de los elementos digitales sujetos al proceso judicial. El rol del primer interventor y la cadena de custodia. Procedimientos iniciales en el lugar del hecho: identificación, aseguramiento y documentación de dispositivos electrónicos. Evidencia digital volátil y no volátil: particularidades y riesgos. Orden de Volatilidad. Métodos de conservación y traslado de soportes digitales. Repositorio de soportes digitales.Protocolos nacionales e internacionales: normativa vigente (CPPF, CPPN y CPP CABA), guías ministeriales y estándares ISO/NIST aplicables. Responsabilidades legales y consecuencias de una preservación deficiente.

14. Informática forense II

Procesos de análisis de imágenes forenses. Sistemas de archivos. Recuperación y análisis de información borrada. Registros del sistema operativo: archivos de log, metadatos, temporales y memoria de uso. Análisis de aplicaciones y programas instalados: historial de navegación, clientes de correo, mensajería instantánea y redes sociales. Herramientas forenses para el análisis digital (open source y licenciadas). Análisis forense de redes y detección de intrusiones.

15. Privacidad de la información digital

Concepto de privacidad en el entorno digital y su vinculación con los derechos fundamentales. Regulación nacional e internacional en materia de protección de datos personales y habeas data. Principios de licitud, finalidad, consentimiento, proporcionalidad y seguridad en el tratamiento de la información. Impacto de las tecnologías de la información y la comunicación en la privacidad: redes sociales, servicios en la nube, dispositivos móviles y sistemas de geolocalización. Análisis de riesgos en el manejo de datos sensibles. Relación entre privacidad, seguridad de la información y evidencia digital. Entornos seguros en el

manejo de la información. Herramientas técnicas para la protección de la privacidad: anonimización, cifrado y control de accesos. Jurisprudencia y casos relevantes en torno a la vulneración de la privacidad en entornos digitales.

16. Criptografía

Evolución de la criptografía en el ámbito de la forensia digital. Criptografía simétrica: algoritmos convencionales y su aplicación en el resguardo de datos. Criptografía asimétrica: algoritmos de clave pública y su uso en firmas digitales, certificados y autenticación. Funciones hash y su rol central en la preservación de evidencia digital y la verificación de integridad en la cadena de custodia. Infraestructura de Clave Pública y modelos de confianza en contextos judiciales. Análisis de la tecnología Blockchain. Herramientas y software de aplicación práctica en pericias: entornos de programación. Relevancia de la criptografía en la protección, análisis y presentación de evidencia digital.

17. Evidencia digital en la nube y en otros entornos virtuales

Abordaje de la evidencia digital en la nube. Modelos de servicios y despliegue en la nube y sus implicancias técnicas y legales para la investigación forense. Procesos de adquisición de evidencia en la nube: principales desafíos vinculados con la distribución geográfica de los datos, la replicación, el acceso restringido y los conflictos de jurisdicción; métodos y procedimientos disponibles para la adquisición remota, limitaciones técnicas y jurídicas. Preservación y análisis forense en entornos virtuales conforme a estándares internacionales, incluyendo el uso de herramientas open source y licenciadas. Estudio de entornos digitales específicos: redes sociales, mensajería instantánea y correo electrónico en la nube; entornos virtualizados y la infraestructura en la nube utilizada por la delincuencia organizada. Aspectos legales y cooperación internacional: marco normativo nacional, problemática de jurisdicciones extranjeras y convenios internacionales, con análisis de jurisprudencia y casos relevantes. Tendencias e innovaciones: blockchain y entornos distribuidos como fuentes de evidencia y retos futuros en la investigación de entornos virtuales.

18. Análisis forense de dispositivos móviles

Análisis forense de dispositivos móviles. Particularidades de la evidencia digital en teléfonos celulares, tablets y dispositivos inteligentes. Arquitectura de sistemas móviles: sistemas

operativos (Android, iOS) y estructuras de archivos. Métodos de adquisición en dispositivos móviles. Tipos De Extracción: lógica, sistema de archivos y física. Técnicas de preservación y consideraciones legales específicas para evidencia móvil. Herramientas forenses aplicadas a móviles: software *open source* y licenciado (Cellebrite, Magnet AXIOM, Autopsy, entre otros). Extracción y análisis de registros. Recuperación de información eliminada. Análisis de memoria volátil y almacenamiento interno. Estado del Dispositivo: BFU vs AFU. Limitaciones, riesgos y desafíos actuales en el análisis forense de móviles: cifrado, bloqueo, contraseñas, autenticación biométrica.

19. Rol del perito y producción de informes periciales

Rol del perito en el proceso judicial: concepto, funciones, normativa aplicable y tipos de peritos. La pericia como medio de prueba. Diferencia entre prueba pericial y prueba testimonial. Requisitos profesionales, título habilitante, aceptación del cargo, juramento, recusación y excusación. Responsabilidad legal del perito: falsedad, falso testimonio e incumplimiento de deberes procesales. Proposición y determinación de puntos de pericia. El informe pericial: estructura, tipos, léxico técnico y modalidades de presentación. Honorarios profesionales. Redacción y análisis de documentos periciales: solicitudes, traslados, pedidos aclaratorios, impugnaciones, observaciones y respuestas ampliatorias. Elaboración de textos impugnativos y defensas. Principios de argumentación y detección de falacias aplicados a informes técnicos. Otras presentaciones judiciales vinculadas a la actuación pericial.

20. Ética profesional

El fenómeno moral. Naturaleza. Ética y Moral. Definición de ética. Método. Fuente. El acto humano. Condicionamientos psicológicos y sociológicos. Elementos. Libertad. Determinismo. Objeto de la Ética. El bien. El fin último. La ley. El razonamiento ético. La cosmovisión griega. La cosmovisión cristiana. Realismo y nominalismo. Ética de fines. La moral formal. Fundamento moderno. Sujeto racional. razón pura – razón práctica. El deber. El bien absoluto. Imperativo categórico. La persona como fin en sí mismo. Ética social. Concepto de sociedad. Tipos. Ética y moralidad: conceptualización y marco teórico. La problemática ética contemporánea: éticas vigentes y morales emergentes. Ética aplicada al ejercicio profesional.

21. Técnicas avanzadas en forensia digital

Funcionamiento interno y estructura de la memoria volátil. Procedimientos de adquisición en vivo y herramientas especializadas. Adquisición y análisis de memoria RAM. Análisis forense de malware y detección de procesos maliciosos en ejecución. Identificación de datos volátiles, conexiones de red y registros. Análisis avanzado de datos y correlación de evidencias. Prácticas en entornos simulados y resolución de casos aplicados a investigaciones.

22. Investigaciones complejas en entornos digitales

Técnicas de correlación de evidencias digitales provenientes de diversos dispositivos y entornos. Uso de herramientas de análisis forense y análisis criminal aplicadas a la investigación digital. Elaboración y uso de matrices investigativas. Marco normativo nacional e internacional: cooperación entre jurisdicciones locales y tratados internacionales. Cooperación entre el sector público y el sector privado. Plataformas de requerimientos de información. Aspectos procesales y desafíos legales de las investigaciones complejas. Elaboración de informes integrales y multidisciplinarios. Estudio de jurisprudencia y casos prácticos.

23. Taller de argumentación oral

La comunicación en el ámbito pericial y judicial. La argumentación científica y su relación con la prueba judicial. El conocimiento especializado explicado en lenguaje común. Claridad, coherencia y pertinencia en la exposición técnica. El informe pericial en función de la teoría del caso de la parte que propone al perito. La declaración del perito durante el juicio oral. Interrogatorio: diferencias entre exámen directo y contraexamen. La necesidad de acreditación del perito como tal en el examen directo. Su conocimiento especializado en la materia. Títulos, conocimiento, práctica y experiencia profesional. La acreditación de su testimonio. Estrategias discursivas y comunicacionales en defensa del informe pericial. Metodología para presentar conclusiones: relato temático vs relato cronológico (conclusiones, procedimientos, pasos y método científico). La rigurosidad del contraexamen.

24. Taller de redacción de informes técnicos informático forenses

Concepto, naturaleza y función del informe técnico informático forense dentro de la investigación judicial. Características particulares del informe informático forense. Elaboración de informes en distintos tipos de evidencia digital: discos rígidos, dispositivos móviles, redes, nube y entornos virtuales. Uso del lenguaje técnico especializado y fundamentación científica. Errores frecuentes en la redacción y sus consecuencias jurídicas. Estrategias de presentación de resultados ante la autoridad judicial y participación del forense en audiencias. Ejercicios prácticos de elaboración y análisis crítico de informes técnicos forenses.

25. Taller integrador de prácticas en informática forense

Instancia curricular que permitirá al estudiante participar en diferentes actividades, poniendo en juego diversos conocimientos adquiridos durante la formación como así también consolidar funciones propias de su perfil profesional.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S

"2026 - Año del 30° Aniversario de la sanción de la Constitución de la Ciudad Autónoma de Buenos Aires"

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2026-13573583-GCABA-DGPDUN

Buenos Aires, Miércoles 18 de Marzo de 2026

Referencia: Anexo - Tecnicatura Universitaria en Informática Forense.

El documento fue importado por el sistema GEDO con un total de 17 pagina/s.

Digitally signed by Comunicaciones Oficiales
Date: 2026.03.18 14:42:31 -03:00

Florencia Pozzuto
Director General
D. G. DE PLANEAMIENTO Y DESARROLLO UNIVERSITARIO
AREA JEFE DE GOBIERNO

Digitally signed by Comunicaciones Oficiales
Date: 2026.03.18 14:42:32 -03:00