ANEXO

Diplomatura en Ciberfraude

1. Identificación de la diplomatura: Diplomatura en Ciberfraude

1.1 Carga horaria total: noventa y seis (96) horas reloj.

1.2 Modalidad de cursada: A distancia (con actividades sincrónicas y asincrónicas).

1.3 Ubicación en la estructura: Secretaría Académica - Dirección de Extensión.

1.4 Unidad académica ejecutora: Secretaría Académica - Dirección de Extensión.

2. Características:

2.1 Fundamentación:

El crecimiento sostenido de los entornos digitales, la digitalización de los sistemas financieros y la expansión del uso de criptoactivos han generado nuevas modalidades de fraude y criminalidad compleja que impactan directamente en los sistemas de seguridad, justicia y control financiero. El ciberfraude y el cibercrimen financiero constituyen hoy una de las principales amenazas para las instituciones públicas, el sector privado y la ciudadanía, requiriendo respuestas profesionales especializadas, interdisciplinarias y actualizadas.

En este contexto, la Diplomatura en Ciberfraude se propone brindar una formación universitaria orientada a la prevención, detección e investigación de fraudes digitales, integrando conocimientos jurídicos, criminológicos, tecnológicos y financieros. La propuesta articula el análisis normativo vigente, las metodologías de inteligencia de fraude, la investigación digital y el abordaje de criptoactivos, con una fuerte orientación práctica y aplicada.

La diplomatura busca fortalecer las capacidades profesionales de quienes se desempeñan o aspiran a desempeñarse en ámbitos vinculados a la seguridad, la justicia, la investigación criminal, el *compliance* y la ciberseguridad, contribuyendo al desarrollo de competencias acordes a las demandas actuales del sistema institucional y a los desafíos emergentes del delito en el ciberespacio.

2.2 Objetivos:

Objetivo General:

Brindar una formación universitaria especializada que capacite a los/as participantes en

la prevención, detección e investigación de fraudes digitales y del cibercrimen financiero, contribuyendo al fortalecimiento de las competencias profesionales requeridas en los ámbitos de la seguridad y la justicia, a través de la incorporación de conocimientos teóricos y prácticos vinculados al uso de criptomonedas, la inteligencia de fraude y la aplicación de tecnologías forenses.

Objetivos específicos:

- Analizar la legislación aplicable al ciberfraude y al cibercrimen financiero, así como el marco normativo vigente a nivel nacional e internacional.
- Identificar y analizar las principales modalidades de fraude digital, sus tipologías y métodos de ejecución en distintos entornos tecnológicos y financieros.
- Aplicar herramientas y metodologías de ciberinteligencia, inteligencia contra el fraude (*Fraud Intelligence)* y análisis forense digital en el abordaje e investigación de casos de fraude.
- Diseñar y evaluar estrategias de prevención y mitigación del fraude en entornos digitales y en sistemas financieros y transaccionales.
- Comprender el ciberfraude como una manifestación de la criminalidad compleja, reconociendo los factores criminológicos, tecnológicos y organizacionales que favorecen su comisión.
- Analizar problemáticas de territorialidad, jurisdicción y cooperación interinstitucional en las investigaciones de ciberfraude.
- Reconocer y aplicar técnicas de trazabilidad de criptoactivos y detección de operaciones sospechosas en el marco de investigaciones financieras digitales.

2.3 Requisitos de ingreso a la diplomatura:

Podrán ingresar a la Diplomatura en Ciberfraude, los graduados del nivel medio o polimodal con título de instituciones reconocidas oficialmente.

2.4 Destinatarios:

Integrantes de Fuerzas de Seguridad y Fuerzas Armadas, Magistrados, funcionarios y empleados de Poderes Judiciales y Ministerios Públicos Fiscales o de la Acusación, integrantes de Cuerpos de Investigación Judiciales o Policías Judiciales, agentes gubernamentales o personal de agencias de seguridad, auditores y especialistas en ciberseguridad y criptoactivos, personal de áreas de Seguridad, Seguridad de la Información, Prevención de Riesgos y Fraudes, y demás interesados en la temática.

2.5 Competencias, destrezas y conocimientos que genera en el estudiantado:

El egresado será capaz de:

- Aplicar estrategias sistemáticas de prevención y detección del fraude en entornos digitales y financieros.
- Utilizar herramientas y metodologías de ciberinteligencia, inteligencia contra el fraude (*Fraud Intelligence)* y análisis forense digital en procesos de prevención, detección e investigación del fraude.

  Realizar análisis forense de evidencia digital en el marco de investigaciones de fraude y cibercrimen financiero, respetando los principios técnicos, legales y procedimentales aplicables.
- Identificar, clasificar y analizar las principales modalidades y perfiles de fraude digital y cibercrimen financiero, en el contexto del sistema bancario, sistemas de pago y criptoactivos, evaluando sus métodos de ejecución, impactos y niveles de riesgo en distintos entornos digitales.
- Interpretar y aplicar la normativa nacional e internacional vigente en materia de delitos informáticos, fraude digital, prevención del lavado de activos y financiamiento del terrorismo, conforme a estándares regulatorios y buenas prácticas institucionales.
- Aplicar metodologías de trazabilidad de criptoactivos y análisis de transacciones sospechosas, conforme a estándares técnicos, regulatorios y de cooperación interinstitucional.
- Elaborar informes técnicos y analíticos, integrando conocimientos técnicos y jurídicos, para asesorar y colaborar con organismos de seguridad, justicia y entidades financieras, actuando con criterios éticos y responsabilidad profesional.

3.Organización de la Diplomatura

3.1 Organización general

N°	Espacio curricular	Carga horaria por materia
1	Marco Jurídico y Normativo del Ciberfraude e *Inteligencia contra el fraude (Fraud Intelligence)*	12
2	Introducción al Ciberfraude e *Inteligencia contra el fraude* (*Fraud Intelligence)*	12
3	Cyber-*Fraud Intelligence* y su aplicación en la Prevención de Fraude	9
4	Criptoactivos	21
5	Evidencia Digital	6
6	Investigación del Ciberfraude	12
7	Seminarios de Actualización Profesional y Casos Aplicados	24
CARGA HORARIA TOTAL		**96 horas**

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

3.2 Contenidos Mínimos:

- **Marco Jurídico y Normativo del Ciberfraude e Inteligencia contra el Fraude (*Fraud Intelligence).***

Legislación Aplicable al Ciberfraude. Normativa nacional e internacional sobre delitos informáticos. Regulaciones sobre ciberfraude y fraude financiero. Responsabilidad penal y civil en delitos informáticos. Responsabilidad de las entidades. Cooperación internacional en la lucha contra el ciberfraude. Principales desafíos jurídicos en la prevención del fraude digital.

Tipificación Legal de conductas involucradas en el Ciberfraude. Acceso no autorizado a sistemas informáticos. Robo. Daño Informático. Daño informático agravado. Fraude. Fraude Informático. Uso de datos de tarjetas por robo, hurto o perdida. Manipulación informática. Uso ilegítimo de documento de identidad. Suplantación de Identidad Digital. Cuestiones de Tipificación. Concurso de delitos. Jurisprudencia.

Regulación de Criptoactivos y *Compliance*. Normativa Nacional sobre Criptoactivos. Regulaciones en Argentina sobre el uso de criptomonedas. Leyes aplicables a la fiscalización de criptoactivos. Marco jurídico sobre el lavado de activos y financiamiento

del terrorismo con criptomonedas. Normativa Internacional sobre Criptoactivos. Regulaciones en la Unión Europea, Estados Unidos y otros países. Tratados y acuerdos de cooperación internacional sobre criptoactivos. Normativas y Organismos de Regulación. Grupo de Acción Financiera Internacional (GAFI). Travel Rule y estándares para prevenir el lavado de dinero con criptoactivos. Comisión Nacional de Valores(CNV): Regulaciones sobre criptoactivos como valores negociables. Unidad de Información Financiera (UIF): Reportes de operaciones sospechosas y obligaciones de *compliance* para exchanges y entidades financieras. Banco Central y reguladores financieros: Supervisión del ecosistema cripto en el ámbito bancario y financiero.

- **Introducción al Ciberfraude e Inteligencia contra el Fraude (*Fraud Intelligence)*.**

Conceptos clave de ciberfraude y *Fraud Intelligence*. Definición de ciberfraude: diferencias con otros delitos informáticos. Evolución del ciberfraude: cómo han cambiado las tácticas y los actores. Tendencias actuales: qué tipos de fraudes están en auge y por qué. Inteligencia contra el Fraude (*Fraud Intelligence)*: definición y su papel en la prevención y detección del fraude. Evolución de la Inteligencia contra el Fraude (*Fraud Intelligence)*: de la detección reactiva a la predicción proactiva. Tendencias actuales en Inteligencia contra el Fraude (*Fraud Intelligence)*: integración con inteligencia artificial, big data y machine learning.

Métodos de fraude más usados en el ecosistema digital. Ataques dirigidos vs. ataques masivos: enfoque individualizado vs. automatización del fraude. Uso de técnicas avanzadas: deepfake, inteligencia artificial y automatización del fraude. Fraudes en redes sociales y mensajería instantánea: cómo los ciberdelincuentes se adaptan a los hábitos digitales. Explotación de vulnerabilidades humanas y técnicas: combinación de ingeniería social y exploits tecnológicos.

Análisis técnico y práctico de las modalidades de fraude.Fraude de inversión: esquemas Ponzi digitales y señales de alerta. Business Email Compromise (BEC): cómo se ejecuta técnicamente un ataque BEC. Phishing y ataques de ingeniería social: detección de intentos de phishing con herramientas forenses. Ataques a sistemas de pago: fraudes en billeteras virtuales y manipulación de transacciones. Rol de los bancos, proveedores de servicios de pago, proveedores de servicios activos virtuales, procesadores de pago. Alertas tempranas. Malware financiero: detección y mitigación de troyanos bancarios y ransomware. Robo de credenciales y SIM swapping: prevención y detección temprana. Ransomware y suplantación de identidad: estrategias de mitigación y respuesta.

Casos de estudio y análisis de ciberfraudes recientes. Análisis de fraudes financieros internacionales recientes. Cómo se investigaron y qué técnicas se usaron para

descubrirlos.

- **Ciberinteligencia contra el Fraude (Cyber-*Fraud Intelligence)* y su aplicación en la prevención de Fraude.**

Conceptos básicos del Ciberespacio. ¿Qué es el ciberespacio y cómo funciona?
Elementos clave del entorno digital y su impacto en la seguridad. Tipos de amenazas digitales que facilitan el fraude.
Fundamentos de Ciberseguridad. Definición de ciberseguridad y sus principios básicos. Diferencia entre seguridad informática y ciberseguridad.
Introducción a la Ciberinteligencia. Definición de ciberinteligencia y su uso en seguridad digital. Métodos básicos de recolección de información en investigaciones de fraude. Uso de la ciberinteligencia para la detección de fraudes.
Principios de la Prevención del Fraude en Entornos Digitales. Diferencia entre prevención y detección de fraude. Métodos tradicionales de prevención vs. enfoques modernos.
Análisis de Datos como Herramienta en la Detección del Fraude. ¿Por qué es importante el análisis de datos en la prevención de fraude? Uso básico de patrones de comportamiento en fraudes digitales. Introducción a la correlación de datos en investigaciones.

- **Criptoactivos.**

Introducción a los Criptoactivos. Definición y características principales. Diferencias entre criptoactivos, monedas virtuales y activos digitales. Usos y aplicaciones en el ecosistema financiero y tecnológico.
Tipología de Criptoactivos. Criptomonedas: Bitcoin, Ethereum y otras altcoins. Tokens: clasificación y funciones. Stablecoins y su rol en la economía digital. Tokens no fungibles (NFTs) y su impacto en el mercado digital.
Blockchain y su Funcionamiento. Concepto de cadena de bloques. Estructura y funcionamiento de un bloque. Diferencias entre blockchain pública, privada e híbrida. Smart Contracts: definición y aplicaciones.
Finanzas Descentralizadas (DeFi) y su Impacto. ¿Qué es DeFi y cómo funciona? Plataformas y protocolos más utilizados. Riesgos en los protocolos DeFi: vulnerabilidades, hacks y fraudes. Estafas y rug pulls en DeFi: casos de estudio. Riesgos Asociados a los Criptoactivos. Investigacion de maniobras asociadas al Lavado de dinero y financiamiento del terrorismo mediante criptoactivos. Fraudes y estafas con criptomonedas. Ransomware y ciberataques relacionados con criptoactivos. Métodos de anonimización y técnicas de ofuscación en transacciones.
Investigación Digital y Evidencia Digital en Criptoactivos. Metodologías, técnicas y

herramientas de investigación digital. Adquisición, tratamiento y análisis forense de evidencia digital. Métodos de análisis de transacciones en blockchain. Identificación de wallets y rastreo de fondos. Herramientas OSINT para análisis de blockchain. Casos de estudio sobre investigaciones en criptoactivos.

Compliance en Criptoactivos. Enfoques de cumplimiento: prevención de lavado (AML) y financiamiento del terrorismo (CFT). KYC (Know Your Customer) y KYT (Know Your Transaction) aplicados a plataformas cripto. Travel Rule del GAFI: implicancias y adopción en Argentina. Heurísticas de riesgo, machine learning y alertas transaccionales. Responsabilidades de los Proveedores de Servicios de Activos Virtuales (VASP). Detección de operaciones sospechosas en exchanges y billeteras descentralizadas

Prácticas en Investigación de Criptoactivos. Simulación de trazabilidad de transacciones. Uso de herramientas para seguimiento de fondos. Análisis de casos reales con herramientas especializadas. Ejercicios de identificación de wallets y detección de actividades ilícitas.

- **Evidencia Digital.**

Definición y características de la evidencia digital. Volatilidad. Escena del hecho digital. Importancia de la cadena de custodia. Buenas prácticas en la recolección y almacenamiento de evidencia. Protocolos de actuación. Métodos de Adquisición de Evidencia Digital. Tipos de adquisición. Herramientas forenses. Extracción de datos desde dispositivos móviles y sistemas de almacenamiento. Herramientas y técnicas para el análisis preliminar de evidencia. Casos de uso en investigaciones de fraude y delitos digitales. Análisis de la Evidencia Digital. Identificación y clasificación de archivos relevantes. Técnicas básicas de recuperación de datos. Metadatos y su importancia en investigaciones.

- **Investigación del Ciberfraude.**

Colaboración Público-Privada y Flujo de Información. Estrategias investigativas en el marco de un proceso penal. Modelos de cooperación interinstitucional. Accesos a base de datos, pedidos de información y protocolos de urgencia. Matrices. Automatización por IA de procesos de análisis. *Compliance* financiero (Bancos tradicionales).

Técnicas y herramientas para la trazabilidad del dinero. Mapeo de flujos financieros en entornos tradicionales y digitales. Herramientas de visualización de operaciones (Chainalysis, Merkle Science, TRM Labs). Integración de bases de datos de transacciones y análisis de estructuras transaccionales. Identificación y perfilamiento de cuentas “mulas” y estructuras de lavado.

Medidas judiciales y cautelares. Bloqueo preventivo de fondos: fundamentos y criterios

de urgencia. Embargos sobre cuentas digitales y activos en plataformas. Levantamiento del secreto bancario y fiscal. Medidas cautelares en ambientes virtuales: desafíos técnicos y jurídicos. Aplicación de técnicas procesales especiales de investigación. Cuestiones de competencia y territorialidad frente al ciberfraude. Reversión de fondos Análisis criminal aplicado al Ciberfraude. Investigacion. Particular y en Conjunto. Modelo SARA. Técnicas de perfilamiento de estructuras criminales financieras. Integracion de las distintas líneas de investigación. Como elaborar matrices de investigación. Análisis de patrones de fraude en delitos complejos y organizados.

- **Seminarios de Actualización Profesional y Casos Aplicados.**

Se dictarán seminarios con un enfoque netamente práctico que permita vincular y entender la teoría con la realidad desde el punto de vista de los distintos actores involucrados en la temática, quienes serán los expositores a cargo de los mismos.

- **Seminario I: Abordaje de víctimas desde la Justicia.** Análisis del rol del sistema judicial en la atención y protección de las víctimas de ciberfraude, abordando buenas prácticas en la toma de denuncias, la contención institucional, la comunicación clara del proceso judicial y la articulación con otros organismos. La figura del querellante, su rol dentro del proceso penal, su intervención en la producción de prueba y el impulso de la investigación. La instancia civil vinculada al ciberfraude, analizando las acciones civiles derivadas del delito, los mecanismos de reparación del daño, la responsabilidad civil de los distintos actores intervinientes y la articulación entre los procesos penal y civil.
- **Seminario II: Organismos reguladores y control de fraude.** El rol del Banco Central de la República Argentina (BCRA). Sistema Nacional de Pagos: su marco normativo, los esquemas de pagos mayoristas y minoristas, y los mecanismos de control aplicables a la prevención del fraude en el ámbito bancario y de los sistemas de pago. Asimismo, se estudiará la función de la Comisión Nacional de Valores (CNV) y de la Unidad de Información Financiera (UIF) en la prevención, supervisión y control del fraude financiero y del lavado de activos, así como su articulación con el sistema judicial y las fuerzas de seguridad en el marco de investigaciones complejas.
- **Seminario III: Cámaras Compensadoras y sistemas de pago.** Estudio del funcionamiento del sistema de compensación electrónica en Argentina. Las cámaras compensadoras en el sistema financiero argentino. COELSA y su función en la compensación electrónica, trazabilidad de transferencias y detección de operaciones sospechosas. Funcionamiento de las redes LINK y BANELCO, su participación en los sistemas de pagos mayoristas y minoristas, los flujos operativos asociados a transferencias, extracciones y pagos con tarjeta, y su relevancia en la investigación del

ciberfraude y en los requerimientos judiciales vinculados a la reconstrucción del circuito del dinero.

- **Seminario IV: Proveedores de Servicios de Pago (PSP) y pasarelas de pago** Análisis del rol de los PSP en el ecosistema de pagos digitales, su participación en el movimiento de fondos, los mecanismos de prevención de fraude, los sistemas de monitoreo transaccional y su interacción con entidades bancarias y autoridades regulatorias.
- **Seminario V – Banca digital y banca tradicional: responsabilidades y desafíos.** Comparación entre banca digital y banca tradicional, con especial atención a las responsabilidades de las entidades financieras, los estándares de seguridad, los deberes de prevención del fraude y el rol de asociaciones de bancos públicas y privadas en la articulación institucional.
- **Seminario VI – Empresas Fintech y billeteras virtuales:** Análisis del funcionamiento de las fintech y las billeteras virtuales, sus modelos de negocio, riesgos asociados al fraude digital, mecanismos de control interno, cumplimiento normativo y cooperación con organismos de control y fuerzas de investigación.
- **Seminario VII – Plataformas de compra, pago y comercio electrónico** Estudio del funcionamiento de las plataformas de compra y pago en línea, los principales esquemas de fraude asociados al comercio electrónico, los mecanismos de prevención y detección, y la cooperación público-privada en investigaciones de ciberfraude.
- **Seminario VIII – Empresas de telecomunicaciones y su rol en el ciberfraude** Empresas de telecomunicaciones en la prevención e investigación del ciberfraude, incluyendo la gestión de líneas telefónicas, fraudes vinculados a SIM swapping, preservación de datos, requerimientos judiciales y colaboración interinstitucional.

4. Metodología

Se desarrollarán diversas estrategias metodológicas a través de la combinación de clases expositivas con espacios interactivos, debates, reflexiones y tutorías a lo largo del cursado, a efectos de lograr un aprendizaje activo mediante trabajos prácticos, análisis de casos, talleres y resolución colaborativa de problemas.

5. Evaluación y aprobación:

Se deberá cumplimentar con el setenta y cinco por ciento (75%) de asistencia y la aprobación de las instancias evaluativas, conforme a la descripción incluida en los programas de las asignaturas, y según el marco normativo de la institución.

6. Certificación a otorgar

El IUSE otorgará la Microcertificación: Diplomado en Ciberfraude acreditando noventa y seis (96) horas reloj, a quienes cumplan con los requisitos de aprobación.

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
Anexo

Número: IF-2026-09458061-GCABA-SAIUS

Buenos Aires, Viernes 20 de Febrero de 2026

Referencia: Anexo- Plan de estudios Diplomatura en Ciberfraude

---

El documento fue importado por el sistema GEDO con un total de 10 pagina/s.

Digitally signed by Comunicaciones Oficiales
Date: 2026.02.20 15:32:46 -03:00

Nessi Alan Martin
Secretario Academico
SECRETARIA ACADEMICA IUS
AREA JEFE DE GOBIERNO

Digitally signed by Comunicaciones Oficiales
Date: 2026.02.20 15:32:45 -03:00