Especialización en

CIBERDELITOS y EVIDENCIA DIGITAL

MENDOZA

2025

INTRODUCCIÓN

Tras el éxito de la primera edición, llega una versión renovada y potenciada de la Especialización en Delitos Informáticos y Ciberdelitos, diseñada para quienes se desempeñan en el ámbito judicial, de seguridad, tecnológico y académico. Esta propuesta surge del trabajo colaborativo con alumnos de toda América Latina, quienes, a través de una encuesta, compartieron sus valoraciones y sugerencias para enriquecer aún más esta formación profesional.

- Fecha de inicio: 04/09/2025

- Modalidad: Virtual sincrónica

- Día y horario de cursada: jueves de 18:00hs a 20:00hs.

- Destinatarios: Fuerzas de seguridad, fiscales, jueces, investigadores digitales, técnicos en cibercrimen y funcionarios públicos del sistema de justicia.

Mejoras incorporadas

Gracias al análisis de las encuestas completadas por los alumnos en otras provincias y América Latina, decidimos redoblar la apuesta y avanzar hacia una formación aún más actualizada, dinámica y conectada con los desafíos reales del cibercrimen incorporando las siguientes mejoras y propuestas:

- Participación especial de la Ing. Karina Gibert, Decana de la Universidad de Cataluña, elegida entre las 100 personas más influyentes de España por la revista Forbes y referente internacional en Inteligencia Artificial (adjuntamos CV). Nos gustaría contar con su presencia en la apertura de esta nueva edición.

- Participación especial del Dr. Christian Walter, director en Guilford County Schools (Estados Unidos), quien compartirá en primera persona cómo se trabaja en la prevención de ciberdelitos, acompañado por un alto funcionario de la Policía estadounidense.

-Posibilidad de participación de profesionales de Boston, sujeta a agenda y disponibilidad presupuestaria o patrocinadores.

- Innovaciones metodológicas: proponemos para esta nueva edición implementar talleres prácticos en salas divididas por Zoom, donde cada participante pueda aplicar en tiempo real los contenidos aprendidos por módulo. Además, incorporaremos una nueva plataforma que permitirá a los participantes tener una experiencia más amigable con el material. Oportunidad de formación internacional: Estamos explorando la posibilidad de ofrecer, en esta segunda edición, una estancia académica en España para aquellos alumnos que lo soliciten, incluyendo una doble titulación (a definir con las instituciones correspondientes)

- Los alumnos contarán con el acceso a un software especializado —herramienta de trazabilidad de activos virtuales— que les permitirá resolver casos prácticos.

DENOMINACIÓN DE LA ACTIVIDAD

ESPECIALIZACIÓN EN CIBERDELITO Y EVIDENCIA DIGITAL.

FUNDAMENTACIÓN

El desarrollo de las nuevas tecnologías de la información y comunicación trajo aparejado la comisión de nuevas modalidades delictivas que luego fueron sancionadas por el legislador. Ello así, la evolución constante en la comisión de dichas prácticas hace necesario la capacitación continua en la temática de los delitos informáticos, a fin de dotar a los operadores del sistema de instrumentos capaz de prevenir y advertir las conductas en cuestión.

Se observa un cambio de paradigma en las Técnicas de Investigaciones Criminales, los delincuentes están utilizando cada vez más Internet para planificar, coordinar y ejecutar actividades ilícitas. Las amenazas cibernéticas, como el fraude electrónico, la distribución de materiales ilícitos y el ciberacoso, requieren habilidades específicas para ser detectadas y abordadas. El uso de tecnologías como la darknet, criptomonedas y comunicaciones cifradas complica la detección y el seguimiento de actividades ilegales.

La necesidad de comprender y utilizar herramientas digitales de tecnología avanzada es crucial para la eficacia en la aplicación de la ley; dicha capacitación mejorará las capacidades de Investigación y proporcionará a los agentes herramientas y conocimientos para rastrear actividades criminales en línea de manera efectiva, aumentando la capacidad de recolectar y analizar evidencia digital, elementos esenciales para procesar cualquier tipo de delito.

En este contexto, se facilitará la prevención de delitos mediante el monitoreo de actividades sospechosas y la identificación de patrones delictivos. Asimismo, mejora la capacidad de colaborar con otras agencias y organismos internacionales en investigaciones transnacionales, fomentando la cooperación con sectores privados y proveedores de servicios de Internet para obtener información crítica.

Todo lo hasta aquí expuesto permite concluir que el material abordado por el cuerpo docente permitirá a las fuerzas de la ley ser más proactivas en la identificación de amenazas potenciales antes de que se materialicen.

OBJETIVOS

Capacitar a los cursantes brindando conocimientos, habilidades y aptitudes específicas en cada uno de los ejes temáticos a abordar que involucran la aplicación de las nuevas tecnologías en el mundo delictivo.

Tratamiento interdisciplinario en materia de prevención de hechos delictivos sometidos a estudio, es decir su conocimiento desde la perspectiva legal, psicológica y desde la informática forense, de manera que cualquiera sea la función que cumpla el operador encargado de hacer cumplir la ley, obtenga las habilidades necesarias y la idoneidad para desempeñar correctamente su actividad laboral y profesional.

OBJETIVOS ESPECÍFICOS

El presente programa prevé la formación, capacitación y entrenamiento de las fuerzas de seguridad del gobierno de la Provincia en las nuevas modalidades delictivas a través de las tecnologías de la información y comunicación que los cibercriminales utilizan para cometer delitos, desde una simple averiguación de paradero, hurto, robo, homicidio, hasta los ciberdelitos como phishing o grooming entre otros.

❖ Se dotará a los participantes del presente programa de las herramientas más recientes para prevenir y erradicar estos delitos.

❖ Se dará comienzo a la actividad con una fase teórica para luego comenzar con una etapa de aplicación práctica mediante la resolución de los casos más frecuentes en los entornos delictivos.

❖ Asimismo, y en el marco de las habilidades que se destaquen por parte de los participantes al presente programa, se propondrá a la autoridad ministerial la formación de equipos especializados en la materia a fin de que las fuerzas de la ley gocen de la presencia de dichos equipos en sus unidades de trabajo para estar a la vanguardia en la prevención y lucha contra el cibercrimen.

❖ Los campos del conocimiento a tratar como asimismo su aplicación en el tratamiento y resolución de casos concretos mejorará significativamente la respuesta del personal de las fuerzas de ley a las demandas del servicio de justicia y de la ciudadanía, ya que podrán colaborar de manera efectiva y eficiente con dichos actores sociales. El presente plan de estudios incluye la capacitación y formación de equipos especializados sin la necesidad de adquirir soluciones tecnológicas costosas, atento que se implementa un nivel inicial de prueba piloto con software libre y tecnología Demos; permitiendo a los agentes extraer información de dispositivos sin necesidad de incautarse, como suele hacerse en otros lugares de América Latina.

❖ Asimismo, al finalizar el presente programa de estudios los agentes estarán capacitados para analizar grandes volúmenes de información, formarse como agentes digitales en redes, brindar apoyo técnico en allanamientos para la incautación de cripto-activos, fortalecer la redacción de denuncias, cooperación público-privada con empresas y exchanges, obtener evidencia digital de manera forense.

PLAN DE ACCIÓN Y CONTENIDO

DURACIÓN: 4 meses

- Capacitación en ciberdelitos (curso I- teórico).
- Capacitación, implementación y entrenamiento de equipos especializados para análisis digital (analistas digitales en general) y para analistas I2. (teórico-práctico)
- Capacitación e implementación teórica con workshops prácticos para la formación de agentes reveladores (teórico-práctico).
- Capacitación e implementación práctica del armado de equipos para incautación de cripto-activos-(CURSO V) (teórico-práctico).
- Capacitación, entrenamiento e implementación de la puesta en marcha de dos (2) oficinas periciales para extracción forense de teléfonos celulares y discos rígidos con software libre. (teórico-práctico).
- Introducción en Inteligencia Artificial y Protección de la información personal en el ecosistema de internet.

EVALUACIÓN Y MEJORA CONTINÚA

El presente programa de capacitación teórico- práctico está diseñado para la evaluación regular de la efectividad de la capacitación a través de métricas de desempeño y retroalimentación entre los participantes y el cuerpo docente.

En definitiva, la capacitación en la implementación y funcionamiento de agentes de investigaciones en Internet es fundamental para que las fuerzas de la ley puedan enfrentar los desafíos del crimen en el entorno digital. Esta formación no sólo mejorará las capacidades investigativas, sino que también fortalecerá la proactividad y la colaboración, asegurando que las fuerzas de seguridad estén preparadas para proteger y servir eficazmente en un mundo cada vez más digitalizado

DATOS ADICIONALES

- **Cantidad de Asistentes:** A confirmar por el Ministerio de Seguridad y Ministerio Público Fiscal.
- **Material Bibliográfico:** Se pondrá a disposición de los agentes a través de su correo electrónico.
- **Plataforma de clases:** A través de las salas de zoom puestas a disposición por CLICLEX los agentes tendrán acceso a las asignaturas.
- **Foro de discusión:** Los agentes tendrán acceso a un canal de comunicación con los docentes

para evacuar dudas y plantear todo tipo de inquietudes que tengan.

ORGANIZACIÓN DEL PLAN DE ESTUDIOS

NIVEL I - INICIAL: *"INCLUSIÓN EN LA SOCIEDAD DE LA INFORMACIÓN"*

I. Introducción a los Ciberdelitos

La educación digital y su importancia en la prevención de delitos. Principios básicos de seguridad de la información: Integridad, Confidencialidad y Disponibilidad. Identificación de los ciberdelitos más comunes dirigidos a niños y adultos. Herramientas y recursos para la seguridad en línea. Fomento de habilidades críticas para evaluar la veracidad de la información digital. Promoción de la ciudadanía digital activa. Planificación y respuesta ante incidentes en línea. Procedimiento práctico para la obtención de evidencia digital como prueba en dispositivos móviles proporcionados por las víctimas y/o denunciantes.

II. Delitos Informáticos

Delitos informáticos. Introducción y aspectos generales. El cibercrimen, legislación nacional y derecho comparado. Ley 27.411. Ley 26.388. Clasificación de los delitos informáticos. Los delitos previstos en la Convención de Budapest. Acceso en forma abusiva a la información. Introducción y ejecución de virus informáticos. Espionaje y falsificación. Violencia sobre bienes informáticos. Abuso de la detención y difusión de códigos de acceso. Cuestiones jurídicas de los nuevos medios de investigación y prueba. Debate sobre el acceso transfronterizo de datos. Agente encubierto digital, técnicas de remote forensic, geolocalización, drones, etc.

III. Ciberestafas y otras defraudaciones en la era digital

Alcances, desafíos y amenazas. Visión y herramientas en lo penal. Conceptualización del "fraude y ciberfraude". Las figuras penales vinculadas al "fraude bancario". Estafa. Defraudación y ciberdefraudación, análisis comparativos metodológicos. Metodologías tendientes a la configuración del fraude. Autoría y participación. Prevención. Detección de operatorias ilegales ¿Cómo proceder? Denuncia. Seguimiento. Colaboración con las investigaciones judiciales.

IV. El delito de Grooming

Concepto de Grooming. Marco normativo. Antecedentes. Perfilación del agresor sexual. Análisis del art. 131 C.P., comparación con otras figuras y su vinculación con la explotación sexual y con el abuso sexual. Su regulación en el derecho argentino. Su relación con las figuras del Sexting, Revenge-Porn, Sextorsión, Stalking. Conceptos, diferencias, alcances, regulación jurídica, casos prácticos. Análisis de Jurisprudencia actual y casuística.

V. MASI (Material de Abuso Sexual Infantil)

Concepto, antecedentes, su relación con el grooming, la pedofilia y sus distintas variantes. Análisis del Art. 128 del Código Penal y las diferentes figuras penales. Ley 26.388. Ley 27.436. Bien jurídico protegido. Sujeto activo, sujeto pasivo. El medio empleado. Punición de la tenencia para autoconsumo. El debate sobre el Posing, Pornografía técnica. Aspectos procesales y ley 27.319.

VI. Ciberdelincuencia y Responsabilidad Directiva en el Contexto Escolar.

La ciberdelincuencia en el ámbito escolar, con especial énfasis en la responsabilidad de los equipos directivos en su prevención y gestión. Se abordan los marcos normativos aplicables, las estrategias institucionales para mitigar riesgos y los protocolos de articulación con autoridades judiciales y policiales, garantizando una actuación eficaz y conforme a derecho

Acciones Propuestas de cierre de Nivel I.

Se propone culminar esta etapa con un taller práctico enfocado en la redacción de oficios judiciales para casos de ciber-estafas. Durante el taller, se desarrollarán los conceptos básicos, incluyendo CBU/CVU, cuenta de origen y cuenta de destino. Además, se abordará la recepción de denuncias penales y la solicitud de medidas preventivas a bancos públicos y privados. El taller también incluirá un protocolo de actuación que cubra congelamientos, incautaciones, devoluciones y decomisos. Se proporcionarán herramientas para la investigación para prevención de delitos sexuales en línea, lo que permitirá a los agentes de la ley iniciar investigaciones proactivas a nivel provincial. Asimismo, se propone el asesoramiento y acompañamiento en la creación de equipos especializados en la temática.

NIVEL II- INTERMEDIO: *“CAPACITACIÓN, DISEÑO, ENTRENAMIENTO E IMPLEMENTACIÓN DE EQUIPOS ESPECIALIZADOS EN ANÁLISIS DIGITAL EN GENERAL y ANALISTAS I2 EN PARTICULAR”*

I. Solicitud de Información a Proveedores de Servicio de Internet (ISPs): Guia y mejores prácticas.

Requerimientos a empresas privadas. Facebook, Instagram, Whatsapp, Tiktok, Google, Gmail, Telcos. Modelos para requerir información. Apertura de cuentas oficiales en los sitios. Análisis de la información una vez obtenida la respuesta. Contacto y correos electrónicos de los responsables de las empresas para casos de URGENCIA. -

II. Conocimiento de nuevas herramientas

Análisis de Telecomunicaciones: Introducción a las Tecnologías de Telecomunicaciones: funcionamiento de las celdas telefónicas y cobertura. Diferencias entre redes 4G, 5G y su impacto en la localización. Análisis Avanzado de Celdas: Identificación de patrones de movilidad y comportamiento de los abonados. Técnicas avanzadas para la triangulación y localización precisa de dispositivos. Ejemplos de casos reales de análisis geoespacial exitoso.

Análisis de Grandes Volúmenes de Datos: Fundamentos del Big Data en la Investigación Criminal: Retos y oportunidades en el manejo de grandes volúmenes de datos. Herramientas y Metodologías: Formación en el uso de I2 Analyst's Notebook y otras herramientas similares. Ejemplos de cómo estructurar y limpiar datos para análisis eficientes Visualización y Narrativa de Datos: Técnicas avanzadas de visualización de datos para representar redes criminales. Desarrollo de informes narrativos efectivos que acompañen los gráficos.

workshop práctico: Deberán resolver un caso práctico real con el apoyo de los tutores designados a tal efecto relacionado al requerimiento y análisis en META, como así también en el análisis de un caso práctico con la herramienta I2.-

Acciones Propuestas de cierre de Nivel II

Resolución de Caso Práctico: Descripción detallada del caso práctico con objetivos claros. Asignación de roles dentro del equipo para fomentar el trabajo colaborativo.

Supervisión y Tutoría: Tutores especializados disponibles para guiar a los equipos. Feedback en tiempo real sobre las estrategias y métodos utilizados.

Presentación Final: Exposición de los resultados del análisis del caso práctico. Discusión de las lecciones aprendidas y propuestas de mejora.

Nivel III. AVANZADO “FORMACIÓN DE AGENTES REVELADORES Y AGENTES DE MONITOREO EN PREVENCIÓN DE DELITOS EN EL ECOSISTEMA DIGITAL”

I. Introducción a OSINT (Open Source Intelligence). Inteligencia de Fuentes abiertas aplicadas a la función pública y privada.

Historia. Evolución. Concepto. Fases. Fuentes de información pública y privadas. Google hacking. Navegadores Privados. ¿Quién utiliza Osint?. Herramientas Osint. Investigación en RRSS. Obtención de datos.

II. La figura del agente revelador. Agente Encubierto. Agente Provocador.

Antecedentes. Conceptos. Regulaciones. Características. Supuestos de su procedencia. Principios de su actuación. Ámbito de aplicación. Canales de actuación. Herramientas de actuación. Plazo en su actuación. Responsabilidades. Valoraciones de su actuación. Casos de éxitos, legislación, diferencia con el agente encubierto y el agente instigador. Introducción al ciber patrullaje. Implementación, cuestionamientos, legislación vigente.

-**Workshop práctico:** En este taller, los participantes tendrán la oportunidad de resolver un caso práctico creando su propio avatar.

Asimismo, bajo guía de un experto de la firma Cellebrite, se demostrará la funcionalidad de la herramienta Smart Search, enfocándose en la búsqueda y relacionamiento de datos en fuentes abiertas.

Actividades del Workshop:

● Creación de Avatar: Los cursantes desarrollarán su propio avatar, el cual será utilizado a lo largo del caso práctico.

● Resolución de Caso Práctico: Los participantes aplicarán técnicas avanzadas para resolver un caso práctico real.

● Demostración de Smart Search: Un experto de Cellebrite mostrará cómo utilizar Smart Search para realizar búsquedas y correlacionar datos en fuentes abiertas de manera efectiva.

Acciones Propuestas de cierre de Nivel III

Se propone el asesoramiento y acompañamiento en la formación de un equipo especializado en la investigación de fuentes abiertas de información y en la creación de un equipo de Agentes Reveladores en el ecosistema digital.

NIVEL IV - AVANZADO: *"CAPACITACIÓN, ENTRENAMIENTO E IMPLEMENTACIÓN DE EQUIPOS PARA INCAUTACIÓN DE CRIPTO-ACTIVOS.*

I. Criptomonedas y Blockchain.

Cripto-activos, Bitcoin: Elementos, estructura y funcionamientos. Consideraciones terminológicas respecto a los tipos de dinero y monedas. Concepto de dinero, dinero electrónico, de curso legal. Monedas Virtuales. Criptomonedas: Litecoin, Dogecoin y Ethereum. El delito de estafa cometido con criptomonedas. Funcionamiento. Regulación. Jurisdicción Internacional en materia de E-Commerce. Casos prácticos exitosos. Resolución en actuales. Gaffi, UIF, jurisprudencia.

II. Los Cripto-Activos y su vinculación con la actividad criminal en Argentina.

Historia de las criptomonedas y su impacto en Argentina. Nuevas modalidades delictivas. Malware. Incautación de cripto-activos. Lavado de Activos - Anticorrupción. Cooperación Internacional. Financiamiento del Terrorismo. Casos de Éxitos. Incautación. Recuperación de activos, solicitud de capturas internacionales**.**

WORKSHOP PRÁCTICO CON PERSONAL EXPERTO DE CELEBRITE: **Título: "Investigación de Criptomonedas con Chainalysis Reactor: Técnicas y Herramientas Avanzadas**" Objetivos para los Usuarios: Dominar el uso de Chainalysis Reactor. Aprender técnicas avanzadas de investigación de criptomonedas. Desarrollar habilidades para identificar y rastrear actividades ilícitas. Intercambiar conocimientos y experiencias con expertos y colegas. Contenido del taller: Introducción a Chainalysis Reactor, descripción de la herramienta y sus funcionalidades.Configuración y personalización de la

plataforma. Investigación de Criptomonedas. Técnicas de rastreo de transacciones y actividades ilícitas. Compartir información y hallazgos con colegas y expertos. Integración con otras herramientas y sistemas.Mejores prácticas para la colaboración en investigaciones.

Entrenamiento e implementación de equipos especializados en la incautación de cripto-activos. Software y hardware. Tecnología. Puesta en marcha. -

Acciones Propuestas de cierre de Nivel IV

Se propone el asesoramiento y acompañamiento en la formación del equipo especializado en la incautación de criptoactivos. Procedimiento para el alta en cuentas oficiales del personal policial en Exchanges y recurso para la remisión de oficios a diversas empresas. Obtención de herramientas para realizar la trazabilidad de activos virtuales.

NIVEL V: *"CAPACITACIÓN, ENTRENAMIENTO E IMPLEMENTACIÓN DE OFICINAS PERICIALES PARA EXTRACCIÓN DE INFORMACIÓN EN TELÉFONOS CELULARES Y DISCOS RÍGIDOS"*

I: Oficina Pericial.

Funcionamiento. Protocolos de actuación. Legislación Vigente. Dispositivos Informáticos. Software y Hardware necesarios. Oficina de Efectos. Cadena de Custodia.

II: Extracción de información de dispositivos móviles y Discos rígidos.-

Extracciones de información de celulares de las víctimas, código hash, acta de confección. Distintos Software Forense. Complejidad. Recomendaciones prácticas. Extracción de información con Autopsy. Funcionamiento. Métodos. Cadena de Custodia. Embalaje. Protocolos. Normativa Legal. Recomendaciones internacionales (F.B.I). Pericias informáticas. Análisis de la información. Ufed Reader. Análisis de la información contenida en un dispositivo. Contactos, llamadas y conversaciones, imágenes, vídeos, ubicaciones, aplicaciones que se instalaron, etc.

III: Etapas de una pericia informática

Importancia del análisis de los puntos de pericia, al momento de aceptar el cargo (especificidad de la tarea, necesidad de ampliar el cuerpo pericial por otras especializaciones). Especialidad y conocimientos técnicos del perito. Tratamiento de excepción o remoción del perito. Reunión inicial. Realización de la pericia. Debate sobre los puntos de pericia. Pedidos de nuevas pruebas. Importancia de una integración pericial con el Tribunal o los abogados de las partes. Utilidad de la Cédula Electrónica.

IV: El Perito de Oficio y el Perito de Parte

Funciones y responsabilidades de cada uno. Importancia de una buena elección del perito de parte. Aporte del perito en forma previa (para nuevos puntos de pericia) y durante el desarrollo de la pericia. Importancia para situaciones futuras (impugnaciones, ampliaciones, discrepancias periciales). Logros pedagógicos: entender las distintas responsabilidades de un perito nombrado por el juzgado y las de un perito que nombre una de las partes.

WORKSHOP PRÁCTICO CON PERSONAL EXPERTO DE CELLEBRITE:
Introducción a Cellebrite: Visión general de las herramientas y soluciones.

Principales Herramientas:

- Cellebrite Inseyets: Desbloqueo y Extracción de información en Dispositivos Móviles.
- Physical Analyzer: Extracciones Selectivas de la información.
- Pathfinder: Investigaciones y entrecruzamiento de datos obtenidos en la extracción.

Acciones Propuestas de cierre de Nivel V

Se propone el asesoramiento y la implementación de las siguientes acciones:

Asesoramiento Técnico y Estratégico: Proporcionar asesoramiento experto para la creación y optimización de oficinas periciales dentro del Ministerio de Seguridad. Evaluar las necesidades específicas y diseñar un plan personalizado que garantice la efectividad y eficiencia de las nuevas oficinas.

Implementación de Software Forense: Software Libre: Identificar y recomendar soluciones de software libre que puedan ser utilizadas para realizar análisis forenses, garantizando así la accesibilidad y reducción de costos.

Software Privativo: Evaluar y seleccionar software privativo que ofrezca funcionalidades avanzadas y soporte técnico especializado, asegurando la máxima precisión y fiabilidad en los procesos periciales.

NIVEL VI: Introducción a la Inteligencia Artificial, Sociedad Digital. Protección de la información personal en el ecosistema de internet.

I: Introducción a la Inteligencia Artificial.

Marco ético y regulatorio. Desafíos actuales. Sociedad Digital: Concepto y alcance . Derechos Digitales y Neuroderechos. Situación actual en organismos públicos y privados en América Latina.

II: Protección de la información personal en el ecosistema de internet.

Concepto. Principales medidas de resguardo. Análisis de la Ley 21719. Análisis comparativo en América Latina. Su relación con el nuevo Reglamento de Protección de datos europeo (GPRD).

Principales diferencias regulatorias. Compliance, concepto, alcance, marco legal. Legal tech: nuevos paradigmas en torno a la protección y colaboración de la información público privada.

III: Lavado de Activos y Criminalidad Organizada:

Convenciones internacionales: FATF/GAFI y la Convención de Palermo. Modalidades comunes de lavado de activos: uso de empresas pantalla, paraísos fiscales, y métodos informales de transferencia de valor. Identificación de estructuras criminales: cárteles, redes de trata y tráfico ilícito de bienes. Estudio de un caso práctico internacional.

EXAMEN FINAL Y CERTIFICACIÓN DEL CURSO DE ESPECIALIZACIÓN EN CIBERDELITOS.

Objetivo del Examen de Entrenamiento:

Los cursantes deberán rendir en la plataforma del FOR-CIC - UNIVERSITY DE BOSTON un examen de entrenamiento que comprenderá preguntas de los módulos cursados. Dicha evaluación tiene como objetivo verificar el conocimiento teórico y práctico adquirido durante el curso, asegurando que los participantes hayan internalizado los conceptos fundamentales y las técnicas avanzadas necesarias para enfrentar los desafíos en el campo de los ciberdelitos.

Certificación de Aprobación del Curso: con una calificación mínima necesaria del 80%, los estudiantes obtendrán la certificación de aprobación del curso de especialización en ciberdelitos, la cual será emitida conjuntamente por el Laboratorio de Lucha contra el Ciberdelito y Nuevas Tecnologías y el Center for Cybercrime Investigation & Cybersecurity de la Boston University, instituciones reconocidas internacionalmente por su excelencia en la formación y capacitación en seguridad digital y ciberinvestigaciones.

Importancia de la Certificación: La certificación conjunta de estas instituciones prestigiosas no sólo valida los conocimientos adquiridos por los cursantes, sino que también les brinda una credencial altamente valorada en el mercado laboral global, garantizando que los profesionales están capacitados para abordar y resolver problemas complejos relacionados con el cibercrimen, utilizando las mejores prácticas y herramientas disponibles en el ámbito internacional.

Licencia de Certificación Adicional:

Asimismo, aquellos alumnos que hayan demostrado una destreza destacable durante el curso tendrán la posibilidad de obtener una licencia de certificación adicional como Peritos Internacionales emitida por el Center for Cybercrime Investigation & Cybersecurity de la Boston University. Esta licencia adicional reconoce el alto nivel de competencia y especialización de los cursantes, permitiéndoles actuar como expertos periciales en casos de ciberdelitos a nivel global; consecuentemente su obtención no solo amplía las oportunidades profesionales de los cursantes, sino que también refuerza la misión de las instituciones certificadoras de promover la excelencia y la especialización en la lucha contra el cibercrimen.

DESTINATARIOS (CONDICIONES DE ADMISIÓN)

Esta diplomatura está dirigida a un público especializado que desempeña roles clave en el ámbito de la seguridad y la justicia. Los destinatarios principales incluyen: Agentes Encargados de Hacer Cumplir la Ley: Policías, investigadores y otros funcionarios que participan directamente en la prevención, investigación, y resolución de delitos, especialmente aquellos relacionados con la cibercriminalidad y el análisis digital.

Fuerzas de Seguridad: Miembros de fuerzas de seguridad nacionales, provinciales y locales que requieren una comprensión avanzada de las telecomunicaciones, el análisis de datos y la investigación digital para enfrentar las amenazas actuales.

Miembros del Ministerio Público: Fiscales y otros funcionarios del Ministerio Público que necesitan conocimientos específicos para solicitar, interpretar, y utilizar datos digitales y de telecomunicaciones en la preparación de casos judiciales.

Funcionarios del Poder Judicial: Jueces, secretarios judiciales, y personal técnico del Poder Judicial que deben evaluar y decidir sobre la validez y relevancia de la evidencia digital y las solicitudes de información en investigaciones penales.

Este curso proporciona las herramientas y conocimientos necesarios para enfrentar los desafíos que presenta la investigación digital en la era moderna, permitiendo a los participantes aplicar técnicas avanzadas y mejores prácticas en su trabajo diario.

CRONOGRAMA DE ESTUDIOS

Nivel	Clase - Tema	Fecha	
	APERTURA ABIERTA PRESENCIAL -Máster Class		Mgter. Rafael Garcia Borda
I	Introducción a Ciberdelitos	04/09/2025	Dr. Martin Laius
I	Delitos Informáticos	11/09/2025	Julio Perez Carreto
I	Ciberestafas y Otras defraudaciones en la Era Digital - Taller Práctico	18/09/2025	Dr. Martin Laius
I	El Delito de Grooming Material de Abuso Sexual Infantil	25/09/2025	Dr. Daniel Ichazo

I	Ciberdelincuencia y Responsabilidad Directiva en el Contexto Escolar.	02/10/2025	Dr. Christian Walter.
I	Taller Practico.	09/10/2025	Dr. Daniel Ichazo.
II	Pedidos de Información - Conocimiento de nuevas herramientas	16/10/2025	Dra. Celeste Segui y Esp. Horacio Martino
II	Requerimiento, análisis en META y herramienta I2	23/10/2025	Dra. Celeste Segui y Esp. Horacio Martino
III	Requerimiento, análisis en META y herramienta I2 OSINT (Historia, evolución, concepto, fases, fuentes de información pública y privadas, Google hacking, navegadores privados). CIberinteligencia en Telegram.	30/10/2025	Esp. Brian Arroyo
III	La Figura del Agente Revelador. Workshop práctico: resolver caso práctico (crear avatar y resolver un caso práctico).	06/11/2025	Esp. Brian Arroyo
IV	Informática Forense: Extracción de información de dispositivos móviles y discos rígidos.	13/11/2025	Perito Jonathan Bazquez
IV	Criptomonedas y Blockchain	20/11/2025	Dra. Sabrina Lamperti
V	Cripto Ac tivos y su Vinculación con la Actividad Criminal	27/11/2025	Dra Sabrina Lamperti
VI	Introducción a la Inteligencia Artificial y Protección de Datos Personales	04/12/2025	Mgters. Yamila Walter/Ing Karina Gibert-España.
VI	Lavado de activos y Criminalidad Organizada. Identificación de estructuras criminales: cárteles, redes de trata y tráfico ilícito de bienes. Estudio de un caso práctico internacional.	11/12/2025	Dr. Juan Ignacio Starcenbaum y
	EXAMEN ON-LINE EN CENTER FOR CIC BOSTON UNIVERSITY	18/12/2025	**Plataforma de Center For CIC -Boston University**
	CEREMONIA DE CLAUSURA		

CRONOGRAMA DE ESTUDIOS

FECHAS DE INICIO Y FINALIZACIÓN

Fecha de inicio: 04/09/2025.

Fecha de finalización:18 /12/2025

CRONOGRAMA DE ESTUDIOS

JUEVES : 18:00 a 20:00 hs.

APROBACIÓN DEL PROGRAMA DE ESTUDIOS

Finaliza con asistencia del 70% de asistencia y la aprobación del examen final.

CERTIFICACIONES

Laboratorio de Lucha contra el Ciberdelito y el Fortalecimiento de las Nuevas Tecnologías y Center for CIC (Center for Cybercrime Investigation & Cybersecurity-Boston University).

AUTORIDADES ACADÉMICAS

DIRECTOR: MAG. RAFAEL GARCÍA BORDA

- *Director General en ClicLex - Laboratorio de Lucha contra el Ciberdelito y Fortalecimiento de las Nuevas Tecnologías*
- *Instructor de American Bar América Bar Association Rule Of Law initiative (Colegio de Abogados de Estados Unidos) - Aba Roli Perú.*
- *Especialista en garantías constitucionales en la Investigación y de la prueba en el proceso penal en la Universidad de Toledo, España*
- *Experto en Informática Forense UTN-FRA*
- *Magister en Ciberseguridad en el Centro de Posgrado Europeo | Coordinador del Equipo Especializado en la Investigación de Cripto-Activos, Procuración General Suprema Corte de Justicia de la Provincia de Buenos Aires.*
- *Consultor Externo en OIT (Organización Internacional del Trabajo dependiente de Naciones Unidas). K-Builder Center for Cibercrime Investigation and Cybersecuirity in Boston University.*
- *Experto en Sistema de Seguridad de la Información en Centro Europeo de Posgrado. –*

Trayectoria **Profesional:**

- Director General en **ClicLex** - Laboratorio de Lucha contra el Ciberdelito y Fortalecimiento de las Nuevas Tecnologías.
- Instructor en la **American Bar Association Rule of Law Initiative** (ABA ROLI, Perú).
- Coordinador del Equipo Especializado en la Investigación de Criptoactivos de la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires.
- Consultor Externo en la **Organización Internacional del Trabajo (OIT)**.
- K-Builder en el **Center for Cybercrime Investigation and Cybersecurity** en Boston University.

CO-DIRECTOR:

Formación Académica:

Trayectoria Profesional:

Experiencia Docente y Formación Complementaria:

- .

PRESENTACIÓN CUERPO DOCENTE

Dr. Martín Hugo Laius

- **Formación Académica:**
  - Abogado, egresado de la Escuela Judicial de la Suprema Corte de Justicia de la Provincia de Buenos Aires.
- **Trayectoria Profesional:**
  - Agente Fiscal de la Unidad Funcional de Instrucción N.º 8 del Departamento Judicial de Junín.
  - Secretario de Primera Instancia en la Unidad Fiscal de Investigación para la causa AMIA.
  - Co-director de la Diplomatura de Posgrado en Cibercrimen y Evidencia Digital.
- **Especialidades:**
  - Derecho Penal.
  - Cibercrimen y Evidencia Digital.
- **Experiencia Docente:**
  - Profesor de grado y posgrado.
- Profesor de grado y posgrado.

Dr. Julio Pérez Carreto

- **Cargo Actual:** Fiscalía Especializada de San Nicolás.
- **Especialidades:** Criminología, Cibercrimen y Evidencia Digital.
- **Trayectoria Destacada:**

- Coordinador de la Secretaría Especializada en Cibercrimen y Evidencia Digital del Ministerio Público Fiscal de la Provincia de Buenos Aires.
- Referente provincial en investigaciones digitales ante la Procuración General de la Provincia de Buenos Aires.
- Miembro del Equipo de Investigaciones en Criptoactivos.

- **Experiencia Docente:**
  - Profesor de Derecho Penal Parte Especial en la Universidad Nacional de Rosario.
  - Docente de posgrado en la Diplomatura Universitaria en Cibercrimen e Investigación Penal en Medios Digitales (Universidad Nacional del Noroeste de Buenos Aires).

Dr. Ernesto Daniel Ichazo

- **Cargo Actual:** Agente Fiscal del Departamento Judicial Quilmes.
- **Especialidades:** Cibercrimen, Trata de Personas, Grooming y Material de Abuso Sexual Infantil.
- **Trayectoria Destacada:**
  - Titular de la Fiscalía Especializada en Cibercrimen.
  - Coordinador de las Fiscalías Descentralizadas de Berazategui.

Experiencia Docente: Profesor de grado y posgrado.

Dr. Christian Walter.

- **Cargo Actual**: Director de Escuela Guilford County Schools, Carolina del Norte (EE.UU)
- **Especialidades:**

• Especialista en Educación (Ed.S). East Carolina University
• Doctor en Educación. East Carolina University.
• Prevención del ciberdelito en el ámbito escolar

Trayectoria Destacada:

- Presentador para el Departamento de Educacion de Carolina del Norte.
- Especialista del Programa TESOL, Guilford County Schools

Dra. Sabrina Lamperti

- **Cargo Actual:** Prosecretaria del Departamento de Ciberdelitos y Tecnologías Aplicadas de la Procuración General de la Provincia de Buenos Aires.
- **Especialidades:** Criminalidad Económica y Ciberdelitos.
- **Trayectoria Destacada:**
  - Miembro del Grupo de Referentes de Investigaciones Digitales.
  - Investigadora académica en el InFo-Lab.
  - Capacitadora y coautora de textos académicos.

Experiencia Docente: Participación como docente invitada en universidades nacionales e internacionales.

Dra. María Sol Cinosi

- **Cargo Actual:** Secretaria en la Fiscalía de Vicente López Este del Ministerio Público Fiscal de la Provincia de Buenos Aires.
- **Especialidades:** Cibercrimen y Criptoactivos.
- **Trayectoria Destacada:**
    - Investigadora del Equipo Especializado en Criptoactivos del Departamento de Ciberdelitos.
    - Consultora independiente para la OEA.
    - Certificaciones avanzadas en investigaciones penales y criptoactivos (TRM y Chainalysis).

Mgter. Jimena Veléz

- **Cargo Actual:** Experta en Cibercrimen de la Oficina de las Naciones Unidas contra la Droga y el Delito. UNDOC.-

Dra. Gisela Burcatt

- **Cargo Actual:** Titular del Departamento de Ciberdelitos y Tecnologías Aplicadas en el Ministerio Público de Buenos Aires.

Trayectoria Destacada: Coordinadora de la UAID y el Sistema de Investigaciones Criminalísticas de la Policía Judicial del MPBA.

Horacio Martino

- **Cargo Actual:** Analista de Evidencia Digital del Ministerio Público de la Provincia de Buenos Aires.
- **Especialidades:** Análisis de evidencia digital, redes sociales y criptoactivos.

Trayectoria Destacada: Miembro del equipo interdisciplinario especializado en investigaciones digitales y criptoactivos.

Dra. María Celeste Seguí

- **Cargo Actual:** Analista de Evidencia Digital del Ministerio Público de la Provincia de Buenos Aires.
- **Especialidades:** Investigación digital, manejo de herramientas forenses y criptoactivos.

Certificaciones Destacadas: Chainalysis Reactor Certification, TRM Professional Certifications.

Mag. Yamila Walter

- **Cargo Actual:** Asesora legaltech en la Dirección de Tecnología de la AFIP.
- **Especialidades:** Derecho Digital, Derecho Administrativo, Control y Fraude Fiscal.
- **Trayectoria Destacada:**

- Jefa de Gabinete de Asesores de la Subsecretaría de Gobierno Digital de la Provincia de Buenos Aires.
- Enfoque en la Sociedad Digital e Inteligencia Artificial.

Formación Académica: Magíster en Derecho Digital.

Docente Internacional. Ingeniera Informática Karina Gibert

Catedrática de Inteligencia Artificial y exdirectora de IDEAI-UPC
Decana del Colegio Profesional de Ingeniería Informática de Cataluña (COEINF)
Catedrática en la Universitat Politècnica de Catalunya (UPC) desde hace más de 30 años. Es licenciada, máster y doctora en ingeniería informática. Cofundadora y exdirectora del Centro de Investigación en Ciencia de Datos Inteligente e Inteligencia Artificial (IDEAI-UPC). Decana de COEINF. Vicepresidenta del Consejo General de Colegios Profesionales de Ingeniería Informática de España (CCII, desde 2023). Miembro de la red europea de excelencia en IA ELLIS (desde 2023) y de su capítulo en Barcelona (desde 2024).

Su investigación se centra en la extracción de conocimiento estratégico a partir de datos y en sistemas inteligentes de apoyo a la decisión, con especial atención a la explicabilidad y la ética en la IA. Experta en la Estrategia Catalana de IA *Catalonia.ai* (Gencat, febrero de 2020), co-redactó dicha estrategia entre 2018 y 2020. Es una de las 12 líderes de CETRA, órgano asesor del Gobierno de Cataluña para la transformación de la Generalitat (2024-).

Miembro del Comité de Ética de los Datos del Gobierno de Cataluña. Miembro del consejo directivo del programa IA y Salud del Departamento de Salud de Cataluña. Miembro del consejo asesor de IA en EIT Digital (Comisión Europea), 3cat, LocalRed, Mesa del Tercer Sector, Fundación Factor Humano, entre otros.

Asesora en IA, ética y transformación digital del Senado de España (desde enero de 2021), de la Secretaría de Estado de Digitalización e IA (2023), de varios gobiernos autonómicos españoles, de la Comisión Europea (2020), de la Commonwealth (desde 2024) y del Gobierno Provincial de Buenos Aires (2025-). Consultora del Departamento de Salud Mental de la OMS (2008–2010).

Fundadora y presidenta de *donesCOEINF* (desde mayo de 2018), iniciativa para reducir la brecha de género en ingeniería informática. Fundadora y presidenta de *donesIAcat* (capítulo de género de la Asociación Catalana de Inteligencia Artificial, desde el 3 de agosto de 2019). Miembro de la Comisión de Mujeres e Igualdad de la Asociación Intercolegial (desde septiembre de 2019). Cofundadora de *Women in Computer Engineering* (CCII, desde junio de 2021).

Embajadora de WiDS-Barcelona (Stanford, desde enero de 2021). Vicepresidenta del capítulo de Barcelona de *Women in ACM* (2023-). Fundadora y directora de los programas *Top Rosies Talent* (2021-) y *ciutadania* (2021-).

Investigadora principal (IP) de la red doctoral Marie Curie *i3WaterS* (2025-) y del proyecto *TFemTIC* (2025-). IP por la UPC del programa postdoctoral COFUND *Ramon Llull* (2023-).

Impulsora y directora tecnológica del movimiento *critvirtual.com* y de las manifestaciones virtuales internacionales por las mujeres afganas (2021, 2023).

Esp. Brian Arroyo

- **Cargo Actual:** Cyber Fraud Intelligence Specialist at Banco Galicia | Cyber Threat Intelligence Consultant | Cybercrime Trainer and Researcher | Intelligence Analyst
- **Especialidades:** analista de ciberinteligencia con más de 10 años de experiencia en el campo de la investigación en ciberseguridad y cibercrimen. He colaborado y asesorado en casos de fraudes, estafas, terrorismo, homicidios, búsqueda de personas y explotación sexual infantil en línea. Además ha tenido una trayectoria destacada en la formación de otros profesionales en el área de la ciberseguridad, impartiendo cursos, charlas y conferencias en universidades nacionales y extranjeras Consultor de inteligencia y ciberseguridad para distintos organismos y empresas.

Dr. Juan Ignacio STARCENBAUM

- Abogado UBA - Orientación Penal - Diploma de Honor AÑO 2004 - Posgraduado en Prevención del Blanqueo de Dinero, Responsabilidad Penal de las Personas Jurídicas y Fraude Fiscal (Universidad Santiago de Compostela 2018) - Posgraduado en Investigaciones Penales con Cripoactivos - UBA 2023 - Posgraduado del programa ejecutivo Fintech Law, Blockchain y Criptoactivos Universidad Torcuato Di Tella 2024. Autor y colaborador en diversas publicaciones de derecho penal económico. Coordinador General de la Diplomatura Lavado de Dinero, Evidencia Digital e Inteligencia Artificial de la AMFJN. Docente de posgrado UMSA y CLICLEX. Prosecretario Administrativo en el Juzgado Nacional en lo Penal Económico Nro. 8 de la Capital Federal.

Dr. Gustavo Gustavo Darío MEIROVICH

- Juez en lo Penal Económico a cargo del Juzgado Nro.8 desde el 31/08/2009. Abogado UBA – Magíster en Derecho Penal– Universidad de Palermo - Posgrado en Especialización en Justicia Internacional y Crimen Organizado. Castilla la Mancha, Toledo, España, 2004. Director de la Diplomatura en “Lavado de dinero: prevención, investigación criminal y evidencia digital” organizada conjuntamente la Asociación de Magistrados de la Justicia Nacional (AMFJN) y la Asociación Internacional de Derecho Penal Económico y la Empresa – AIDPEE. Expositor en múltiples congresos y cursos dictados en el Paraguay, Bolivia, México y Alemania.
- Autor de diferentes publicaciones desde 2004 en materia de Sociedad de Riesgo, Ilícitos Económicos y Responsabilidad de las Personas Jurídicas, en publicaciones argentinas y españolas, y recientemente coordinador general por parte de Magistrados y funcionarios del

Poder Judicial en el marco de la jornada efectuada el 25 de agosto de 2022 por parte de la OPDAT en la residencia del Embajador de los EEUU.

- Co -director del libro “ilícitos Económicos y Evidencia Digital”, Editores 2023. Coordinador del Instituto Superior de la Magistratura en la Asociación de Magistrados y Funcionarios del Poder Judicial de la Nación.

Dr. José María Arrieta

Cargo actual: Profesor Adjunto de Derecho Penal Parte General (UNNE). Abogado en ejercicio. Formación Académica:

- Abogado (UNNE, 1992).
- Especialista en Derecho Penal (UNNE, 1997/1998).
- Maestrando en Derecho Penal (UNNE, tesis aprobada). Especialidades: Derecho Penal General y Especial, Criminología. Trayectoria destacada:
- Co-director de múltiples proyectos de extensión universitaria vinculados a derechos humanos y sistema penitenciario.
- Jurado en numerosos concursos del Consejo de la Magistratura de Corrientes, Chaco y Misiones.
- Coautor de diversas publicaciones científicas y jurídicas.
- Integrante de institutos de Derecho Penal (UNNE y Cuenca del Plata). Experiencia docente:
- Profesor en la UNNE y en la Universidad de la Cuenca del Plata.
- Docente en carreras de grado y posgrado en Derecho Penal.
- Coordinador académico y disertante en múltiples seminarios, jornadas y diplomaturas.
- Formación de recursos humanos a través de dirección de adscriptos y pasantes.