a) **Denominaciónn**

Diplomatura Universitaria de Estudios Avanzados en Cibercrimen, Evidencia Digital y Tecnologías Emergentes

b) **Destinatarios (enunciar el perfil del postulante)**

Abogados, licenciados en informática, sistemas o en ciberseguridad ya sea que se desempeñen en el ámbito privado o como empleados, funcionarios o magistrados del poder judicial o de los ministerios públicos, miembros de fuerzas de seguridad y/o cuerpos de investigación, que estén interesados en profundizar conocimientos sobre cibercrimen y adquirir habilidades para la obtención, tratamiento y litigación con evidencia digital.

c) **Requisitos de ingreso (estudios primarios/ secundario/pregrado/grado/ posgrado, formación en área específica, etc)**

Contar con título de abogado o título universitario de grado o de nivel superior no universitario de cuatro (4) años de duración como mínimo, para los postulantes de carreras afines.
Asimismo, dado que la diplomatura tiene una modalidad de dictado parcialmente virtual, los postulantes deberán contar con dispositivos adecuados (con cámara y micrófono) y buena conectividad.

d) **Objetivos**

Objetivo General
Formar profesionales con competencias teóricas y prácticas para investigar y litigar en materia de ciberdelincuencia y delitos vinculados con entornos digitales, con capacidad para intervenir en la obtención, preservación, análisis y valoración de evidencia digital, en el marco del ordenamiento jurídico vigente y con fundamento en principios éticos y de derechos humanos.
Objetivos específicos
Resultados de aprendizaje
Al finalizar la diplomatura, las personas estarán en condiciones de:
- Analizar y calificar jurídicamente conductas constitutivas de ciberdelincuencia conforme al derecho penal argentino y a los instrumentos internacionales aplicables, identificando problemas de subsunción normativa y nuevas modalidades delictivas en entornos digitales.
-Interpretar y aplicar principios del derecho procesal penal vinculados con la obtención, aseguramiento e incorporación de prueba digital, evaluando su adecuación a las garantías constitucionales y a la jurisprudencia relevante.
-Identificar y valorar evidencia digital pertinente en un caso concreto, determinando métodos adecuados para su preservación, análisis e incorporación al proceso judicial.

-Diseñar estrategias de investigación en entornos digitales, seleccionando técnicas y herramientas apropiadas según las características del caso.

-Elaborar estrategias de argumentación jurídica para la presentación, admisibilidad y valoración de prueba electrónica, incluyendo la identificación y fundamentación de planteos de nulidad.
-Analizar críticamente problemáticas vinculadas con tecnologías emergentes, tales como criptoactivos, inteligencia artificial, protección de datos personales y violencia digital, a la luz del marco normativo vigente y su impacto en los derechos humanos.

e) **Justificación**

En las últimas dos décadas, las tecnologías de la información y la comunicación (TIC) han transformado por completo la forma en que las personas se comunican entre sí y la forma en que almacenan, acceden y comparten información. La creciente digitalización de la vida cotidiana tiene muchas ventajas y, por lo tanto, a menudo se considera una evolución positiva. Sin embargo, el uso generalizado de estas tecnologías se ha convertido en una oportunidad para la proliferación del delito sin precedentes, lo que se ha visto materializado con la creciente complejidad de los delitos informáticos y el aumento exponencial de los delitos convencionales cometidos en entornos digitales. Asimismo, la evidencia digital se ha convertido en un componente clave de cualquier proceso judicial, desplazando a los medios de prueba tradicionales y requiere, para su obtención, tratamiento y valoración judicial, de conocimientos y habilidades específicas.
Ello demanda la formación de profesionales expertos en dichos aspectos que, desde los diferentes lugares que ocupen en el marco de un proceso judicial, puedan contribuir al correcto funcionamiento del servicio de justicia.

f) **Pertinencia respecto a la/s unidad/es académica/s o área central que la propone**

El cibercrimen y la evidencia digital han comenzado desde hace unos años a incluirse en la currícula de grado, mediante la incorporación de algunos de sus tópicos en asignaturas troncales como derecho penal II y derecho procesal civil, laboral, penal, etc así como también mediante asignaturas opcionales como cibercrimen, entre otros.
Asimismo, desde el área de posgrado en otras instituciones universitarias públicas se han llevado a cabo distintas propuestas de formación vinculadas con la temática, tales como las propuestas de posgrado de la UBA (Programa de Actualización en Cibercrimen y evidencia digital, Especialización en cibercrimen y evidencia digital) con excelentes resultados.
A nivel laboral, existe una gran demanda de profesionales capacitados en cibercrimen y evidencia digital, tanto en estudios jurídicos (asesoramiento de clientes afectados como imputados o víctimas a algún proceso vinculado a la temática o donde se procure presentar o litigar con evidencia digital) a empresas (para áreas de compliance, por ejemplo) como en instituciones públicas (poder judicial, agencias gubernamentales, etc.).
Si bien la diplomatura es interdisciplinaria, la formación tiene una base esencialmente jurídica.
La diplomatura diversifica la oferta académica y viene a cubrir una demanda disciplinar no cubierta en las instituciones locales con profundidad.

g) **Estructura (módulos, unidades). Carga horaria por módulos o por unidad. Metodología**

La diplomatura se compone de 5 módulos y dos seminarios específicos a elección del alumno según su perfil e intereses particulares.

Los módulos 1 y 2 tienen una carga horaria de 30 horas totales (20 horas de cursado y 10 horas de trabajo autónomo).
Los módulos 3 y 4 tienen una carga horaria de 24 horas totales (16 horas de cursado sincrónico y 8 horas de trabajo autónomo).
El módulo 5 tiene una carga horaria de 22 horas totales (16 horas de cursado sincrónico y 4 horas de trabajo autónomo).
Cada seminario específico tiene una carga horaria de 11 horas totales (8 horas de cursado y 3 horas de trabajo autónomo).
El dictado de los distintos módulos y seminarios será presencial en aula física y/o mediante plataforma Meet o similar.
La metodología de dictado se estructura a partir de la combinación de diversas estrategias didácticas activas, promoviendo la interacción con docentes y entre participantes, mediante actividades grupales e individuales, promoviendo la reflexión crítica, la construcción e integración de conocimientos provenientes tanto del derecho como de diversas áreas tecnológicas vinculadas por la temática. Cuenta con clases expositivas, participativas, que incentiven la interacción entre docentes y alumnos, así como también la lectura y análisis crítico de normativa nacional e internacional,se prevé la utilización de técnicas y sistemas de investigación en entornos digitales en el aula, estudios de casos y prácticas vinculadas con estrategias de litigación. Se utilizan guías de trabajo para realizar tareas en equipo, simulación de debates que promueven la aplicación práctica de conocimientos sobre interpretación normativa, argumentación jurídica y litigación oral. Se emplearán diversas herramientas propias de los entornos digitales que complementan el desarrollo de la actividad práctica y promueven la participación activa de los participantes.

h) **Contenidos de cada unidad o módulo**

Módulo 1: Derecho Penal Sustantivo vinculado al cibercrimen. Ley 26.388 y Convención de Budapest contra el Cibercrimen. Primer Protocolo Adicional al Convenio sobre penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Convención de Naciones Unidas contra la Ciberdelincuencia. Análisis dogmático de las principales figuras reguladas en el código penal argentino: Delitos contra la integridad sexual en entornos digitales (abuso sexual, grooming, sextorsión, ofrecimiento y distribución de imágenes relacionadas con abuso y explotación sexual infantil, etc.). Delitos contra la intimidad (acceso ilegítimo a sistemas y datos informáticos. Publicación indebida de comunicaciones electrónicas, etc.). Delitos contra el patrimonio (nuevas modalidades de estafa, uso no autorizado de tarjetas y claves falsas o sustraídas o de sus datos, fraude informático, daño informático, etc.) . Problemas de subsunción normativa. Nuevas modalidades de comisión delictiva de delitos tradicionales. Derecho comparado. Análisis de jurisprudencia nacional e internacional. Nuevas conductas no contempladas en el Código Penal.
Módulo 2: Derecho Procesal Penal aplicado al cibercrimen y la evidencia digital. Marco legal argentino e internacional. Garantías constitucionales y nuevos medios de prueba. Principio de libertad probatoria y Principio de nulla coactio sine lege. Aseguramiento y retención de datos. Tipos de datos. Registro y secuestro de datos. Interceptación de datos. Obtención de datos alojados en el extranjero. Allanamiento remoto. Jurisprudencia local y extranjera.
Módulo 3: Evidencia digital e informática forense. Herramientas. Análisis de dispositivos. Técnicas de recuperación de datos. Triage.

Módulo 4: Técnicas de investigación en entornos digitales. OSINT. Medios especiales de investigación. Ciberseguridad y gestión de incidentes. Protocolos. Respuesta ante ataques. Protección de infraestructuras.
Módulo 5: Litigación oral y prueba electrónica. Cadena de custodia. Solicitud. Admisibilidad. Presentación. Valoración. El rol del perito informático. Planteos de nulidad.
Seminarios (el estudiante debe optar por dos de cuatro alternativas):
- Criminalidad económica y nuevas tecnologías. Estructura de Blockchain, criptoactivos, trazabilidad, fraudes digitales y otros delitos vinculados con activos virtuales.
- Violencia de género en entornos digitales. Modalidades de violencia. Marco normativo. Ley Olimpia. Supresión de contenidos ante ESP.
- Inteligencia Artificial. Algoritmos, sesgos, uso de IA en investigaciones. Software de policía predictiva. Software de gestión de casos y soporte de decisiones. IA en la función judicial.
- Protección de datos personales. Categorías. Convenio 108+ del Consejo de Europa. Ley 25.326. Decreto N° 1558/01. GDPR. Programas de compliance.

i) **Modalidad de cursado**

Presencial en aula física y por Meet o plataforma similar, una vez por semana.

j) **Cronograma de dictado y Carga horaria total expresada en horas y créditos (CRE)**

MÓDULO	**HORAS DE INTERACCIÓN PEDAGÓGICA**	**HORAS DE TRABAJO AUTÓNOMO**
I	**20**	**10**
II	**20**	**10**
III	**16**	**8**
IV	**16**	**8**
V	**16**	**4**
SEMINARIO 1	**8**	**3**
SEMINARIO 2	**8**	**3**

Horas de interacción pedagógica: 104.
Horas de trabajo autónomo: 46.
Carga horaria total: 150 horas totales. 6 CRE.

k) **Nómina de equipo directivo y de docentes y CV nominal de cada uno**

Apellido/s	Nombre/s	DNI	Email	Cargo docente en la UNC (si corresponde)	Función en la Diplomatura
Pilnik	Franco	26.313.280	franco.pilnik@unc.edu.ar	Profesor UNC	Codirector y **docente a cargo de módulo 3.** Docente de módulo 2.
Vergara	María Victoria	28.270.679	victoria.vergara@unc.edu.ar	Profesor UNC	Codirectora y **docente a cargo de módulo 1.** Docente de módulo 2.
Arocena	Gustavo	22.561.159	gustavo.alberto.arocena@unc.edu.ar	Profesor UNC	Miembro de Comisión Académica y docente de módulo 1
Hairabedián	Maximiliano	20.345.894	maxihairabedian@yahoo.com.ar	Profesor UNC	Miembro de Comisión Académica y docente de módulo 2
Salt	Marcos	16.037.555	salt@fibertel.com.ar	Profesor UBA y profesor UNC	Miembro de Comisión Académica y **docente a cargo de módulo 2**
Cafferata Nores	José	7.987.656	cafferatajose@gmail.com	Profesor UNC	Docente de módulo 2
Daglio	Alejandra	25.557.389	daglioalejandra@gmail.com	Profesor UBA	Docente módulo 1
Vezzaro	Eugenio Darío	18158009	dariovezzaro@hot	Profesor UNC	Docente módulo 1

			mail.com.ar		
Cornejo	Sofía	23.147.988	sofiacornejosola@gmail.com	Profesora Universidad Católica de Salta (UCASAL)	Docente de módulo 1
Azzolin	Horacio	23.249.456	HAzzolin@mpf.gov.ar	Profesor UBA	Docente módulo 2
Pasqualli	Luciano	30.968.773	lucianopasquali@gmail.com	Especialista informático	Docente módulo 4 (apertura de celulares)
Winkler	Eduardo	21.812.422	eduardowinkler@gmail.com	Profesor Universidad Nacional Scalabrini Ortiz (UNSO)	**Docente a cargo de módulo 4** (OSINT)
Dutra	Enrique	18.573.415	edutra@puntonet.tech	Especialista en ciberseguridad	Docente invitado módulo 4 (ciberseguridad)
Castellucci	Ailin	40.649.104	castelluccciailin@gmail.com	Profesor invitado de UBA	Docente módulo 4 (ciberseguridad)
Rossi	Ivana	29.207.208	ivirossi@gmail.com	Profesor UNC	**Docente a cargo de módulo 5**
Soria	Patricia	14.377.590	patricia.soria@gmail.com	Profesor UNC	Docente módulo 5.
Martel Seward	Alfonso	35.272.035	alfonsomartel@gmail.com	Profesor UBA y UTDT	Docente (seminario cripto)

Blanco	Hernán	23.086.595	hernanblanco72@gmail.com	Profesor UBA, UTN, - Universidad de San Isidro - Unniversidad Kennedy - Universidad de Seguridad Marítima de la Prefectura Naval Argentina.	**Docente a cargo de seminario cripto**
Gershanik	Martín	25.769.471	martin.gershanik@gmail.com	Profesor UBA	docente seminario cripto
Brugge	Juan	16.157.274	juan.brugge@unc.edu.ar	Profesor UNC	**Docente a cargo de seminario Datos Personales**
Godoy Luque	Manuel	31.921.910	godoyluque@gmail.com	Profesor UNC	Docente seminario datos personales
Reale	Julián	37.896.954	julireale@gmail.com	Profesor UBA	Docente seminario datos personales
Díaz Dávila	Laura	14.366.049	laura.diaz@unc.edu.ar	Profesor UNC	**Docente a cargo de seminario IA**
Correa	Ana	20.009.927	correa.anae@gmail.com	Profesor UBA	**Docente a cargo de seminario Violencia de Género Digital**

l) **Modalidades de evaluación (parcial y final)**

Las modalidades de evaluación varían conforme el módulo que se trate. En los casos de módulos estrictamente jurídicos y teóricos consistirá en un examen de desarrollo o de respuestas de opción múltiple, mientras que en los casos de módulos técnicos consistirá en la realización de un trabajo práctico o de aplicación de conocimientos.

El examen final consistirá en un trabajo final integrador de conocimientos, que adoptará la modalidad de caso práctico donde el participante deberá responder a diversas preguntas vinculadas con la tipificación de la conducta, la identificación de evidencia digital útil para el caso y la selección de métodos de incorporación

y gestión de la evidencia, formas de presentación de la evidencia, identificación de resoluciones que ameriten planteos de nulidad u oposiciones y potenciales respuestas a los mismos.

m) **Requisitos de aprobación**

El alumno deberá cumplir con un 80% de asistencia, aprobar los exámenes correspondientes a cada módulo con nota 7 (siete) o superior (pudiendo ser exámenes teóricos o elaboración de trabajos prácticos) y, para su aprobación final, deberán aprobar con nota 7 o superior un trabajo final integrador de conocimientos, con formato de caso práctico.

n) **Bibliografía (incluir material postpandemia y enlaces digitales a contenidos de código abierto)**

Artículos de doctrina:

- Moneva Pardo, Asier, "Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1ª) 301/2016, de 12 de abril [ROJ: STS 1487/2016] Abusos sexuales a menor de trece años. Infracción de ley. No es necesario el contacto físico", *AIS: Ars Iuris Salmanticensis*, *4*(2), pp. 273–275.

-Posada Maya, Ricardo, El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual, *Revista Nuevo Foro Penal* ,Vol. 13, No. 88, enero-junio 2017, pp. 72-112. Universidad EAFIT, Medellín.

-García García-Cervigón, Josefina, El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico, *icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, nº 74, mayo-agosto 2008, pp. 289-308.

-Miró Linares, Fernando, La respuesta Penal al Ciberfraude. Especial atención a la responsabilidad de los muleros del phishing, *Revista Electrónica de Ciencia Penal y Criminología,* RECPC 15-12 (2013).

-Ortiz Pradillo, Juan Carlos. Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos

- Linares María Belén, Delitos informáticos en el Código penal argentino, REVISTA CHILENA DE DERECHO Y CIENCIA POLÍTICA, diciembre 2020, e-ISSN 0719-2150,VOL. 11, No 2. Págs 122-144.

Jurisprudencia:

"Villarroel, Oscar Alberto" Cam. Acus., Auto N° 447 del 1/11/2021.

"Aragón, Raúl Federico y otros p.ss.aa. asociación ilícita" Cam. Acus. A N° 549 del 16/12/2021.

"Dávila Marcos José" TSJ Sala Penal S. N° 122 del 19/08/2018.

"Torres, Carlos Javier", TSJ, Sala Penal, S. N° 63 del 27/03/2023.

"Quilpidor, Armando Andrés" Cam. Acus. A. N° 332 del 08/09/2020.

"Russo, Ricardo Alberto Guillermo s/ art. 128, CP" Juzg. de 1° instancia en lo Penal, Contravencional y de faltas N° 6 C.A.B.A. S. DEB 33010/2018-8 del 06/11/2019.

"Carignano, Franco Daniel p.s.a. producción de imágenes pornográficas de menores de 18 años, etc." TSJ, Sala Penal, S. N° 203 del 28/07/2020.

"N.N. s/violación sist. informático art. 153 bis 1° párrafo" - FMP 95/2018/1/CS1, Dictamen PGN del 10/09/2020.
STS 4526/2025, Sentencia del Tribunal Supremo Español, Sala de lo Penal del 16/10/2025.
STS 301/2016, Sentencia del Tribunal Supremo Español, Sala de lo Penal del 12/4/2016.
Caso C-670/22 | M.N. (EncroChat), Sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, del 30/04/2024.
Caso Bărbulescu c. Rumania (Demanda nº 61496/08), Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala), del 5/9/2017, .

Enlaces:
Consejo de Europa, Convenio sobre Ciberdelincuencia, Reporte explicativo sobre el convenio sobre ciberdelincuencia de Budapest, https://rm.coe.int/16802fa403
Consejo de Europa, Convenio sobre Ciberdelincuencia,, Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, https://rm.coe.int/1680a7bbf3
Consejo de Europa, Convenio sobre Ciberdelincuencia, Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas, https://rm.coe.int/1680a83724
Organización de Naciones Unidas, Convención de las Naciones Unidas contra la Ciberdelincuencia, https://www.unodc.org/unodc/es/cybercrime/convention/text/convention-full-text.html#top

o) **Modelo de Certificado a otorgar**

La Secretaría de Posgrado de la Facultad de Derecho de la Universidad Nacional de Córdoba CERTIFICA que .....(NOMBRE DE LA PERSONA) DNI (NÚMERO DE DNI) ha cumplimentado con los requisitos para APROBAR la Diplomatura Universitaria de Estudios Avanzados en Cibercrimen, Evidencia Digital y Tecnologías Emergentes aprobada por Resolución ..... (RR /RHCD No.....) con una carga horaria de 150 horas y/o un valor de seis (6) CRE.

Firma Firma Firma
(autoridad que determine la
(Docente coordinador) Facultad/Secretaría/Centro/Instituto) SAA-UNC

El presente certificado no habilita para el ejercicio profesional

Si bien no consta en la Reglamentación, **es recomendable** vincular la Diplomatura con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030. A continuación. se puede consultar los contenidos de cada uno de ellos: https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

A continuación, se presenta una tabla con los 17 Objetivos de Desarrollo Sostenible (ODS). Por favor, seleccione los que considere relevantes para esta Diplomatura.

ODS	Vinculación con la propuesta (marque con una cruz)
	
	
	
	
	X
	
	
	X
	
	
	
	

 13 ACCIÓN POR EL CLIMA	
 14 VIDA SUBMARINA	
 15 VIDA DE ECOSISTEMAS TERRESTRES	
 16 PAZ, JUSTICIA E INSTITUCIONES SÓLIDAS	X
 17 ALIANZAS PARA LOGRAR LOS OBJETIVOS	

Universidad Nacional de Córdoba
2026

Hoja Adicional de Firmas
Informe Gráfico

Número: IF-2026-00077630-UNC-SP#FD

CORDOBA, CORDOBA
Lunes 23 de Febrero de 2026

Referencia: Proyecto de Diplomatura Universitaria

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

Digitally signed by GDE UNC
DN: cn=GDE UNC, c=AR, o=Universidad Nacional de Cordoba, ou=Prosecretaria de Informatica, serialNumber=CUIT 30546670623
Date: 2026.02.23 10:32:02 -03'00'

MARIA SOLEDAD PRIOTTI
Directora General
Secretaría de Posgrado Facultad de Derecho
Universidad Nacional de Córdoba

Digitally signed by GDE UNC
DN: cn=GDE UNC, c=AR, o=Universidad Nacional de Cordoba, ou=Prosecretaria de Informatica, serialNumber=CUIT 30546670623
Date: 2026.02.23 10:32:40 -03'00'