Mar del Plata, 14 de agosto de 2024.-

RESOLUCIÓN DEL RECTORADO N° 442/24

VISTO:

El expediente por el cual, en representación del Consejo Académico, el Sr. Decano de la Facultad de Ingeniería de la Universidad FASTA solicita la aprobación de la creación de la carrera de posgrado de *Maestría en Ciberseguridad e Informática Forense*; y

CONSIDERANDO:

Que la propuesta presentada se inscribe en las políticas de la Universidad FASTA, estando indicada en el área de desarrollo académico de posgrado;

Que el proyecto de carrera ha sido aprobado en forma unánime por el Consejo Académico de la Facultad de Ingeniería en su sesión del 3 de julio de 2024;

Que se han cumplido las prescripciones de la Resolución del Rectorado N°270/02 y concordantes, respecto de los trámites internos pertinentes para la aprobación de la carrera;

Que, en función de lo relacionado *ut supra*, la propuesta reúne las condiciones exigidas por la Secretaría de Educación de la Nación y la Comisión Nacional de Evaluación y Acreditación Universitaria (CONEAU);

Que el Honorable Consejo Superior de la Universidad FASTA resolvió, en sesión de fecha 30 de julio de 2024, dar dictamen favorable a la carrera y aprobar el plan de estudios del posgrado;

Por ello, y en uso de las facultades que le confiere el Estatuto Universitario,

EL RECTOR DE LA UNIVERSIDAD FASTA
DE LA FRATERNIDAD DE AGRUPACIONES SANTO TOMAS DE AQUINO
R E S U E L V E

Artículo 1º.- APROBAR la creación de la carrera de posgrado de *Maestría en Ciberseguridad e Informática Forense* de la Facultad de Ingeniería de la Universidad FASTA.-

Artículo 2º.- APROBAR el plan de estudios de la carrera de posgrado de *Maestría en Ciberseguridad e Informática Forense*, de conformidad con la propuesta presentada por el Sr. Decano de la Facultad de Ingeniería de la Universidad FASTA, que obra como ANEXO de la presente Resolución.-

Artículo 3º.- ELEVAR copia de la presente resolución a la CONEAU, conforme lo establece el procedimiento correspondiente a la presentación de proyectos de posgrado.-

Artículo 4º.- Dese a conocer y archívese.-

Mg. Abg. MARÍA PAULA GIACCAGLIA
SECRETARIA GENERAL
UNIVERSIDAD FASTA

DR. JUAN CARLOS MENA
RECTOR
UNIVERSIDAD FASTA

ANEXO

RESOLUCIÓN DEL RECTORADO N° 442/24

PARTE I: INSTITUCIONAL

1. LA CIBERSEGURIDAD Y LA INFORMÁTICA FORENSE

La ciberseguridad se encarga de la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio poniendo el eje en la seguridad de las personas. La ciberseguridad contempla la problemática de los delitos informáticos (diferente a los incidentes de seguridad informática) donde, por ejemplo, la ingeniería social puede dar lugar a ellos, sin que conformen un problema de seguridad informática. La ciberseguridad no se reduce a una cuestión técnica de la informática, ni es sinónimo de "seguridad informática".

El avance de incidentes de ciberseguridad que generan perjuicios en las organizaciones que requieren de profesionales expresamente formados en ciberseguridad que puedan dar respuesta al incremento de la demanda que en tal sentido requieren las mismas. Las instituciones miran con mucha preocupación la situación de vulnerabilidad en la que se encuentran frente al avance de los incidentes de ciberseguridad, muchos de los cuales incluso se tratan de ciberdelitos, tales como las intrusiones indebidas y los secuestros de datos. Estas situaciones requieren de una rápida respuesta de acción inmediata, así como también, actuar en la prevención.

La Informática Forense actúa a posteriori, cuando el hecho ya ha ocurrido. Es una rama de las ciencias forenses que trabaja con datos que han sido procesados y guardados en un medio computacional. Es el uso de las tecnologías de la información para recuperar "evidencia digital", la aplicación forense de las ciencias informáticas. Comprende la recolección, adquisición, extracción, análisis, preservación, interpretación, documentación y presentación de la evidencia digital (información de valor almacenada o transmitida en una forma binaria). Se aplica tanto en el ámbito judicial como extrajudicial.

La Informática Forense requiere de personal entrenado en la materia, que pueda actuar metódicamente, mantener la cadena de custodia y evitar contaminar la prueba, principios forenses básicos. En la actuación informática forense en general o en las pericias informáticas en particular, se procura obtener indicios y/o evidencias, a fin de intentar reconstruir la real sucesión de los hechos estudiados. La tarea clave es la correcta recuperación de toda la información posible, tanto visible como oculta, relacionada con el hecho de estudio.

A la hora de recuperar información, el informático forense debe interactuar con diferentes tecnologías, diversos métodos de almacenamiento, tecnologías que naturalmente eliminan rastros, mecanismos internos de protección de la información, ausencia de herramientas específicas, aplicaciones que cubren solo una parte del proceso, diferentes sistemas de criptografía, entre otros problemas, y todo ello garantizando un proceso reproducible de adquisición, examinación, análisis, preservación y presentación de la evidencia para que tenga valor probatorio. Dada esta complejidad se requiere de profesionales altamente calificados desde lo técnico, respetuosos de los procedimientos que fijan los códigos procesales para la actuación forense, y conscientes de los principios de las ciencias forenses.

Con la experiencia lograda en la carrera de Especialización en Informática Forense, se pretende brindar una formación complementaria y específica sobre Ciberseguridad que, partiendo del análisis forense, vincule de manera natural la carrera de Especialización en Informática Forense con un

siguiente estadio de posgrado, y que amplíe la proyección profesional de los posgraduados hacia un área más abarcativa como lo es la Ciberseguridad.

Prueba fehaciente de esta demanda puede apreciarse en el constante interés por la carrera de Especialización en Informática Forense, que se imparte desde el año 2021, y el desarrollo continuo de las acciones de formación de recursos humanos y transferencia realizadas por el Grupo de Investigación en Informática Forense de la FI-UFASTA en atención a demandas de diferentes actores e instituciones.

2. OBJETIVO GENERAL DE LA PROPUESTA INSTITUCIONAL

La carrera de **MAESTRÍA EN CIBERSEGURIDAD E INFORMÁTICA FORENSE** de la Facultad de Ingeniería de la Universidad FASTA **tiene como objetivo primordial la formación de profesionales para gestionar la ciberseguridad y para la actuación forense.**

La propuesta contempla la titulación de Magíster en Ciberseguridad e Informática Forense, título al que se accede al cumplimentar el cursado de la carrera y la presentación del Trabajo Final Integrador.

La propuesta ha sido desarrollada por la Dra. Beatriz Parra de Gallo y la Esp. Ing. Ana Di Iorio, integrantes del Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA y docentes de la Especialización en Informática Forense. Asimismo, la propuesta ha sido aprobada por el Consejo Académico de la Facultad de Ingeniería en su sesión del 3 de julio de 2024.

3. FUNDAMENTACIÓN DE LA PROPUESTA INSTITUCIONAL

"Ser digital es diferente. No se trata de una invención, sino que está aquí y ahora.
Podríamos decir que es genético por naturaleza,
ya que cada generación será más digital que la que la precede".
Nicholas Negroponte. Being Digital, 1995.

La explosión de las tecnologías de la información y la comunicación ha transformado las vidas, la sociedad, la cultura, haciéndolas digital. Una generación posterior a Negroponte 1995, ya nadie duda que el mundo es digital, irreversiblemente digital.

El mundo, tal como se lo percibe, sigue siendo un lugar estrictamente analógico. Desde un punto de vista macroscópico, no es digital en absoluto, sino continuo. No obstante, está cada vez más soportado por información digital.

A diario se interactúa de diversas maneras con la tecnología de la información y las comunicaciones. Al despertar, al moverse, al comunicarse, al informarse, al ubicarse, al estudiar, al trabajar, al jugar, al viajar, al comprar, vender pagar, cobrar, se comparte y se "es", mediados por la tecnología digital. Por el solo hecho de la vida en sociedad, se consume y produce o provoca la producción de información digital, cada día más, cada minuto más, cada segundo más. Y en ese ser y vivir digital, se dejan permanentemente huellas o "rastros digitales"; información digital que habla de cada uno y de sus acciones. Evidencias digitales del mero paso por la vida.

Sumada a esta realidad, el ciberespacio es un ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee

existencia física, sino que es un dominio virtual que engloba todos los sistemas TICs[1]. El ciberespacio es un dominio muy complejo. Allí se desarrollan actividades de creación, procesamiento, almacenamiento, intercambio y visualización de información usando software y hardware interconectado. Lo constituyen tanto la Internet como todas aquellas redes aisladas que se utilizan con finalidades particulares. En este mundo digital interconectado donde todos, personas y dispositivos, producen información en cada instante, el volumen de la información crece geométricamente y su administración es cada vez más compleja, aparece, entonces, una dimensión de riesgos que ponen en jaque a las organizaciones en general y a las personas en particular. Cada vez son más las amenazas que existen en el mundo digital y cada vez, entonces, es más necesario utilizar y gestionar la tecnología en forma segura y con responsabilidad, desde los escenarios más complejos como instalaciones críticas digitales, de producción y servicios hasta los dispositivos aparentemente inofensivos y generalmente no administrados como un celular, un reloj inteligente, un electrodoméstico o un sensor que se vincula con cientos de sistemas informáticos y otros dispositivos. Son cada vez más frecuentes los incidentes de ciberseguridad, como ataques de Ransomware o Phishing que ponen en verdadero riesgo a las organizaciones y a las personas. Muchos de estos incidentes constituyen delitos informáticos y requieren no sólo de la gestión activa de la seguridad sino del estudio del fenómeno para poder prevenirlos y combatirlos y la concurrencia de la informática forense para la investigación ex post de lo ocurrido ante cada incidente.

La informática forense posibilita la detección y recuperación de la información digital que sirve de evidencia a la hora de reconstruir un hecho o sucesión de hechos. La actuación forense en informática permite recuperar y enhebrar esos rastros digitales de nuestro paso, segundo a segundo, por la vida, garantizando su valor probatorio.

La demanda de pericias informáticas (actuación forense) por parte de la justicia es cada vez mayor, y crece permanentemente, dado que los rastros digitales crecen más que linealmente y son cada vez más importantes y determinantes en la investigación. La necesidad de evidencias digitales válidas que permitan reconstruir los hechos por parte de la justicia es evidente e imperiosa y la responsabilidad de la justicia respecto de la incorporación de estas evidencias digitales al proceso investigativo y de administrar justicia es ineludible.

Además, el avance de los incidentes vinculados a la ciberseguridad y de los ataques cibernéticos también requiere de profesionales expresamente formados que puedan dar respuesta a esta demanda tal como lo requieren las organizaciones y los estados. Incluso, las instituciones miran con mucha preocupación la situación de vulnerabilidad en la que se encuentran frente al avance de las intrusiones indebidas, los secuestros de datos y la necesidad de dar una rápida respuesta preventiva y de acción inmediata frente a este panorama.

En este contexto, internacional y nacional, se requiere de profesionales calificados que trabajen en equipos sólidos para atender la creciente demanda. La escasez de profesionales y la urgente necesidad por parte de organizaciones que requieren tomar medidas frente a la gran cantidad de amenazas y delitos informáticos que circulan día a día y con actores maliciosos en constante evolución que imponen un gran dinamismo al escenario de la ciberseguridad demandan imperiosamente una respuesta desde el sistema universitario.

[1] JEFATURA DE GABINETE DE MINISTROS. SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN. Resolución 1523/2019. Anexo II - Glosario de Términos de Ciberseguridad.

Dependiendo de su infraestructura, las organizaciones suelen conformar equipos de ciberseguridad orientados a atender diferentes sectores o estructuras de la empresa, siendo los equipos encargados de la seguridad del área de operaciones, seguido por el área de administración, gestión de riesgo y *compliance* los que más profesionales ocupan, seguidos por desarrollo seguro de software, pruebas de penetración o forense. Existen diferentes aspectos que cubrir en el mundo de la ciberseguridad, tales como seguridad en la nube, evaluación, análisis y gestión de riesgos, gobernanza, *compliance*, análisis de inteligencia de amenazas y seguridad, monitoreo de redes, detección de intrusión, pruebas de penetración, normatización, gestión, etc. Cada campo requiere determinados conocimientos y competencias y, para poder trabajar en equipo y hacer un abordaje integral, es clave tener una visión holística de la problemática. Por otra parte, ante un incidente de ciberseguridad, es necesario en clasificar el incidente y diagnosticar la forma y el mecanismo mediante el cual se produjo el evento, para lo cual se requiere realizar un análisis forense del sistema, y la identificación, extracción, análisis y preservación de las evidencias digitales del hecho. De allí que, para pensar en la formación de profesionales expertos en ciberseguridad, es necesario incluir fuertes competencias relativas a las actividades, técnicas y herramientas que brinda la informática forense.

En Argentina hay muchos menos profesionales informáticos especializados en informática forense que los que la justicia demanda; es decir, profesionales matriculados habilitados como tales y con los conocimientos específicos requeridos, conforme lo establecen las diferentes regulaciones de las provincias. Incluso, hay muy pocos profesionales capacitados para la investigación y práctica forense, dado que los contenidos y prácticas específicas de la Informática forense excepcionalmente se contemplan en la instancia universitaria de grado.

A partir de la puesta en marcha de la carrera de Especialización en Informática Forense de la Universidad FASTA, que hizo posible la formación de más de 50 profesionales especializados en el tratamiento de la evidencia digital, se ha iniciado el camino para avanzar con una propuesta de formación superior, que incluya las temáticas abordadas por la Especialización en Informática Forense, y las complemente con otros conocimientos de avanzada sobre la evidencia digital y la ciberseguridad.

Por otro lado, cada vez son más los laboratorios periciales de informática forense que se crean y muchos más los que deberían crearse, no solo en el ámbito judicial, sino también en el ámbito de seguridad y ciberdefensa. En ese contexto, otras provincias con legislaciones y estructuras similares ven en la experiencia del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense - InFo-Lab (una iniciativa conjunta promovida en 2014 por la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, la Universidad FASTA y la Municipalidad de General Pueyrredón) una referencia para su retroalimentación y mejora. Tanto es así, que la Facultad de Ingeniería, a solicitud del Ministerio Público de la provincia, ha desarrollado la Guía Técnica para el Diseño, Implementación y Gestión de Laboratorios de Informática Forense y a posteriori una Guía Técnica para el diseño y la Implementación de un Sistema de Gestión de Calidad en Laboratorios de Informática Forense. Estos desarrollos le continuaron a la puesta en vigencia en junio de 2016 mediante Resolución 483/16 de la Procuración General de la Suprema Corte de Justicia de la Guía Integral de empleo de la Informática Forense en el proceso penal. Esta Guía, basada en el Proceso Unificado de Recuperación de la Información PURI de la Universidad FASTA, establece los procedimientos de actuación forense vigentes en la provincia de Buenos Aires.

En esta línea de trabajo el Grupo de Investigación en Informática Forense cuenta con una extensa actividad de investigación, transferencia y vinculación, que se explica en detalle en el apartado correspondiente del presente documento.

En este contexto, caracterizado por la complejidad técnica propia de la aplicación forense de la informática, la dinámica y permanente evolución de las tecnologías de la información y comunicación y las herramientas forenses, el avance de los incidentes de ciberseguridad que ponen en riesgo a las personas, los aspectos procesales y legales que involucran a la prueba digital y las cuestiones relativas a la ciberseguridad de las instalaciones tecnológicas que se deben contemplar, así como la creciente demanda de profesionales de la informática experimentados y debidamente formados para desarrollar una efectiva actuación forense y para dar respuesta a las problemáticas propias de la ciberseguridad, la Facultad de Ingeniería de la Universidad FASTA, a través del Grupo de Investigación en Informática Forense, ha diseñado y propone esta carrera de MAESTRÍA EN CIBERSEGURIDAD E INFORMÁTICA FORENSE, como una continuación de las acciones de formación de posgrado iniciadas con la puesta en marcha de la Especialización en Informática Forense.

Desde lo institucional, esta carrera de posgrado complementa y fortalece la oferta académica de la Facultad de Ingeniería, en una materia en la que ha desarrollado una vasta y valiosa experiencia, y donde cuenta con reconocidos antecedentes en investigación, desarrollo de tecnología, extensión, asesoramiento, transferencia y capacitación. El Grupo de Investigación en Informática Forense que da origen y sustento académico a esta carrera tiene más de 15 años de comprometido trabajo en la temática, con destacado desempeño en la docencia, extensión e investigación, con 8 proyectos nacionales acreditados por el Ministerio de Ciencia, Tecnología e Innovación Productiva, proyectos internacionales en red con universidades de Iberoamérica, relevantes publicaciones en Argentina y otros países y una fuerte vinculación con instituciones de la justicia y de la industria en este campo, 44 proyectos de I+D de los cuales 16 fueron desarrollados en conjunto con otras Universidades.

También es importante señalar que el Grupo de Investigación en Informática Forense retroalimenta a la carrera de Licenciatura en Criminalística que dicta la Facultad de Ciencias Jurídicas y Sociales, a la carrera de Especialización en Medicina Legal de la Facultad de Ciencias Médicas y a la carrera de Ingeniería Informática de la Facultad de Ingeniería. Por otra parte, la creación de la carrera de Licenciatura en Ciberseguridad, creada en el ámbito de la propia Facultad de Ingeniería, como resultado de la amplia experiencia que esta unidad académica ha logrado en el tiempo también permite proyectar una segunda carrera de posgrado en esta temática. En todas estas carreras hay asignaturas específicas en la temática de Ciberseguridad y/o de Informática Forense dictadas por integrantes del Grupo de Investigación en Informática Forense y eso contribuye a fortalecer el perfil profesional y a desarrollar competencias distintivas en estos egresados. El trabajo conjunto y articulado entre las 3 unidades académicas no solo retroalimentó a las carreras y mejoró la formación de los egresados, sino que contribuyó a posicionar a la Universidad como referente en el campo de la forensia en general en el ámbito universitario, tanto a nivel nacional como latinoamericano, dando lugar a la reciente creación del Instituto de Ciencias Forenses de la Universidad FASTA.

Esta carrera se desarrolla para dar respuesta a una demanda concreta de la sociedad a nivel nacional y latinoamericano, en particular en el campo de la ciberseguridad y la informática forense, y de la maduración de un grupo de investigación que puede y pretende dar respuesta a esa demanda en ámbito de la formación de posgrado.

La propuesta se enmarca en lo previsto en el Plan Estratégico de la Universidad FASTA:

- ***Objetivo Estratégico 2*** que señala “Consolidar el nuevo paradigma de docencia, basado en el desarrollo de las competencias y los rasgos identitarios del graduado, orientándolo a las exigencias de la era digital”, y responde a las líneas de acción relacionadas a los graduados, particularmente

en la que se indica cómo "**Elaborar un programa de acompañamiento a los graduados en su inserción profesional**".

- ***Objetivo Estratégico 3*** que propone "Transformar la gestión de la investigación y desarrollo tecnológico en la Universidad, adecuándola a la cultura digital y orientándola a dar respuesta a las demandas sociales", que contiene dos líneas de acción en las que impacta esta carrera: "**Vincular la investigación y el posgrado entendiendo la primera como sustento de la segunda**" e "**Incrementar el apoyo a los estudios de posgrado como una política prioritaria de desarrollo de los investigadores**".

Asimismo, el proyecto está previsto en el Plan de Desarrollo de la Facultad de Ingeniería de la Universidad FASTA, en tanto amplía y complementa la oferta académica de posgrado en un área temática distintiva de la unidad académica y que supone una opción de formación de posgrado tanto para sus graduados de Ingeniería en Informática como para los de Licenciatura en Ciberseguridad. Asimismo, los egresados de estos posgrados retroalimentan la planta docente de la propia maestría y de las carreras de grado afines de la Unidad Académica y la planta de investigación del InFo-Lab. Además, esta maestría comparte su foco temático con la Revista "InFo-Cyber - Cybersecurity and Digital Forensics Journal" que la facultad ha lanzado en mayo de 2024 (RDFI UFASTA 135/24). Se trata de una revista científico-tecnológica universitaria, digital y abierta, sobre Ciberseguridad e Informática Forense, con formato de journal de publicación semestral que pretende convertirse en una referencia en el área de Ciberseguridad e Informática Forense, con un enfoque de excelencia académica e innovación, promoviendo la investigación, el desarrollo y la difusión del conocimiento científico-tecnológico en Latinoamérica y el Caribe. Prevé como misión proporcionar un espacio de alta calidad para la presentación y discusión de investigaciones originales, revisiones críticas y desarrollos técnicos en el campo de la ciberseguridad y la informática forense, incentivar la colaboración entre investigadores, académicos, profesionales de la industria y responsables políticos, con el objetivo de abordar los desafíos más actuales en la temática.

Desde el punto de vista institucional, la Facultad de Ingeniería propone, con este proyecto, la continuación de su política de responder a demandas de formación actualizada y que atiendan problemáticas sociales vinculadas a la aplicación de las tecnologías informáticas en nichos de alta demanda profesional.

4. AUTORIDADES DE LA FACULTAD DE INGENIERÍA

Decano
Esp. Ing. Roberto Giordano Lerena

Vicedecana
Lic. Sandra Cirimelo

Secretario Académico
Ing. Roberto Sotomayor

Secretaria de Investigación
Lic. Mónica Pascual

Secretaría de Extensión
Abog. Antonela D'Onofrio

Secretaria Administrativa
Téc. Virginia Sebastián

Director de la carrera Ingeniería Informática
Ing. Luis Buffoni

Director de la carrera de Licenciatura en Ciberseguridad
Ing. Santiago Trigo

Directora Académica de la carrera Especialización en Informática Forense
Esp. Ing. Ana Haydée Di Iorio

Directora Ejecutiva de la carrera Especialización en Informática Forense
Lic. Lucía Algieri

Director del Grupo de Investigación en Informática Forense y del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense
Ing. Bruno Constanzo

Asistente de Coordinación del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense
Abg. Lic. Josefina Riva Posse

PARTE II: LA CARRERA de MAESTRÍA EN CIBERSEGURIDAD E INFORMÁTICA FORENSE

5. PRESENTACIÓN

Denominación:	Maestría en Ciberseguridad e Informática Forense
Título que otorga:	Magister en Ciberseguridad e Informática Forense
Nivel de la carrera:	Posgrado - Maestría
Unidad Académica:	Facultad de Ingeniería
Organización:	Carrera Institucional, perteneciente a una institución universitaria, y con un único proceso formativo.
Plan de Estudio:	Estructurado. Está predeterminado por la institución y es común para todos los estudiantes.
Modalidad:	A distancia. Las actividades curriculares previstas en el plan de estudio (cursos, seminarios, talleres u otros espacios académicos) no requieren la presencia del estudiante en ámbitos determinados institucionalmente.
Duración:	4 semestres.
Carga Horaria:	3.000 horas / 120 créditos académicos 2.500 hs. de cursado y práctica / 100 créditos académicos 500 hs. de Trabajo Final Integrador / 20 créditos académicos.

Asignaturas:	19 asignaturas más Trabajo Final Integrador.
Sede de dictado:	Plataforma de Educación a Distancia de la Universidad FASTA.
Requisitos de titulación:	Para la titulación se requiere la aprobación de las 19 asignaturas y la presentación de un Trabajo Final Integrador, individual, cuya aprobación conduce al otorgamiento del título de "Magister en Ciberseguridad e Informática Forense"
Modo de acreditación:	Carrera nueva. Aún no ha sido puesta en funcionamiento y no cuenta con estudiantes.
Inicio del dictado:	El inicio de la primera edición está sujeto a la aprobación de la Carrera por parte de CONEAU.
Frecuencia de dictado:	Anual.
Vacantes por edición:	50

6. ANTECEDENTES

La carrera de Maestría en Ciberseguridad e Informática Forense tiene como principal antecedente a la carrera de Especialización en Informática Forense, cuya primera cohorte ingresó en el año 2021 y que a la fecha cuenta con 65 profesionales que la cursaron o están cursando, de los cuales 21 ya obtuvieron su título de posgrado.

Las acciones de docencia, investigación, extensión en estas temáticas desarrolladas a partir del año 2007 por la Facultad de Ingeniería de la Universidad FASTA se suman a los antecedentes que, en su momento, mostraron la interrelación alcanzada entre las funciones sustantivas de la universidad cuando se presentó la carrera de Especialización en Informática Forense.

La madurez lograda con el dictado completo de tres cohortes y de la actual (en curso) de la carrera de Especialización en Informática Forense, permite avanzar con una propuesta superadora, que genere una instancia superior de formación permitiendo a los graduados y posgraduados avanzar en su formación profesional en temáticas vinculadas a la Informática Forense, como lo es la Ciberseguridad. Por otra parte, el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de UFASTA sostuvo una línea de crecimiento permanente en proyectos de investigación, acciones de extensión y transferencia, así como en la formación específica de recursos humanos.

La oferta de formación en ciberseguridad ha crecido, y se observa interés en las instituciones universitarias por generar capacitaciones cortas y diplomaturas que permitan la captación de los interesados en estas temáticas, pero muy pocas de estas acciones se transformaron en carreras formales. Hasta el año 2022, la CONEAU aprobó 9 carreras de posgrado (3 maestrías y 6 especializaciones) vinculadas a seguridad informática e informática forense, éstas son: Maestría y Especialización en Seguridad Informática (UBA), Maestría en Ciberdefensa (UDN), Maestría en Ciberdefensa y Ciberseguridad (UBA), Especialización en Redes y Seguridad (UNLP), Especialización en Criptografía y Seguridad Teleinformática (UDN), Especialización en Seguridad Informática (UAI) y Especialización en Informática Forense (UFASTA).

En este sentido, desde la Universidad FASTA, reconociendo que la falta de profesionales formados en ciberseguridad e informática forense es un problema cada vez más preocupante y limitante tanto para el Estado como para el resto de las organizaciones, instituciones y empresas expuestas a incidentes de

ciberseguridad, el Grupo de Investigación de Informática Forense de la Universidad FASTA ha desarrollado de manera continua y sin pausa, desde 2014, acciones de capacitación vinculadas a la ciberseguridad y a la informática forense que se detallan en el apartado 6.2 del presente proyecto. A esto se suman la carrera de grado de Licenciatura en Ciberseguridad y la carrera de posgrado de Especialización en Informática Forense.

En síntesis, no existe en el país, ni en Latinoamérica, ofertas de carreras de posgrado que propongan de manera conjunta las temáticas de Ciberseguridad e Informática Forense y que, además, se dicten en modalidad no presencial, con un abordaje y perfil técnico, criminalístico, criminológico, legal y ético en las dos áreas temáticas, tal como se propone en esta carrera.

En el ámbito del Consejo Académico de la Facultad de Ingeniería se definió como política institucional que la investigación debería estar orientada a las temáticas propias de las carreras y sus asignaturas, y como instrumento de enriquecimiento de las mismas, sin perjuicio de proyectos transversales o de carácter institucional. Esto significa, ver a la función de investigación como una "palanca" que, además de sus propios fines, retroalimenta y redunda en mejoras en la docencia, extensión y vinculación.

Los grupos de investigación de la Universidad FASTA tienen en sus respectivas Facultades un conjunto de asignaturas vinculadas a los proyectos de investigación que se desarrollan, generando un espacio para compartir, interactuar y enriquecer tanto a estudiantes como a docentes con un análisis de las problemáticas abordadas en dichos proyectos. Generalmente los investigadores de los grupos son, a su vez, docentes de sus respectivas asignaturas en las que se abordan las temáticas que ellos mismos investigan. Cada año, en la planificación docente de estas asignaturas, se prevé la presentación a los estudiantes por parte del grupo de investigación, de los proyectos en que están trabajando, en una clase abierta a su vez a otros docentes. Esta actividad contribuye a que los estudiantes conozcan de los temas de investigación, los vinculen a los contenidos de cada asignatura, se interesen por la investigación y las temáticas, se vean motivados a integrarse al grupo y, en algunos casos, a desarrollar su Práctica Profesional Supervisada e incluso sus proyectos integradores de graduación en ese campo.

En este caso, el Grupo de Investigación en Informática Forense cuenta con un grupo de asignaturas en la carrera de grado "Ingeniería en Informática" donde se logra la interacción directa entre la docencia y la investigación, tales como "Informática y Derecho", "Gestión de la Seguridad Informática", "Taller de Seguridad Informática", "Sistemas Operativos", "Sistemas Distribuidos" e "Informática Forense", cuyos docentes integran el Grupo de Investigación y encuentran allí el espacio para retroalimentar y potenciar la docencia e investigación en beneficio de los estudiantes. Los grupos de investigación proponen trabajos prácticos en las asignaturas que les permiten a los estudiantes la experimentación y el desarrollo vinculados con la temática.

También desde los grupos de investigación se proponen actividades de actualización profesional que retroalimentan a los estudiantes y graduados que quieran cursarlos. Finalmente, cuando el nivel de madurez alcanzado por los grupos lo permite, estos se transforman en generadores de las carreras de posgrado de la Universidad, como es el caso del Grupo de Investigación en Informática y Derecho con la carrera de Especialización en Gestión Legal de la Tecnología de la Información, y en este proyecto, el Grupo de Informática Forense, que habiendo dado lugar a la carrera de Especialización en Informática Forense, propone ahora una carrera superadora como lo es la Maestría en Ciberseguridad e Informática Forense.

Asimismo, la investigación contribuye fuertemente a la proyección institucional y posicionamiento de las Facultades. La necesidad de los grupos e investigadores de divulgar su producción, participar de

congresos y foros, intercambiar experiencias, trabajar en forma conjunta con otros grupos de otras instituciones nacionales y extranjeras, hace imprescindible el apuntalamiento de la función extensión a la investigación, facilitando el desarrollo de estas actividades. Así, la organización de seminarios, congresos, talleres, etc., permite dar visibilidad a las actividades de investigación y facilita el acceso de docentes y estudiantes a estos encuentros, retroalimentando, entonces, la docencia. La vinculación y trabajo colaborativo con grupos de otras instituciones permite el intercambio de experiencias y contribuye al desarrollo de competencias de vinculación y trabajo en equipo.

El Grupo de Investigación en Informática Forense integra el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab). El InFo-Lab nuclea en la ciudad de Mar del Plata a un equipo interdisciplinario de 36 investigadores científicos y tecnológicos, profesionales y técnicos altamente calificados, con el objeto de investigar y desarrollar soluciones a las demandas en el campo de la Informática Forense y su aplicación.

El Grupo de Investigación en Informática Forense de la UFASTA ha creado y publicado en el año 2012, el "Proceso Unificado de Recuperación de Información Digital PURI®", una referencia para informáticos forenses respecto de las tareas que se deben llevar a cabo para obtener evidencias digitales válidas. Por ello, el Ministerio Público de la provincia de Buenos Aires convocó al Grupo de Investigación a efectos de formalizar, a partir de PURI, un protocolo estándar de actuación para la obtención de evidencias digitales válidas cumpliendo los principios forenses básicos que dan garantía al proceso judicial. Así surge el Proyecto de Desarrollo Tecnológico Social PAIF-PURI®, que fuera oportunamente acreditado por el MinCyT y dio lugar al Protocolo de Actuación Forense PAIF-PURI y a la Guía Integral de Empleo de la Informática Forense en el Proceso Penal®, que contempla los diversos roles que pueden desempeñar los especialistas informáticos, conforme sus diferentes niveles de experticia (entre ellos: el Rol de asesoramiento, el Rol investigativo y el Rol pericial) y las diversas responsabilidades (entre ellas: Identificación, Recolección, Adquisición, y Pericia). Además, incorpora lineamientos referidos al abordaje de los casos, la planificación y gestión de la investigación penal y la litigación.

Esta guía, formalmente adoptada y promovida en su uso por el Ministerio Público de la Provincia de Buenos Aires Resolución 483/16 de la Procuración General de la Suprema Corte de Justicia, fue la única en su tipo en Latinoamérica durante mucho tiempo, sigue vigente en la Provincia de Buenos Aires y su aplicación contribuye a una mejor administración de justicia, permitiendo la recuperación de evidencias digitales respetando los principios forenses básicos y dando con esto las garantías necesarias para las partes.

Considerando el perfil y las actividades que actualmente están desarrollando los investigadores del Grupo de Informática Forense dentro de la línea de trabajo en Ciberseguridad, es necesario formalizar las experiencias que ya tienen adquiridas, transformándolas en competencias profesionales. Este pasaje del "conocimiento informal" al "conocimiento científico" es lo que destaca de una carrera como la Maestría en Ciberseguridad e Informática Forense como la que aquí se propone.

Asimismo, la extensión por medio de transferencia y servicios también es un aspecto para destacar de los grupos de investigación, ofreciendo soluciones a demandas y problemas concretos y brindando servicios calificados muy específicos que la sociedad no encuentra en el mercado profesional. De estas acciones se brinda detallada información en el apartado 6.2 del presente proyecto.

Se presentan a continuación los antecedentes específicos en Docencia, Investigación y Extensión en el campo de la Ciberseguridad e Informática Forense que dan marco a la propuesta de la carrera de Maestría en Ciberseguridad e Informática Forense de la Facultad de Ingeniería de la Universidad

FASTA.

6.1. **DOCENCIA**

Los docentes de esta carrera de posgrado tienen un perfil orientado al trabajo interdisciplinario entre informáticos, abogados y criminalistas, con un fuerte componente relacionado con las demandas sociales y problemáticas que surgen como de interés para carreras como ésta.

El cuerpo docente está integrado por profesionales posgraduados que tienen titulaciones de base diferentes, vinculadas a la Informática, el Derecho y la Criminalística. Todos mantienen vínculos de interacción conjunta surgidos de la experiencia de impartir la Especialización en Informática Forense. Y a este modelo de trabajo es que se invita a los docentes que se sumen a la carrera de Maestría en Ciberseguridad e Informática Forense.

El cuerpo docente propio de la Facultad de Ingeniería de la Universidad FASTA que integra la carrera de Maestría en Ciberseguridad e Informática Forense ha participado desde el año 2014 de acciones de capacitación formal en temáticas vinculadas a este posgrado y varios de ellos son investigadores del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) e integran el Grupo de Investigación en Informática Forense.

En la Universidad FASTA, en la carrera de Ingeniería en Informática se dictan las asignaturas de “Informática y Derecho”, “Gestión de la Seguridad Informática”, “Taller de Seguridad Informática”, “Sistemas Operativos”, “Sistemas Distribuidos” e “Informática Forense”, todas con contenidos y trabajos prácticos relacionados a la Informática Forense.

En la carrera de Licenciatura en Ciberseguridad se dictan las asignaturas “Ciberseguridad I”, “Ciberseguridad II”, “Ciberseguridad III”, “Aspectos legales de la Ciberseguridad”, “Taller de Ciberseguridad”, “Informática Forense I”, “Informática Forense II” y “Taller de Informática Forense” cuyos docentes integran el Info-Lab.

En la carrera de Licenciatura en Criminalística se dicta la asignatura “Informática Aplicada”, orientada a la aplicación forense de la Informática, cuyos docentes son también integrantes del InFo-Lab; y en la carrera de Abogacía, se dicta la asignatura “Derecho de las Nuevas Tecnologías” con énfasis en la interrelación entre la informática y el derecho, dedicando una unidad a la problemática de la informática forense y las pericias informáticas.

Los docentes de todas estas asignaturas integran el cuerpo docente de la carrera de Maestría en Ciberseguridad e Informática Forense.

En cuanto a la docencia de posgrado, la Facultad de Ingeniería dicta desde el año 2021 la carrera de Especialización en Informática Forense, acreditada por CONEAU, precedente importante para este proyecto. Asimismo, se cuenta también con la carrera de Especialización en Gestión Legal de la Tecnología de la Información, acreditada por CONEAU, y en la Facultad de Ciencias Médicas se dicta la asignatura Informática Forense en la carrera de posgrado de Especialización en Medicina Legal. En todos estos casos, los docentes integran el plantel docente de este posgrado.

6.2. **EXTENSIÓN**

La actividad de extensión, transferencia y servicios en este campo está soportada por el Grupo de Investigación en Informática Forense, que cuenta con amplia experiencia y antecedentes en los siguientes temas:

Servicios en informática forense:

- Servicios de consultoría en informática forense.
- Recuperación de archivos o datos eliminados.
- Adquisición y Preservación de prueba digital.
- Asesoramiento en el diseño e implementación de soluciones de informática forense.
- Desarrollo de guías de buenas prácticas en el campo de la informática forense.

Servicios en ciberseguridad:

- Auditoría en ciberseguridad.
- Análisis de ataques de ciberseguridad.
- Desarrollo de simulacros de ciberataques para preparación y formación.
- Asesoramiento en cumplimiento de normativas de ciberseguridad.
- Creación y mantenimiento de bases de datos de ciberamenazas.
- Desarrollo de guías de buenas prácticas en el campo de la ciberseguridad.
- Desarrollo de estrategias de recuperación ante desastres cibernéticos.
- Creación y mantenimiento de bases de datos de ciberamenazas.
- Formación en legislación y ética en ciberseguridad.

Servicio de gestión de laboratorios en informática forense:

- Asesoramiento en cumplimiento de normativas de informática forense y ciberseguridad.
- Asesoramiento en el diseño e implementación de laboratorios de informática forense.
- Desarrollo de guías de buenas prácticas para la gestión de laboratorios de I+D en informática forense.
- Investigación de nuevas tendencias y tecnologías en informática forense y ciberseguridad:
- Análisis de demandas.
- Comparación de productos o soluciones existentes.

Servicios de Capacitación y Formación

- Formación en informática forense
- Formación en ciberseguridad

Servicios de Creación de Contenido

- Creación de contenido audiovisual y digital para formación.
- Creación de contenido audiovisual y digital para difusión.
- Creación de programas de concientización sobre ciberseguridad.
- Publicación de boletines regulares sobre las últimas tendencias en informática forense y ciberseguridad.
- Creación de un repositorio de casos de estudio de informática forense o ciberseguridad.

Línea Internet Sana

- Asesoramiento, consultoría y capacitación sobre Grooming, Ciberbullying, Sexting, Sharenting.
- Capacitaciones sobre los cuidados en el mundo digital. Talleres enfocados a niños,

niñas y adolescentes. Talleres enfocados a docentes, para padres, adultos mayores y público en general.

- Formación de formadores en (servicio de formación a profesionales).
- Diseños de código de convivencia digital en Instituciones.

Asimismo, el Grupo de Investigación ha diseñado y ha dictado desde el 2014 hasta el 2019 el Programa de Actualización Profesional en Informática Forense de la Universidad FASTA. De igual manera, se brindan capacitaciones y talleres por demanda, a la medida de las necesidades de cada institución.

Proyectos de extensión:

(2016 - 2018) Conversando sobre Grooming con docentes y padres

Es un programa de capacitación destinado a docentes de colegios primarios y secundarios y padres de niños, niñas y adolescentes que prevé el dictado de cursos cortos de capacitación donde se desarrollarán conceptos básicos sobre esta modalidad delictiva, la manera de prevenirla y/o detectarla, y consejos para el control parental sobre los menores en relación al uso de las nuevas tecnologías. Asimismo, prevé espacios de discusión y consultas sobre la temática con los asistentes.

(2019 - 2020) CUIDADOS EN LA RED: Dispositivos de prevención y asesoramiento en vínculos tecno-mediados.

Abordar interdisciplinariamente la vulneración de derechos producida en el marco de vinculaciones tecno-mediadas.

(2019 - 2020) Diagnóstico y Mejora de la Calidad en procesos de coordinación interinstitucional del Departamento Judicial Mar del Plata

Este proyecto tuvo como objetivo diagnosticar, estudiar e implementar mejoras en los procesos de coordinación entre la Justicia Penal y la Justicia Civil y Comercial, de manera de brindar una mejor atención a los ciudadanos que deben tramitar el mismo caso en ambas instancias respectivamente.

(2018 - 2023) Consultorio Interdisciplinario para la orientación a las víctimas de delitos en el marco de vínculos tecno-mediados

El proyecto se inicia como respuesta al pedido de asesoramiento y orientación a víctimas que denuncian situaciones de vulneración de sus derechos a través de medios tecnológicos y redes sociales que hace la Defensoría del Pueblo de la MGP. Implica la creación de un consultorio interdisciplinario que funcionará en la sede del InFo-Lab y recibirá las derivaciones de las consultas originadas en la Defensoría del Pueblo de la Municipalidad de General Pueyrredon, como así también de casos emergentes del espacio de difusión preventiva del Proyecto de Extensión Permanente “Internet Sana” de la Facultad de Ingeniería.

(2020 - 2023) Desarrollo de una guía de recomendaciones para una adecuada infraestructura técnica, legal y de convivencia digital que soporte el proceso de enseñanza aprendizaje mediado por la tecnología en colegios

Esta guía pretende generar un marco mínimo y seguro en términos técnicos, legales y de convivencia para las actividades mediadas por la tecnología, que acompañe a los actores involucrados, y sin ser un instrumento riguroso que genere obstáculos en el desarrollo de las mismas.

(2023 - 2024) Convivencia Digital

Este proyecto fusiona y asume los objetivos de los proyectos de extensión "Conversando sobre Grooming con docentes y padres" (RDFI No 389/16) y "Consultorio Interdisciplinario para la orientación a las víctimas de delitos en el marco de vínculos tecnomediados"

(2020 - 2024) Taller de juegos lúdicos y estrategias teatrales para Investigadores de la Facultad de Ingeniería y del InFo-Lab

La comunicación es una característica esencial en las personas. Sin la capacidad expresiva no podríamos relacionarnos con los demás. Este espacio nace para entrenar las capacidades expresivas y de esa manera colaborar en el desarrollo personal y profesional de los investigadores.

(2022 - 2023) E-Experiencias: Sistematización de experiencias en las dimensiones del cuidado integral de la niñez en el mundo digital

Sistematizar y difundir hallazgos, teorizaciones e intervenciones sobre la socialización de la niñez y adolescencia en el mundo digital, Recopilación y ordenamiento de las conceptualizaciones vinculadas a los ciber vínculos infantiles y adolescentes desde un enfoque institucional y social, Compilación de antecedentes sobre datos argentinos respecto a ejes de potenciación y vulneración de derechos en interacciones online de Niños, Niñas y Adolescentes, Sistematización de experiencias y prácticas argentinas promotoras, preventivas y reparadoras institucionales respecto al ejercicio ciudadano digital de menores. Y posteriormente la elaboración de un documento de difusión en formato de libro digital e impreso.

(2021-203) Encuestas de Victimización sobre ciberdelitos

Este estudio realizado junto con el "Observatorio de la Ciudad" de la Universidad FASTA tiene como objeto investigar y relevar información sobre la comisión de delitos mediados por la tecnología en la ciudad de Mar del Plata. Para la concreción de este informe, fueron realizadas 500 encuestas de manera online y presencial sobre victimización con el fin de conocer la percepción de la seguridad de los encuestados marplatenses, detectar potenciales víctimas, determinar los canales adecuados para prevención y concientización, conocer las medidas de seguridad adoptadas por los ciudadanos, cuantificar los tipos de delitos sufridos y explorar el nivel de cifra "negra" de los mismos.

Este proyecto (RDFI 156 - 2021) fue realizado en coordinación con las Facultades de Ingeniería y de Ciencias Jurídicas y Sociales de la Universidad FASTA, el cual posee una vasta experiencia en investigaciones vinculadas al fraude electrónico y violencia digital. En una primera sección de este informe se indaga sobre cuáles son las medidas de seguridad que adoptan los ciudadanos al navegar o realizar trámites online y sobre si se sienten o no seguros al utilizar este tipo de herramientas. En segundo término, se presentan datos sobre cuáles son los medios que la sociedad utiliza para informarse sobre este fenómeno a los efectos de direccionar los mecanismos de prevención y concientización. En tercer lugar, se indaga sobre si los encuestados fueron víctimas de algún delito y por último, se pregunta sobre las reacciones frente a esas circunstancias.

Transferencias:

Taller de Transferencia InFo-Lab UFASTA - INVESTIGA a la Facultad Regional Delta de la Universidad Tecnológica Nacional - UTN Delta

En esta transferencia se capacitó a los representantes de UTN Delta respecto a la funcionalidad de INVESTIGA, su inserción en el contexto de la investigación criminal, y las necesidades y aportes del software, como así también sobre uso del sistema y en la arquitectura del mismo.

Asesoramiento para el diseño e implementación de un Laboratorio Judicial de Informática Forense.

El objetivo general de la propuesta es el asesoramiento integral al Poder Judicial de la provincia de San Juan para el diseño e implementación de su Laboratorio de Informática Forense (LIF PJ San Juan), brindando las capacitaciones necesarias al efecto a través de su Escuela de Capacitación Judicial.

Transferencia al Poder Judicial del Chaco

Se realizó un Informe Técnico producto de una investigación sobre el software malintencionado (malware) Hive Ransomware realizada por investigadores especialistas del Grupo de Investigación y Desarrollo de Tecnología en Informática Forense de la Universidad FASTA, que tiene su sede en el Laboratorio de Investigación y Desarrollo de Tecnología InFo-Lab. La investigación estuvo a cargo del Ing. Bruno Constanzo, y fue realizada en el mes de febrero de 2022.

Transferencia al Instituto de Innovación, Tecnología y Justicia (IFITEJ) de Píldoras Formativas bajo el eje "Introducción a la Ciberseguridad para usuarios de sistemas"

El plan de capacitación constituyó en la producción de píldoras formativas digitales de concientización para usuarios, bajo el eje "Introducción a la Ciberseguridad para usuarios de sistemas". Se produjeron 9 píldoras formativas, divididas en tres bloques conceptuales. Dichos lotes de tres videos se entregaron a lo largo del año 2023.

6.3. **INVESTIGACIÓN**

La vasta experiencia y antecedentes en investigación aplicada y el desarrollo de tecnología en Informática Forense es el sustento principal para la implementación de la carrera de Maestría en Ciberseguridad e Informática Forense que se presenta.

La investigación aplicada y desarrollo de tecnología en la Facultad de Ingeniería de la Universidad FASTA ha tenido un importante desarrollo en los últimos 20 años. En ese tiempo, los grupos de investigación permanente se han ido consolidando en las respectivas temáticas y articulando conocimientos y experiencias entre ellos.

Uno de los grupos pioneros en la Universidad es el grupo de Informática y Derecho, que reúne a un equipo interdisciplinario de investigadores de las Facultades de Ciencias Jurídicas y Sociales y de Ingeniería en proyectos donde el derecho contribuye a regular el desarrollo de la informática y la informática contribuye al derecho en general. La Informática Forense es una disciplina que se desarrolla en este campo interdisciplinar donde la informática va en auxilio del derecho en general y de la justicia en particular. En esto es importante conocer tanto el marco legal como el marco técnico y que "ambos mundos hablen entre sí". En ese sentido, la experiencia del Grupo de Investigación en Informática y Derecho es un antecedente y fortaleza fundamental para el desarrollo de la investigación en Informática Forense que lleva adelante el Grupo de Investigación en Informática Forense.

Se presenta a continuación una breve reseña de los antecedentes de ambos grupos de investigación, destacando la conformación del Info-Lab, el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense de la Universidad FASTA, que nace de una iniciativa conjunta con la Procuración de la Suprema Corte de Justicia de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon.

Estos grupos y el laboratorio son la base del conocimiento, experiencia y docentes que sostienen la carrera de Maestría en Ciberseguridad e Informática Forense de la Universidad FASTA.

6.3.1. **Grupo de Investigación en Informática y Derecho**

El Grupo de Investigación en Informática y Derecho (Res. Rector 182/11), es un grupo interdisciplinario integrado por ingenieros en informática y abogados, y dependiente tanto de la Facultad de Ingeniería como de la Facultad de Ciencias Jurídicas y Sociales. Inició sus actividades a fines del 2007, dirigido por la Dra. Abog. Bibiana Luz Clara, con el Proyecto *Modelos de aplicación a la contratación del Software y Servicios Informáticos* en ámbito de Defensa del Consumidor, que logró conformar un marco adecuado de protección a las partes en la contratación de bienes y servicios informáticos, a fin de evitar inequidades en el desarrollo de la relación entre el profesional y el cliente, dada la disparidad de conocimientos existentes entre ambas partes. Este proyecto generó como producto una Guía de recomendaciones a los usuarios de Software y Servicios Informáticos, desde la perspectiva de sus derechos.

A la par de este proyecto, el Grupo de Informática y Derecho de la Universidad FASTA, en forma conjunta con el Instituto de Gobierno Electrónico, Inteligencia Jurídica y Sistemas I3G (Brasil), la Universidad Federal de Santa Catarina UFSC (Brasil), la Universidad de Chile y la Universidad Politécnica de Madrid UPM (España), en el marco de los correspondientes convenios interinstitucionales, abordan el desarrollo de un ambicioso proyecto internacional de I+D: *Ontojuris*. En su primera etapa (*Ontojuris I*, 2007-2009) el proyecto pretendía proponer el diseño conceptual y formal de una herramienta para la gestión de Ontologías, aplicada específicamente, al campo de la Legislación en el área de Propiedad Intelectual, Derechos del Consumidor y Derecho Electrónico en los 4 países. Cumplido el objetivo, el equipo continuó en esa línea por 2 años más (*Ontojuris II*, 2009-2011) para proponer el diseño conceptual y formal de un sistema multilingüe de búsqueda de información en la web en el dominio legal, basado en ontologías, en UNL (Universal Network Language). Estas investigaciones recibieron ayuda económica del Conselho Nacional de Desenvolvimento Científico e Tecnológico de Brasil - CNPQ, por medio de las adjudicaciones de fondos para proyectos internacionales de investigación; Edital MCT/CNPq 15/2007 y Edital Universal MCT/CNPq 14/2009 y alcanzaron los resultados esperados.

La actuación y resultados publicados por el equipo argentino del Proyecto Ontojuris motivaron la convocatoria de la Universidad FASTA para integrar la Cátedra UNESCO de Tecnologías Lingüísticas al servicio de la educación "TECLIN", bajo la dirección del profesor Dr. Jesús Cardeñosa Lera, investigador del proyecto *Ontojuris*.

La experiencia adquirida en el diseño, construcción y validación de ontologías y herramientas basadas en ontologías en el campo legal y en la formalización conceptual de la normativa específica en UNL, motivó el Proyecto *Análisis de consistencia de la legislación de Defensa del Consumidor*, en este caso en forma conjunta c3on el Grupo de Investigación *FormaLex* del Departamento de Computación de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. Este proyecto tiene como objeto analizar la consistencia de la legislación argentina sobre Defensa del Consumidor mediante métodos formales y adaptación de técnicas nacidas en el ámbito de la Ingeniería del Software y adaptadas para ser aplicadas al dominio legal (en concreto, mediante FL, un lenguaje deóntico de validación).

En paralelo a Ontojuris, al finalizar la investigación sobre Derechos del Consumidor, el grupo continuó sus actividades en la temática, con el Proyecto de Contrataciones Digitales en Internet (2009-2010) que analizó la realidad y marco técnico-jurídico de las contrataciones digitales y formuló recomendaciones para usuarios, consumidores y proveedores que contratan servicios a través de Internet y el Proyecto de Protección de los derechos de usuarios y consumidores de Redes Sociales y

Cloud Computing (2011-2012) que analizó las nuevas figuras jurídicas que utilizan los usuarios de redes sociales y computación en la nube y las consecuencias que como consumidores pueden sufrir en dichas contrataciones y elaboró recomendaciones de uso responsable y cuidado de la privacidad y de los datos que en las mismas se brindan. Las conclusiones de estos 3 trabajos han sido compiladas dando lugar al libro Defensa del consumidor en la contratación de bienes y servicios informáticos, editado por la Universidad FASTA en 2013 (ISBN 978-987-1312-51-1).

En el año 2012, extendiendo sus actividades de investigación, se firman convenios con el grupo FormaLex de la Facultad de Ciencias Exactas de la UBA, la Universidad Autónoma de Los Andes – UNIANDES y la Federación Iberoamericana de Asociaciones de Derecho Informático – FIADI.

Dos nuevos proyectos de I+D se desarrollan en forma conjunta: Análisis de consistencia de la legislación de Defensa del Consumidor mediante métodos formales con el grupo FormaLex de la Facultad de Ciencias Exactas de la UBA y Diseño de un centro de resolución electrónica de conflictos – CREC con la Universidad Autónoma de Los Andes – UNIANDES. En ambos proyectos se ha desarrollado un fructífero trabajo que ha sido potenciado por el trabajo interdisciplinario y la conjunción de ideas y aportes de investigadores extranjeros.

La sanción de la Ley 26994 en octubre de 2014 y su posterior promulgación, a través de la que entró en vigencia el nuevo Código Civil y Comercial de la Nación, introduce modificaciones en los aspectos vinculados a la tecnología, ya sea en las características que deben tener los contratos celebrados de manera electrónica, como es el caso del contrato para aceptar un CREC, como la firma digital, entre otros. Esto implica una revisión en el trabajo realizado para adaptar el proyecto CREC a la nueva normativa para su correcta implementación. Es así que, en el año 2015 el Grupo de Investigación propone trabajar en un nuevo proyecto: Impacto del nuevo Código Civil y Comercial de la Nación en el Proyecto Centro de Resolución Electrónica de Conflictos.

En ocasión del Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática (CIIDDI) 2015 se abre una nueva oportunidad de trabajo conjunto con otra universidad extranjera, la Universidad Federal de Santa María de Brasil. Se pretende analizar la influencia de las nuevas tecnologías de la información y las comunicaciones en el acceso a la información pública de los poderes de los Estados de América Latina y el Caribe. Es así que, al finalizar el mismo año 2015, se comienza a trabajar en el proyecto: La reconfiguración del Estado en la Sociedad en Red. Experiencias democráticas de promoción de inclusión digital, participación política y transparencia en América Latina y el Caribe. En este proyecto se prevé que podrán sumarse investigadores de otras universidades de la región interesadas en la problemática.

El Grupo de Informática y Derecho articula su labor con las respectivas materias de las carreras de Ingeniería en Informática y Abogacía, integra docentes, graduados y estudiantes, y realiza permanentemente actividades de extensión a la comunidad y asesoramiento. Articula y da marco al trabajo del Grupo de Investigación de Sistemas Operativos e Informática Forense.

El Grupo de Informática y Derecho ha conseguido gran cantidad de publicaciones en los congresos y revistas más importantes de la temática, en 9 países, tales como los Congresos Iberoamericanos de Derecho e Informática, el Congreso Mundial de Ingeniería 2010, y el International Journal "Informatica e diritto" de Italia. Sus integrantes han conformado comités académicos de congresos nacionales e internacionales, han presidido en dos oportunidades el Simposio de Informática y Derecho de las Jornadas Argentinas de Informática (JAIIO) de la Sociedad Argentina de Informática (SADIO) y presidieron y organizaron los Congresos Iberoamericanos de Investigadores y Docentes de Informática y Derecho CIIDDI 2012, 2014 realizados en Mar del Plata, y el CIIDDI 2021 co-

organizado con la UTN Regional Delta y el 2024 co-organizado con la Universidad Champagnat de Mendoza.

La Facultad de Ingeniería es miembro de la FEDERACIÓN IBEROAMERICANA DE DERECHO INFORMÁTICO - FIADI. Además, la Universidad FASTA es miembro fundador y ocupa la Secretaría Permanente de la RED IBEROAMERICANA DE UNIVERSIDADES E INSTITUTOS CON INVESTIGACIÓN EN DERECHO E INFORMÁTICA - Red CIIDDI. En el período 2013-2015 la Universidad FASTA ocupó, también, la presidencia de la Red.

Integrantes del Grupo de Investigación en Informática y Derecho

- Dra. Abg. Bibiana LUZ CLARA (Directora)
- Dr. Abg. Enrique Horacio del CARRIL
- Dr. Abg. Horacio Roberto GRANERO
- Mg. Abg. María Fernanda GIACCAGLIA
- Mg. Ing. Gonzalo RUIZ DE ANGELI
- Abg. María Cecilia OTERO
- Abg. María Soledad GASPARI
- Abg. Antonela D'ONOFRIO
- Abg. María CANZOBRE

6.3.2. **Grupo de Investigación en Informática Forense**

A fines del año 2006 la empresa Microsoft libera el código del kernel de su sistema operativo Windows 2003/Windows XP, y en el marco de su Proyecto OZ invita a los docentes de las materias Sistemas Operativos de todas las Universidades del país a participar de este proyecto.

En la Facultad de Ingeniería de la Universidad FASTA, se conformó un grupo de estudio Proyecto OZ I que tuvo como objetivo principal el estudio del Administrador de Procesos, Administrador de Memoria y Administrador de Dispositivos de Entrada / Salida del kernel del Sistema Operativo Windows 2003/XP y la producción de guías teóricas y prácticas al respecto. Dichas guías fueron administradas a los estudiantes de la materia Sistemas Operativos y forman actualmente parte del contenido práctico de la materia.

La investigación comenzada por este grupo fue continuada en el Proyecto OZ II, que tuvo como objetivo profundizar el estudio del Administrador de Memoria Caché, Dispositivos de Almacenamiento, File System, Networking y Seguridad del kernel del Sistema Operativo Windows 2003/XP y la producción de las guías teóricas y prácticas correspondientes.

A partir de la experiencia adquirida en la administración y alojamiento de la información de sistemas a bajo nivel, el grupo comienza a realizar transferencia y asesoramiento, auxiliando a peritos informáticos de la ciudad que carecían de los conocimientos y técnicas necesarias para la eficiente recuperación de la información en sistemas informáticos. En este contexto, el grupo detecta la inexistencia de metodologías y procesos normados a efectos de la recuperación de la información con valor probatorio, lo que da origen al Proyecto Proceso Unificado de Recuperación de Información – PURI, que tiene por objeto estudiar las técnicas y herramientas disponibles en el mercado para la recuperación de la información, el diseño de propuestas de desarrollo de nuevas técnicas y herramientas y el diseño de un Proceso Unificado de Recuperación de la Información (PURI) que sirva de asistencia a la justicia para mejorar técnicamente la recuperación de la información en pericias.

El Grupo de Informática Forense articula su labor con la asignatura Sistemas Operativos y con la asignatura Informática Forense de la carrera de Ingeniería en Informática, donde en ambas la directora Esp. Ing. Ana Di Iorio es Profesora Titular, integrando docentes, graduados y estudiantes, y realizando permanentemente actividades de extensión y transferencia a la comunidad. En el año 2011, y gracias a los resultados obtenidos, el grupo de investigación migró al proyecto de investigación: "Proceso Unificado de Recuperación de Información (PURI)" que inicia la exploración del área de Informática forense. A su vez, a partir de los resultados alcanzados con ese proyecto, el Grupo de Investigación da inicio a otros 2 que desarrolla en forma concurrente: "Proceso Unificado de Recuperación de la Información en Entornos Distribuidos - PURI en Clusters" y "Proceso unificado de Recuperación de la Información en SmartPhones". Este último, en forma conjunta con la Universidad Autónoma de Los Andes **(**UNIANDES), en el marco de un acuerdo interinstitucional de cooperación.

El año 2014 marca un hito en el grupo de investigación, pues en el marco de un convenio con el Ministerio Público de la Provincia de Buenos Aires, la Municipalidad de Gral. Pueyrredon y la Facultad de Ingeniería de la Universidad FASTA, se integró el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense – InFo-Lab, a través del cual se presentan en el Ministerio de Ciencia, Tecnología e Innovación Productiva, cuatro proyectos que se acreditan como Proyectos de Desarrollo Tecnológico y Social (PDTS). Entre los proyectos del Grupo de Investigación se destacan:

(2007 -2009) Proyecto OZ

Durante el año 2006, Microsoft lanza su proyecto OZ, que consiste en un ambiente experimental basado en un espacio de abstracciones para CPU, MMU y mecanismos TRAP. Estas abstracciones se implementan utilizando las NT APIs del núcleo de Windows Kernel 2003. El Proyecto OZ fue provisto en formato fuente a todas las universidades del país, junto a material especial de estudio. Es así que, sumándose a este proyecto, docentes y estudiantes de la materia "Sistemas Operativos" iniciaron un Grupo de Estudio, dividido en dos etapas.

En la Etapa 1 se trabajó en la instalación y puesta en marcha del proyecto OZ provisto. Luego se estudiaron las características generales del kernel, la Administración de Memoria, la Administración del Procesador y la Administración de Entrada/Salida.

En la Etapa 2 se estudió la Administración de la Memoria Caché, la Administración de Dispositivos de Almacenamiento, la Administración de Archivos, el Sistema de Networking y el Sistema de Seguridad.

De cada uno de los temas abordados se generaron guías de trabajos prácticos que forman parte del material de la cátedra Sistemas Operativos de la carrera Ingeniería Informática de la Universidad FASTA.

(2011-2013) Proyecto PURI: Proceso Unificado de Recuperación de Información

La recuperación de la información en el ámbito de la informática forense puede ser considerada hoy en día un proceso crítico. Una de las mayores problemáticas es la falta de un proceso unificado que guíe a los expertos forenses en la recuperación de la información, y que, también, pueda servir de guía a los operadores de justicia.

El objetivo del proyecto PURI "Proceso Unificado de Recuperación de la Información" fue formalizar un proceso macro que abarque las fases, etapa, tareas, técnicas y herramientas disponibles.

Una vez definido el PURI se validó para los Sistemas Operativos Windows XP, Mac OSX, Linux

Ubuntu y Android, y se detectaron las actividades del proceso carentes de técnicas y herramientas.

La segunda etapa del proyecto estuvo abocada a proponer soluciones a estas carencias, es así que surgen dos temáticas que son las que se abordaron: la validación de archivos recuperados mediante herramientas de File Carving y el desarrollo de un proyecto para recuperación de información de perfil.

(2012 - 2013) Proyecto PURI en Smartphones

El proyecto PURI se centró en la recuperación de información en equipos de computación. Al momento de realizar la validación de PURI se optó por probar su validez en la plataforma Android, detectando la necesidad de un trabajo específico en Dispositivos Móviles, es así que nace este proyecto que consiste en la aplicación, validación y adaptación del proceso unificado "PURI" en Smartphones y la presentación de propuestas de soluciones para las áreas carentes de técnicas y herramientas ad hoc.

El proyecto fue desarrollado por la UNIANDES de Ecuador con la transferencia y colaboración del grupo de investigación de Informática Forense de la Universidad FASTA.

(2012 - 2013) Proyecto CIRA: Framework de File Carving - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto final de graduación presentado por Constanza Ferrara y Agustín Gugliotta.

El File Carving es el proceso de extracción de archivos u objetos del disco en ausencia de metadatos del sistema de archivo, es decir, accediendo directamente al contenido de los bloques. El Framework de CIRA se estructura alrededor de un proceso definido en tres etapas: pre procesamiento, carving y pos procesamiento y está pensado de manera tal que el algoritmo de carving propiamente dicho es ajeno a los detalles de acceso a la imagen de disco "Lectura" y extracción de los archivos "Escritura".

Este proyecto logró desarrollar un Framework de file carving que signifique un aporte a los productos disponibles en la actualidad, constituyendo un marco flexible y extensible, capaz de aplicar diferentes algoritmos y de añadir módulos de preprocesamiento, posprocesamiento y validadores.

(2012 - 2015) Proyecto BIP-M: Búsqueda de Información de Procesos en Memoria - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto final de graduación presentado por Gonzalo Ruiz De Angel y Juan Alberdi.

El proyecto BIP-M tuvo por objetivo el estudio e implementación de un framework de análisis forense de memoria volátil para el Sistema Operativo Windows 7 en sus ediciones de 32 y 64 bits. El proyecto se planteó de forma tal que sus resultados formen una base sobre la cual nuevos proyectos puedan construir nuevo conocimiento y nuevas funcionalidades.

El objetivo de la etapa de desarrollo es el diseño e implementación de un framework extensible y adaptable, apoyándose en patrones de diseño orientados a objetos con el propósito de lograr bajo acoplamiento, alta cohesión y definiendo claramente las diferentes responsabilidades de cada módulo. El framework pretende brindar un marco para analizar la memoria y encontrar cualquier tipo de objeto que se requiera, denominado genéricamente entidades. Un objeto, ya sea un proceso, módulo, conexión, driver, archivo o un nuevo artefacto que se desee contemplar, puede considerarse un tipo especial de entidad y esto permite extender funcionalidad para la búsqueda de nuevos objetos.

(2014 - 2015) Proyecto PURI en Clusters: Proceso Unificado de Recuperación de la Información en Entornos Distribuidos

El objetivo del proyecto fue ampliar el Proceso Unificado de Recuperación de Información – PURI a entornos distribuidos, aplicando particularmente los conceptos forenses de recuperación de evidencia digital a sistemas con redes informáticas, arreglos de discos y cloud computing.

Se realizó el estudio y análisis de las actividades a seguir para la recuperación de la información según las buenas prácticas sugeridas por organismos internacionales en RAID, Cloud Computing y Networking. Se desarrolló, documentó y validó la técnica de recuperación de arreglos de discos para RAID 5 y Sistemas de Archivos NTFS. Esto permitió evolucionar el proceso PURI "Proceso Unificado de Recuperación de Información", a un modelo, a partir del cual puedan construirse los Procesos de acuerdo con el objeto origen de las tareas de Recuperación de Información.

(2014 - 2016) PDTS INVESTIGA: Ambiente integrado de visualización y análisis de datos

El Proyecto INVESTIGA tuvo como objetivo el desarrollo de un sistema informático que permitiera la consolidación de datos provenientes de múltiples fuentes en un ambiente integrado que facilite su visualización gráfica y análisis.

El sistema informático objetivo de este proyecto reemplaza al software que utiliza el Ministerio Público con fines similares, ganando en flexibilidad e independencia tecnológica.

(2014 - 2015) PDTS PAIF-PURI: Protocolo de Actuación en Informática Forense basado en PURI

El Proyecto PAIF-PURI tuvo como objeto la elaboración de una Guía de Actuación en Informática Forense para ser adoptada y promovida por el Ministerio Público de la Provincia de Buenos Aires como estándar oficial de trabajo, tanto para peritos como para investigadores judiciales, en base a lo establecido por el Proceso Unificado de Recuperación de Información.

Dicho proceso ha sido desarrollado por el Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA, formalizando un proceso general que guía a peritos informáticos en la obtención de información digital que pueda ser considerada como evidencia válida por los operadores de justicia.

La Sra. Procuradora General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, bajo resolución 483/16, aprueba y recomienda la aplicación de la Guía Integral de Empleo de la Informática Forense en el Proceso Penal, registrada bajo el ISBN 978-987-1312-73-3.

(2014 - 2017) PDTS FOMO: Forensia en Equipos Móviles

El Proyecto FOMO tuvo como objetivo el desarrollo de un sistema informático que permitiera realizar el análisis forense de la información contenida en equipos de telefonía móvil.

Se pretendía complementar al software privativo y extranjero que utilizaba el Ministerio Público con fines similares; desarrollándose un sistema informático propio específicamente orientado a Smartphones Android, ganando en flexibilidad e independencia tecnológica.

(2014 - 2017) Proyecto FOMO en ANDROID - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Trabajo final de graduación presentado por Sebastián Lasia, Nicolás Battaglia y Gabriel Cardacci.

Vinculado al proyecto FOMO, el proyecto FOMO en ANDROID tuvo como objetivo la búsqueda, extracción forense y análisis de datos en equipos móviles con Sistema Operativo Android en su versión 2.0.

Este proyecto construyó un módulo de la plataforma FOMO, desarrollado de manera tal que pueda integrarse a extracciones forenses de otras herramientas líderes del mercado, tales como UFED y XRY.

(2015 - 2017) PDTS GT-LIF: Guía Técnica para la Implementación de un laboratorio de Informática Forense Judicial

El Proyecto GT-LIF tuvo como objetivo el desarrollo de una Guía Técnica para la implantación de un laboratorio de informática forense para ser utilizada por el Ministerio Público de la Provincia de Buenos Aires (MP) y en el resto de las provincias, a través del Consejo Federal de Procuradores. Esta guía técnica complementa la "Guía integral de empleo de la informática forense en el proceso penal".

El proyecto produjo una guía que permite estimar y evaluar los aspectos claves de diseño de un laboratorio forense a nivel estratégico, institucional, edilicio, estructural y tecnológico.

(2015 - 2018) Proyecto DIMA: Elaboración de indicadores para la detección de malware

El proyecto tuvo por objetivo la elaboración de un documento de Marco Teórico, ejercicios prácticos, casos de prueba y propuesta de indicadores. El proyecto definió un método que permite detectar la presencia de malware en un equipo a partir de indicadores de análisis forense de memoria y tráfico de red.

(2015 - 2016) Proyecto VISOR Web INVESTIGA - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto final de graduación presentado por Martín Delgado y Gerardo Peralta.

Vinculado al proyecto INVESTIGA, el proyecto VISOR Web INVESTIGA tuvo como objetivo el desarrollo de una aplicación local que permita realizar la presentación de los resultados obtenidos mediante el análisis del software INVESTIGA en una estación desconectada de la red y con prestaciones vinculadas a la litigación, y/o exposición ante un magistrado. De esta manera, al análisis de datos se pueden vincular archivos multimedia tal como audio, video o imágenes. El software desarrollado fue entregado al Ministerio Público y está siendo utilizado por el mismo en el Departamento Judicial Mar del Plata.

(2016 - 2017) PDTS BIG DATA INVESTIGA: Sistema de exploración y selección de "Grandes Datos" relacionados a Investigaciones Judiciales

El Proyecto BIG DATA - INVESTIGA tuvo como objetivo el desarrollo de un sistema de exploración y selección de "Grandes Datos" relacionados a Investigaciones Judiciales. El sistema está conformado por una serie de módulos que permiten la constitución del subconjunto de los grandes datos de interés de la investigación judicial de un caso determinado, permitiendo explorar, clasificar, formalizar y consolidar la información disponible proveniente de múltiples fuentes heterogéneas para luego depurarla, detectando y descartando la redundante, inconsistente e irrelevante, y constituyendo finalmente un subconjunto de información relevante y de calidad asegurada a efectos de ser analizado luego por el sistema INVESTIGA a efectos de descubrir patrones en datos complejos que contribuyan a la investigación judicial y a las mejores decisiones procesales.

El proyecto se desarrolló en forma conjunta con la Facultad Regional Delta de la Universidad Tecnológica Nacional.

(2016 - 2019) Proyecto SherloQ Media - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto final de graduación presentado por Jorge Luis Herlein, Martin Blanco, Carlos Mathias y Martin Matus.

Cuando una pericia informática involucra contenido multimedia, ya sean fotografías o videos, queda en el perito informático la tarea de ver, clasificar y determinar la utilidad de los archivos para la investigación, de acuerdo a lo que indican los puntos de pericia.

Hay varios factores que convierten a esta tarea en algo poco deseable: consume mucho tiempo, requiere un cierto nivel de atención que rápidamente se pierde debido a la repetición de una tarea monótona, suele encontrarse una gran cantidad de contenido que no tiene que ver con los puntos periciales y distrae del objetivo, entre otros factores. Además, en la actualidad hay una enorme cantidad de contenido multimedia presente en los dispositivos informáticos.

El proyecto SherloQ Media ha desarrollado una herramienta que a partir de la aplicación de algoritmos y técnicas de visión artificial y procesamiento digital de archivos multimedia permite identificar patrones con el objeto de facilitar la investigación de los peritos informáticos.

(2017 - 2019) SAVE: Herramientas de análisis inteligente de extracciones forenses

El Proyecto SAVE desarrolló una suite de herramientas de software orientada a facilitar el procesamiento, análisis y visualización de datos de manera unificada y coherente. El foco de las herramientas desarrolladas estuvo puesto en la automatización de tareas simples que consumen gran cantidad de tiempo y esfuerzo. Al liberar a los operadores judiciales de las mismas, los prototipos realizados permiten que se enfoque la atención en las tareas de investigación y el análisis de la información con la que se cuenta, permitiendo un trabajo más efectivo y eficiente.

(2017 - 2020) Guía Técnica para la implementación de un Sistema de Gestión de Calidad en un Laboratorio de Informática Forense.

El proyecto tuvo por objeto desarrollar una guía técnica para la implementación de un sistema de gestión de calidad en laboratorios de informática forense. Esta guía pretende colaborar en la resolución de una necesidad de carácter práctico del poder judicial, justificado en el interés y necesidad de contar con laboratorios con acreditada calidad y competencia técnica, desde el personal calificado, métodos normalizados y herramientas debidamente validadas.

(2018) OSINT Investiga - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Trabajo final de graduación presentado por Martín Gamalero y Ezequiel Ramirez.

Software que utilizando técnicas de OSINT (Open Source Intellingence) permite obtener datos de individuos cuya información se encuentra conocida parcialmente. A partir de un dato, y a través de fuentes de datos abiertos, se obtiene nueva información desconocida del individuo.

(2018) Fotografía en la escena del crimen - Trabajo final de graduación de la carrera de Licenciatura en criminalística de la Universidad FASTA.

Trabajo final de graduación presentado por Belén Álvarez - Licenciatura en criminalística, UFASTA.

(2018) Planificación Estratégica de Recursos Humanos del InFo-Lab - Trabajo final de graduación de la carrera de Licenciatura en recursos humanos de la Universidad FASTA.

Trabajo final de graduación presentado por Mariana Greco - Licenciatura en recursos humanos, UFASTA.

Sus principales objetivos fueron sentar las bases del Plan Estratégico de Recursos Humanos de InFo-Lab generando dos productos de gran relevancia: el diccionario de competencias y el manual de puestos del Laboratorio.

(2018 - 2020) PDTS: Proyecto Desarrollo de una Guía de Cuidados de niños, niñas y adolescentes en el Mundo Digital para la Intervención en el Aula.

Es una suite de guías, herramientas y mecanismos para el cuidado, prevención, detección de grupos de riesgo y guías de intervención en casos de ocurrencia. Este proyecto hizo uso de conocimientos científicos y tecnológicos propios de la Informática Forense y recurre a otras disciplinas como la Psicología, la comunicación social y la responsabilidad social institucional, con el fin de crear material didáctico (audiovisual, plataformas digitales y manuales de procedimiento) organizado en una guía que oriente a los educadores en la intervención en el aula frente a los nuevos fenómenos que surgen del uso de las redes sociales entre niños, niñas y jóvenes ocasionando conflictos en la escuela y graves riesgos a la población menor.

(2019) Desarrollo de un Software de Análisis de Texto con Herramientas de Procesamiento de Lenguaje Natural - Proyecto final de graduación de la carrera Ingeniería en informática de la UNMDP.

Proyecto final de graduación presentado por Rodrigo Casanelli y Gerardo Alias.

(2019) Planificación Estratégica para InFo-Lab: el camino para convertirse en un Referente en Investigación, Desarrollo e Innovación en Ciencias de Aplicación Forense en Argentina - Proyecto final de graduación de la carrera de Máster universitario en Dirección Estratégica en Tecnologías de la Información (UNEA)

Proyecto final de graduación presentado por Gonzalo Ruiz De Angeli.

Su objetivo fue el diseño de un Plan Estratégico para InFo-Lab, que consistió en un diagnóstico organizacional y un análisis del entorno para poder identificar fortalezas, debilidades, oportunidades y amenazas y la definición de la misión y visión del Laboratorio. Con esto como base, el diseño de diferentes estrategias y planes de acción que permitan ir alcanzando diferentes objetivos estratégicos que acerquen cada vez más el presente al futuro deseado de InFo-Lab: ser un referente en Investigación, Desarrollo e Innovación en Ciencias de Aplicación Forense en Argentina.

(2019) Plan de Marketing para el InFo-Lab - Proyecto final de graduación de la carrera Tecnicatura en Marketing de la Universidad FASTA.

Trabajo final de graduación presentado por Juan Cruz García - Tecnicatura en Marketing, Ciencias Económicas, UFASTA.

(2019) GLIF – Gestión de Laboratorios de Informática Forense - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto Final Ingeniería Informática presentado por Martín Rodriguez y Bernardo Grande. Se desarrolló un sistema de gestión y automatización de tareas en el proceso de adquisición de pericias informáticas. Esta fase comprende toda actividad vinculada con la generación de una o más réplicas exactas del contenido digital alojado en un dispositivo de almacenamiento. El sistema contempla la generación de dichas réplicas, así como también la distribución de éstas a los distintos equipos heterogéneos dentro de un laboratorio de Informática Forense, agilizando los tiempos del proceso pericial, y permitiendo a los usuarios enfocar su atención en el análisis de los resultados y las

particularidades del caso.

(2019 - 2022) TRIAGE-ED: Herramientas de análisis inteligente de extracciones forenses

El volumen de evidencia que se maneja en las investigaciones judiciales modernas sobrepasa ampliamente la capacidad de lectura, interpretación y análisis que se puede afrontar con recursos humanos. Los operadores de la justicia necesitan de herramientas que les permitan procesar la gran cantidad datos que presentan las investigaciones en pleno Siglo XXI. La Suite integrará productos basados en Inteligencia Artificial (IA) que brindarán diferentes tipos de servicios, tanto mediante programas de usuario disponibles para un entorno global, librerías, y servicios de red. Los desarrollos se acompañarán con la documentación propia de cada uno.

(2019 - 2020) AREX-TI – Análisis, Reconocimiento y Extracción de Texto en Imágenes - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto final de graduación presentado por Javier Angelucci, Pablo Casettai y Mariano Cortinez.

Este proyecto tuvo como objetivo el de herramientas de desarrollo para extraer e indexar el texto de capturas de pantalla con técnicas de Deep Learning

(2019 - 2021) Audiolab - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Proyecto final de graduación presentado por Germán Lopez Fricker y Adriel Chambi.

El objetivo de este proyecto fue el desarrollo de un programa para la transcripción y etiquetado de audios.

(2020 - 2023) Proyecto E-Convivencia: Diseñando Estrategias de Cuidado en la Convivencia Digital

Las nuevas tecnologías forman parte de la convivencia escolar. Hoy la virtualidad es un nuevo espacio social que promueve formas diversas e inéditas de presencialidad, corporeidad y vinculación en el aula.

En esta esfera virtual los jóvenes se encuentran expuestos a situaciones de riesgo derivadas del uso de estas plataformas.

Este espacio digital puede exponer a los adolescentes a que su intimidad quede al descubierto con acciones que pueden provocar impotencia, humillación, vergüenza, dando lugar a un maltrato, hostigamiento y ciberviolencias.

Frente a este escenario la comunidad educativa precisa de la construcción de recursos que permitan abordarlo. Desatender estas problemáticas puede complejizar otras cuestiones estructurales.

Este proyecto implica un trabajo interdisciplinario e interinstitucional para co-construir dispositivos, herramientas y un programa de estrategias para prevenir y abordar problemáticas derivadas de la ciudadanía digital y las ciberviolencias. Esto significa la articulación de tres disciplinas científicas (Psicología, Educación e Informática), El presente proyecto tiene por objetivo el co-diseño, junto a escuelas secundarias de gestión Pública y privada, de un conjunto de estrategias de abordaje de la convivencia digital y problematización de las ciberviolencias, de forma tal de dar respuesta a la demanda emergente del trabajo realizado por el proyecto de extensión permanente de Internet Sana.

La sistematización de las intervenciones en un programa que cuente con estrategias de abordaje de estas problemáticas aportará herramientas comunitarias relevantes y factibles de ser replicadas e

implementadas, con las adaptaciones necesarias.

(2020 - 2023) Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales.

El proyecto busca desarrollar una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales compuesta por tres secciones: Evaluación de Riesgos de Seguridad Informática en Sistemas de Automatización. Recomendaciones para Mitigar los riesgos de Sistemas de Automatización. Actuación para dar Respuesta a Incidentes y Análisis Forense en Sistemas de Automatización.

Esta guía permitirá trabajar tanto ex ante (prevención) como ex post (actuación, remediación, análisis forense) en el abordaje de incidentes de ciberseguridad en infraestructuras que requieren una gestión de extrema seguridad, por su condición de criticidad para la propia organización y la población en general; especialmente, en instalaciones industriales del Estado o de empresas que brindan servicios esenciales (agua, energía, comunicaciones, combustibles, etc). Un problema de seguridad en estas instalaciones puede significar el colapso de servicios vitales para la población. De ahí la importancia de desarrollar un producto tecnológico de soporte a la gestión.

(2021) Protección de datos en las redes sociales - Proyecto final de graduación de la carrera de Abogacía de la Universidad FASTA.

Trabajo final de graduación presentado por Alexis Antoniucci - Abogacía UFASTA

(2021) Sistema de gestión y búsqueda de sentencias judiciales utilizando procesamiento del lenguaje natural - Proyecto final de graduación de la carrera de Ingeniería en informática de la UNMDP.

Trabajo final de graduación presentado por Juan Gumy, UNMDP. El proyecto tuvo como objetivo la implementación de un sistema informático para el Juzgado de Garantías N° 4 de la ciudad de Mar del Plata a utilizar por jueces, abogados y profesionales del área del derecho el cual sería utilizado para la gestión e indexación de las sentencias dictadas por el juzgado. Este trabajo pretendía realizar la aplicación de técnicas del Procesamiento del Lenguaje Natural para el análisis de los textos de las sentencias.

(2021) Autocuidados en el mundo digital. Estudio sobre percepción de riesgos y socialización en la virtualidad - Proyecto final de graduación de la carrera de psicología de la UNMDP.

Trabajo final de graduación presentado por Paula Farfaglia, Lic. en Psicología UNMDP.

(2021 - 2022) Phantom Desktop - Proyecto final de graduación de la carrera Ingeniería en informática de la Universidad FASTA.

Trabajo final de graduación presentado por Javier Mora. El objetivo del presente proyecto fue el desarrollo de un entorno de análisis y procesamiento de imágenes digitales.

(2021 - 2022) Aplicación de la tecnología BlockChain a la Cadena de Custodia - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Cristian Marcos. La preservación de la cadena de custodia en las diferentes pruebas forenses durante un proceso judicial siempre ha sido un hecho de suma importancia. La rotura de la misma supone una causa de nulidad de las pruebas que se desean proteger. Esta preservación históricamente ha estado abocada a las pruebas materiales. Con el

advenimiento de las nuevas y diferentes tecnologías de la información y comunicaciones entre personas, la cantidad de pruebas digitales se ha visto incrementada de forma casi exponencial durante los últimos años. Es por ello que se hace necesario la implementación de algún sistema que permita resguardar tanto la integridad de las pruebas como la integridad de los hechos y personas que han intervenido en una cadena de custodia. Hoy en día la mejor forma, por no decir la única, que se tiene para garantizar la inalterabilidad de la información digital una vez almacenada es la denominada Block Chain o Cadena de Bloques. Es por ello que se propone el uso de dicha tecnología para tal fin.

(2021 - 2022) Desarrollo de una Guía Metodológica para realizar análisis forenses orientados a incidentes en Servidores de Bases de Datos de SQL Server y MySQL - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Verónica Uriarte. Estudio y análisis del funcionamiento de las bases de datos relacionales más relevantes (SQL Server y MySQL) desde el ámbito forense y el desarrollo de una Guía Metodológica para realizar análisis forenses orientados a incidentes en Servidores de Bases de Datos de SQL Server y MySQL

(2021 - 2022) Diseño e implementación del Laboratorio de Informática del COPROCIER - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Silvia Aranguren. Hoy en día los peritos cuentan con muchos desafíos; como ser las diferentes y dinámicas modalidades de los delitos informáticos, el aumento exponencial de la cantidad de información digital y de variedad de dispositivos o soportes de posible evidencia y la incesante evolución tecnológica. La provincia de Entre Ríos cuenta con pocos Laboratorios de Informática Forense; el interés se centra en diseñar un Laboratorio de Informática Forense y procedimientos de calidad para que los peritos que conforman el grupo de peritos del COPROCIER (Colegio de Profesionales de Ciencias Informáticas de Entre Ríos); actúen de manera metódica y utilicen procedimientos que garanticen calidad en el proceso de obtención, análisis, preservación y presentación de información que han sido procesados electrónicamente y/o almacenados en un medio computacional de evidencia digital dentro de un proceso judicial. Este trabajo propone la creación del Laboratorio de Informática Forense en el ámbito del COPROCIER para que los peritos cuenten con herramientas de vanguardia, procedimientos y software especializado para el trabajo pericial apostando siempre a la cultura de la calidad y la mejora continua para que los servicios de este Laboratorio de Informática Forense sean útiles, confiables, oportunos y eficientes.

(2021 - 2022) Análisis de vulnerabilidades sobre redes informáticas - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Mariela Puelman. El objetivo general del trabajo es presentar un análisis de vulnerabilidades y amenazas que pueden afectar a las redes informáticas, y presentar algunas herramientas y técnicas para la detección de evidencias digitales para el análisis forense en redes informáticas.

(2021 - 2022) Informática forense en el ámbito empresarial - Análisis de caso - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Cristian Fernando García. Análisis, abordaje y documentación de un caso real de intrusión indebida en el ámbito empresarial privado, específicamente en una organización del rubro Oil&Gas que ha sido vulnerada e infectada en gran parte de sus activos con un malware del tipo ransomware.

(2021 - 2022) Estudio de la factibilidad y aspectos a considerar para la creación de un laboratorio forense en la Provincia de Formosa - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Andrea Villalba. Estudio de la factibilidad y aspectos a considerar para la creación de un laboratorio forense en la Policía de la provincia de Formosa

(2021 - 2022) Guía de buenas prácticas para la toma de evidencias en redes sociales - Proyecto final de posgraduación de la carrera Especialización en Informática Forense de la Universidad FASTA.

Trabajo final de posgraduación presentado por Verónica Tomich. Elaboración de una guía de buenas prácticas para la toma de evidencias en redes sociales

(2021 - 2023) Desarrollo de un Sistema Integrado de gestión de calidad y de Seguridad de la Información en laboratorios de Informática Forense

El proyecto tuvo como objeto la elaboración de una guía técnica para el desarrollo de un sistema integrado de Gestión de Calidad en Laboratorios de Informática Forense, que incorpora al Sistema de Gestión de la Calidad las normas de Ciberseguridad y Seguridad de la Información relevantes y pertinentes al actuar pericial informático, y que permite tanto su implementación en Laboratorios de Informática Forense judiciales como extrajudiciales. Esta guía técnica complementa, desde el estudio e incorporación de las normas seleccionadas, a las guías ya desarrolladas por el InFo-Lab.

(2021 - 2023) Desarrollo de una Guía de Recomendaciones para la Implementación de Protocolos de Adquisición, Preservación y Presentación de la Prueba Digital - PAFE-CCyLF

El proyecto tuvo como objeto la elaboración de una Guía de actuación y de obtención de evidencia digital destinada a abogados y peritos informáticos de parte y funcionarios judiciales de los fueros civil y comercial, laboral y familia. La Guía de Actuación está integrada por un conjunto de protocolos de extracción, preservación e incorporación de evidencia digital y el modelo de Acordada para su implementación, de manera de facilitar su adopción por cada organización de Justicia Provincial de acuerdo a la particularidad de su código procesal. El proyecto fue desarrollado en forma conjunta por: Universidad FASTA, Universidad Champagnat, Suprema Corte de Justicia de la Provincia de Mendoza, Instituto Federal de Innovación, Tecnología y Justicia - Junta Federal de Cortes y Superiores Tribunales de Justicia de las Provincias Argentinas y Ciudad Autónoma de Buenos Aires (Ju.Fe.Jus) y el Ministerio Público de la provincia de Buenos Aires.

(2022 - 2024) Sistematización y producción de conocimiento en inteligencia artificial y evidencia digital - SPICA.

En los proyectos SAVE (2017) y TRIAGE-ED (2019) se exploró la utilización de herramientas de procesamiento de datos, machine learning, e Inteligencia Artificial para el análisis de volúmenes masivos de evidencia digital. En ellos se crearon prototipos y programas aplicando el conocimiento desarrollado por los investigadores. Este nuevo proyecto busca sistematizar y compilar ese conocimiento generado en los proyectos anteriores, actualizándolo, y desarrollando conocimiento nuevo donde sea pertinente, para proveer una fuente única de referencia en la temática.

(2023) Suspensión de Ruido en Audio Mediante Programas Informáticos - Trabajo final de graduación de la carrera de Licenciatura en Criminalística de la Universidad FASTA.

Proyecto final de graduación presentado por Josefina Riva Posse en la carrera de Licenciatura en

Criminalística, UFASTA.

(2023 - 2024) Validación del desarrollo de un sistema integrado de gestión de calidad y de seguridad de la información en laboratorios de informática forense - SIGYSI-VAL

El proyecto es la continuación del proyecto denominado "SIGYSI-LIF: Desarrollo de un Sistema Integrado de gestión de calidad y de Seguridad de la Información en laboratorios de Informática Forense", y se formula con la intención desarrollar actividades complementarias al proyecto original que permitan la construcción e implementación de la Guía Integrada en el Laboratorio de Informática Forense del Ministerio Público Fiscal, Departamento Judicial Mar del plata y del DigiLab de la FI-UCASAL., con el objeto de, mediante esta validación de la implementación se obtenga una Guía modelo que permita tanto su implementación en Laboratorios de Informática Forense judiciales como extrajudiciales.

(2023 - 2024) Validación y Difusión de Protocolos de Adquisición, Preservación y Presentación de la Prueba Digital - VALPA

Este proyecto, como continuación del proyecto de "Desarrollo de una guía de recomendaciones para la implementación de protocolos de adquisición, preservación y presentación de la prueba digital" pretende desarrollar instrumentos de validación, comunicación, y difusión, de los protocolos de adquisición de sitios web, de adquisición de información de redes sociales, adquisición de información de servicios de mensajería, adquisición de archivos, preservación y presentación desarrollados con la comunidad judicial con el fin de lograr una retroalimentación y validación de los protocolos que facilite la adopción de los mismos por los poderes judiciales provinciales.

(2023 - 2024) Validación y Difusión de Guía para el abordaje de incidentes de Ciberseguridad en Infraestructuras Críticas Industriales – GUIA-ICI

Este proyecto se desarrolla en conjunto con UAI y la Facultad de Ingeniería del Ejército. Este Proyecto, como continuación del proyecto "Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Críticas Industriales", desarrollado en conjunto entre la Facultad de Ingeniería de la Universidad Abierta Interamericana y la Facultad de Ingeniería del Ejercito y Trend Ingeniería como adoptante; con el objeto de generar instrumentos de Validación, Comunicación y Difusión de las guías de identificación y recomendación de riesgos en infraestructuras críticas industriales, y de esta manera lograr una retroalimentación y validación de estos productos que facilite la adopción de los mismos por las empresas u organismos de estas características.

(2024) Desarrollo de una herramienta de análisis automático de texto para usuarios inexpertos del ámbito judicial. Trabajo final de graduación de la carrera de Ingeniería en Informática de la UNMDP.

Trabajo final de graduación presentado por Valentina Fernandez y Pablo Buendia. Con el crecimiento de las comunicaciones digitales, la evidencia judicial proveniente de estos medios ha aumentado exponencialmente, incrementando la complejidad y el tiempo requerido para su procesamiento y análisis. A veces, el volumen de datos supera los recursos disponibles, haciendo indispensable el uso de herramientas de automatización. Este proyecto tiene como objetivo agilizar y mejorar el análisis de evidencia textual, a partir del desarrollo de un sistema que integre modelos de procesamiento de lenguaje natural y los ponga a disposición de usuarios sin experiencia en el campo de la IA.

Integrantes del Grupo de Investigación en Informática Forense

- Ing. Bruno CONSTANZO (Director)

- Esp. Ing. Ana Haydée DI IORIO
- Dra. Abog. Bibiana LUZ CLARA
- Ing. Santiago TRIGO
- Mg. Ing. Gonzalo RUIZ DE ANGELI
- Esp. Abg. Pablo Adrián CISTOLDI
- Lic. Lucía ALGIERI
- Lic. María Belén ALVAREZ CESTANO
- Esp. Ing. Fernanda ROSALES
- Abg. Mario ADARO
- Abg. Fernanda DIAZ
- Abg. Marisa REPETTO
- Ing. Fernando GRECO
- Mg. Ing. Mariela AMBRUSTOLO
- Lic. Abg. Josefina RIVA POSSE
- Dr. Ing. Adolfo ONAINE
- Ing. Marina MIGUELES
- Ing. Enzo NOTARIO
- Esp. Lic. Ezequiel Roberto LAMAS
- Abg. Juliana HUARTE
- Abg. Leonela PANCANI
- Ing. Valentina FERNANDEZ
- Mg. Ing. Hugo Javier CURTI
- Mg. Ing. Gerardo Fabián GONZALEZ

6.3.3. **Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense *InFo-Lab***

El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab es una síntesis de lo que significa el trabajo interdisciplinario, interinstitucional y la contribución de la Universidad a la sociedad y la experiencia de la Universidad FASTA en este campo del conocimiento.

El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) nuclea en la ciudad de Mar del Plata a un equipo interdisciplinario de investigadores científicos y tecnológicos, profesionales y técnicos altamente calificados, con el objeto de desarrollar soluciones a las demandas en el campo de la informática forense y su aplicación. Es, a su vez, la sede del Grupo de Investigación en Informática Forense de la Universidad FASTA.

Ya con diez años de trayectoria, el InFo-Lab es un ejemplo icónico de trabajo interdisciplinario y cooperación interinstitucional para el desarrollo local que sintetiza el desarrollo de la investigación en la Universidad FASTA en este campo y evidencia el efectivo respeto a los principios y directrices definidas en la planificación estratégica institucional.

6.4. CONVENIOS Y MEMBRESÍAS

En el marco del trabajo sostenido en docencia, investigación, extensión y transferencia en el campo de la Ciberseguridad y la Informática Forense, la Facultad de Ingeniería cuenta con los siguientes convenios y/o proyectos interinstitucionales y membresías:

- ATICMA - Asociación de Tecnología de la Información y Comunicaciones de Mar del Plata.
- Agencia Nacional de Seguridad Vial
- Comité Técnico de Calidad en Tecnología de la Información del Instituto Argentino de Normalización y Certificación IRAM.
- Comité Técnico de Gestión de la Innovación del Instituto Argentino de Normalización y Certificación IRAM.
- Comité Técnico de Seguridad y Tecnología de la Información del Instituto Argentino de Normalización y Certificación IRAM.
- COPITEC - Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación
- CPCIBA - Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires
- COPROCIER - Consejo Profesional de Ciencias Informáticas de la Provincia de Entre Ríos
- Colegio de Psicólogos Distrito X
- Colegio de Abogados Provincia Bs As
- Colegio Libre de Estudios Universitarios (México)
- Consejo de la Judicatura de la República de Ecuador
- CYTED - IBERCHIP - Subprograma IX IBERCHIP de Microelectrónica del Programa Iberoamericano de Ciencia y Tecnología para el Desarrollo
- Defensoría del pueblo de la provincia de Santa Fe
- Defensoría del Pueblo del Municipio de General Pueyrredon
- Facultad de Ingeniería del Ejército
- Facultad Porto Alegrense
- FIADI - Federación Iberoamericana de Asociaciones de Derecho Informático
- Fundación Universitaria Católica del Norte
- Universidad Católica de Costa Rica
- Fundación Universitaria Agraria de Colombia
- Fundación GROOMING Argentina
- Intel Argentina
- IRAM - Instituto Argentino de Normalización y Certificación
- IBM
- Industria Argentina de Software
- IUA - Instituto Universitario Aeronáutico
- Instituto Europeo Campus Stellae (España)
- LEFIS - Legal Framework for the Information Society
- MGP - Municipalidad de General Pueyrredon

- Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires
- Ministerio de Seguridad de la provincia de Tucumán
- Procuración de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Ministerio Público Fiscal
- RED CIIDDI - Red de Universidades e Institutos con Investigación en Informática y Derecho
- RED UNIF - Red de Universidades de Informática Forense
- Red de Laboratorios Forenses de Ciencia y Tecnología del Ministerio de Ciencia, Tecnología e Innovación Productiva MinCyT.
- RUSE - Red Universitaria de Sistemas Embebidos
- Servicios Educativos para América Latina S.R.L
- Tecnológico de Antioquia (Colombia)
- Universidad Alcalá
- Universidad Autónoma de Madrid
- Universidad Autónoma (Guadalajara)
- Universidad Alfonso X El Sabio (Madrid, España)
- UCASAL - Universidad Católica de Salta
- Universidad del Aconcagua
- Universidad del Cono Sur
- Universidad Católica de Córdoba
- Universidad Champagnat
- Universidad Camilo Cela (España)
- Universidad Carolina del Norte (Colombia)
- Universidad de Concepción del Uruguay
- Universidad de Jaen (España)
- UniLibre Colombia
- Universidad del Cono Sur de las Américas (UCSA)
- Universidad Miguel Hernández de Elche (Alicante, España)
- Universidad Maimonides
- Universidad Santo Tomás de Mozambique (Brasil)
- Universidad Nacional de Amazonia Peruana
- Universidad Nacional del Centro de la Provincia de Buenos Aires (UNICEN)
- Universidad Nacional del Noroeste de la Provincia de Buenos Aires (UNNOBA)
- Universidad Panamericana (México)
- Universidad Republicana (Colombia)
- Universidad de Ixtlahuaca (México)
- Universidad de la Vera
- UChile - Universidad de Chile – Facultad de Derecho (Chile)
- Universidad del Bio Bio (Chile)

- Universidad Particular de Chiclayo (Perú)
- Universidad de Santo Tomas (Chile)
- Universidad Rey Juan Carlos (Madrid, España)
- UNIFAFIBE (Brasil)
- UFSM - Universidad Federal de Santa María (Brasil)
- Universidad de Granada (España)
- UNIANDES - Universidad Regional Autónoma de los Andes (Ecuador)
- UNNOBA - Universidad Nacional del Noroeste de la Provincia de Buenos Aires
- UPM - Universidad Politécnica de Madrid. Grupo de Validación y Aplicaciones Industriales de la Escuela Técnica Superior de Ingenieros Informáticos
- USAL - Universidad de Salamanca (España)
- UTN FRD - Universidad Tecnológica Nacional. Facultad Regional Delta (Argentina)
- Poder Ejecutivo de la Provincia de Santa Cruz

7. **OBJETO**

En un contexto caracterizado por la complejidad técnica propia de la ciberseguridad y la informática forense, la dinámica y permanente evolución de las tecnologías de la información y comunicación, así como la ciberdelincuencia y las problemáticas relacionadas con los procesos y herramientas propias de la Informática Forense, requiere de profesionales de la informática experimentados y debidamente formados para desarrollar una efectiva actuación en el ámbito de la ciberseguridad y la informática forense. La Facultad de Ingeniería de la Universidad FASTA, a través del Grupo de Investigación en Informática Forense, ha diseñado y propone esta carrera de MAESTRÍA EN CIBERSEGURIDAD E INFORMÁTICA FORENSE, que tiene por objeto **la articulación de la informática, el derecho y la criminalística para la resolución de problemáticas vinculadas a las ciberseguridad y la informática forense**, sea que éstas se desarrollen en el ámbito judicial, extrajudicial o en otros espacios en los que se demande de profesionales con este perfil.

Se pretende que los profesionales que cursen y culminen esta carrera desarrollen las competencias necesarias para prevenir, detectar y dar respuesta a las situaciones de ciberseguridad propias de este tiempo, así como la adecuada y ética investigación y práctica forense, incorporando los conceptos, conocimientos, técnicas, herramientas y prácticas actualizados respecto del estado del arte de la ciberseguridad y la informática forense.

8. **OBJETIVOS DE LA CARRERA**

Esta carrera tiene como objetivo mejorar el desempeño de los profesionales de la informática en el campo de la ciberseguridad y la informática forense, a partir del perfeccionamiento de los aspectos técnicos, legales, criminológicos y éticos que le permitan responder a las demandas de las organizaciones respecto de problemáticas vinculadas a la ciberseguridad, ciberdelitos y ciberdelincuencia.

Desde el punto de vista institucional, la Universidad FASTA propone con este proyecto la continuación de su política de responder a demandas de formación en ciberseguridad e informática forense, creando la primera carrera específica de maestría en la República Argentina, que aborda dos

temáticas muy relacionadas: ciberseguridad e informática forense, en modalidad a distancia, para llegar con la oferta académica a los profesionales interesados en la materia en todo el territorio nacional e internacional de habla hispana.

La carrera de Maestría en Ciberseguridad e Informática Forense tiene como propósito formar profesionales con competencias técnicas, procedimentales, legales y éticas, que le permitan tratar y resolver problemas vinculados a la ciberseguridad y a la informática forense.

El alcance de esta propuesta, plasmada en los contenidos que se abordan, está definido desde la problemática de la ciberseguridad poniendo el foco en las personas y considerando el avance de la ciberdelincuencia en el contexto de los escenarios digitales que se están desarrollando. La formación del Magíster en Ciberseguridad e Informática Forense le permitirá desempeñarse en cualquier ámbito empresarial y/o institucional que busque prevenir, detectar y mitigar los incidentes de ciberseguridad.

Desde el punto de vista social el desarrollo de esta carrera permitirá compartir los conocimientos, métodos, técnicas, herramientas y experiencias del Grupo de Investigación y el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense con los posgraduandos y contribuir así a la formación de profesionales que demanda el contexto digital de nuestra época.

9. CONTEXTO Y DEMANDA POTENCIAL DE LA CARRERA

9.1. CONTEXTO REGIONAL Y NACIONAL

El mundo vive una revolución de la información, una transformación que implica de manera directa a las personas y sus relaciones. La información digital es cada vez más necesaria y su utilización masiva se evidencia como creciente y sin posibilidad de retorno para los Estados y todas sus áreas institucionales.

Año a año se incrementa a nivel global y de manera sostenida el volumen de contenido digital que las personas producen y consumen en promedio. En Argentina, durante el cuarto trimestre del año 2023, el 88.4% de la población utilizó internet y de éstos un 72.5% lo hizo a través de un dispositivo móvil. Y lo mismo sucede con las causas penales que involucran delitos informáticos: en el año 2020 hubo 9.604 delitos informáticos investigados, y en el 2021 ese número creció a 11.593 denuncias.

Cuanto mayor sea la penetración de la tecnología en la vida cotidiana, mayor será la necesidad de capacidad de investigación y actuación forense sobre esa información a efectos de proteger a las personas e instituciones, obteniendo evidencias digitales que permitan descubrir lo sucedido, sea esto un hecho punible o no y soportar y potenciar el proceso de investigación. Esto es una necesidad no solo en el campo judicial, sino también en la que respecta a la detección y prevención de incidentes perjudiciales o ilegales mediante uso de la tecnología, tales como intrusiones y malware, fundamentalmente por el creciente desarrollo de la delincuencia virtual.

Asimismo, la creación de los Cuerpos de Investigación Judicial tanto en la provincia de Buenos Aires como en todo el país, como el requerimiento de expertos en resolver ataques de intrusión indebidos en las organizaciones en general, hacen prever una demanda creciente del auxilio de la Ciberseguridad y la Informática Forense para su actuación efectiva.

Por ello, la ciberseguridad como área de estudio, y la Informática Forense como disciplina integrante son cada vez más importantes, necesarias y demandadas, tanto en el ámbito de la justicia como en el de las organizaciones preocupadas por la protección de su infraestructura tecnológica.

Los organismos responsables de la Defensa y la Justicia requieren cada vez más capacidad de investigación y actuación forense, lo que supone mayor necesidad de laboratorios debidamente adecuados al efecto de la tarea pericial y, fundamentalmente, de expertos en informática forense. Asimismo, el avance de los incidentes de ciberseguridad es una de las principales preocupaciones de las empresas de hoy en día. Esto genera un contexto nacional de alta necesidad y demanda insatisfecha.

9.2. **DEMANDA POTENCIAL DE LA CARRERA**

La ciberseguridad se encarga de la preservación de la confidencialidad, integridad, autenticidad y disponibilidad de la información en el ciberespacio, poniendo el eje en la seguridad de las personas, de los ciudadanos. La ciberseguridad contempla la problemática de los delitos informáticos (diferente a los incidentes de seguridad informática) donde, por ejemplo, la ingeniería social puede dar lugar a ellos, sin que conformen un problema de seguridad informática. La ciberseguridad no se reduce a una cuestión técnica de la informática, ni es sinónimo de "seguridad informática".

El avance de incidentes de ciberseguridad que generan perjuicios en las organizaciones que requieren de profesionales expresamente formados en ciberseguridad que puedan dar respuesta al incremento de la demanda que en tal sentido requieren las mismas. Las instituciones miran con mucha preocupación la situación de vulnerabilidad en la que se encuentran frente al avance de los incidentes de ciberseguridad, muchos de los cuales incluso se tratan de ciberdelitos, tales como las intrusiones indebidas y los secuestros de datos. Estas situaciones demandan la necesidad de dar una rápida respuesta de acción inmediata, así como actuar en la prevención.

Prueba fehaciente de esta demanda puede apreciarse en el constante interés por la carrera de Especialización en Informática Forense, que se imparte desde el año 2021, y el desarrollo continuo de las acciones de formación de recursos humanos y transferencia realizadas por el Grupo de Investigación en Informática Forense en atención a demandas de diferentes actores e instituciones.

El análisis del contexto local y nacional permitió detectar señales que marcan la necesidad de profesionales informáticos con competencias en Ciberseguridad e Informática Forense, tales como:

- El 2° Protocolo del **Convenio de Budapest**, que fuera firmado por nuestro país en el año 2021, y tiene por objeto afianzar los lazos en materia de cooperación internacional y facilitar la obtención de evidencia electrónica para poder brindar una respuesta eficaz en la investigación criminal para trabajar contra el ciberdelito.
- Las diversas respuestas de la **Unión Europea** a la ciberdelincuencia quien, atenta al crecimiento de los ciberdelitos, está trabajando fuertemente en la definición de políticas, estrategias, normas y acciones de culturización, respecto de los retos de la ciberdelincuencia, la ciberresilencia, la ciberdiplomacia y la ciberdefensa.
- La normativa de la **Dirección Nacional de Ciberseguridad** de nuestro país cuenta con numerosos documentos técnicos entre las que se destacan la Resolución 580/2011 que crea del Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad, la Disposición 1/2021 que crea el Centro Nacional de Respuestas a Incidentes Informáticos (CERT.ar) en el ámbito de la Dirección Nacional de Ciberseguridad y la Resolución 829 / 2019 que aprueba la Estrategia Nacional de Ciberseguridad.
- La Resolución 86/22 del **Ministerio de Seguridad de la Nación** aprueba el "PROGRAMA DE FORTALECIMIENTO EN CIBERSEGURIDAD Y EN INVESTIGACIÓN DEL CIBERCRIMEN

(ForCIC)" que tiene como objetivo coordinar, asistir y brindar asesoramiento en técnicas de seguridad de las infraestructuras digitales y en técnicas de investigación en materia de ciberdelitos y delitos con presencia de la tecnología y/o utilización de tecnologías. En el marco de este programa, emitió además la Resolución 232/23 que aprueba el "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital: El Ministerio de Seguridad de la Nación mediante Resolución 232/23 aprobó el protocolo para la identificación, recolección, preservación, procesamiento, y presentación de evidencia digital.

En el nuestro país también se observan normas legales que van a requerir de profesionales con formación avanzada en Ciberseguridad e Informática Forense. Tal es el caso de la Provincia de Salta, en el año 2023 se aprobó la Ley 8.386, que contiene ocho artículos con textos que incorporan las nuevas herramientas para la investigación de delitos informáticos. Este articulado está referido específicamente a los aspectos procesales de la evidencia digital, incorporando medidas como el Aseguramiento de datos, la orden de presentación de datos informáticos, el registro y secuestro de datos informáticos, la interceptación de datos de tráfico y de contenido y la investigación encubierta de en entornos digitales.

Por su parte, la provincia de Mendoza ha incorporado a partir del año 2023 la figura del Agente Encubierto digital, enmarcando esta disposición en el cumplimiento del Convenio de Budapest, con el fin de proteger a la sociedad de los delitos informáticos.

Estos precedentes provinciales hacen prever su extensión en todas y cada una de las provincias, con el consecuente requerimiento de profesionales calificados para su abordaje.

En ese contexto, se prevé una demanda potencial suficiente y creciente para la carrera de Maestría en Ciberseguridad e Informática Forense.

10. PERFIL DEL EGRESADO

Se espera que, al finalizar la carrera de Maestría en Ciberseguridad e Informática Forense, el profesional postgraduado sea capaz de:

1. Reconocer el fenómeno de inclusión de la TI en la sociedad y sus efectos, y analizarlo tanto desde la perspectiva técnica, legal y ética.
2. Reconocer y aplicar las técnicas y herramientas para la implementación de medidas de ciberseguridad de una infraestructura tecnológica, adecuadas a su contexto.
3. Formular políticas de ciberseguridad en las organizaciones.
4. Formular planes de concientización y prevención con el objetivo de minimizar los riesgos y el impacto de posibles ataques a las organizaciones.
5. Formular los planes de ciberseguridad y definir las estrategias de contención y primera respuesta ante un ataque.
6. Colaborar en la implementación de planes de ciberseguridad en infraestructuras digitales de producción y de servicios, considerando su criticidad.
7. Identificar y analizar las vulnerabilidades y riesgos de una infraestructura tecnológica.
8. Mitigar y controlar riesgos de ciberseguridad mediante la elaboración y administración de planes para disminuir la probabilidad de ocurrencia de incidentes y el impacto que estos generan.
9. Aplicar las respuestas a incidentes de ciberseguridad acorde al alcance y profundidad del evento ocurrido.

a) Aplicar estrategias de investigación sobre casos reales e hipotéticos de ataques con el fin de evaluar los sistemas de seguridad informática de la organización.
b) Identificar a las partes interesadas ante un incidente de ciberseguridad.
c) Elaborar esquemas y reportes de notificación de los incidentes ante las autoridades correspondientes

10. Obtener evidencias digitales residentes en equipos informáticos, en software de aplicación, en sistemas operativos, en sistemas de archivos y en las estructuras de administración de memoria.
    a) Extraer información de diferentes plataformas tecnológicas respetando los principios de las buenas prácticas forenses.
    b) Analizar la información obrante en un sistema informático a partir de una secuencia temporal de hechos.
    c) Describir las tareas, métodos y técnicas utilizadas en una actividad forense.
    d) Comunicar la actividad forense realizada, en un lenguaje acorde al público objetivo, respetando la terminología propia de la actividad.
11. Recuperar evidencia digital en entornos de redes y dispositivos móviles, mediante el uso de técnicas y herramientas específicas y adecuadas.
12. Realizar análisis forense de los incidentes de ciberseguridad para la obtención de evidencias digitales
13. Procesar y analizar archivos multimedia con el objeto de obtener la información específica requerida.
14. Reconocer el marco de actuación de los informáticos forenses en términos legales, de criminalística y de investigación judicial.
15. Identificar el conjunto de técnicas y herramientas de seguridad informática y criptografía a utilizar de acuerdo al caso en el que se actuará.
16. Diferenciar las actividades de respuesta a incidentes y de ciberdefensa respecto de las de informática forense y pericias informáticas.
17. Actuar con integridad ética y responsabilidad acorde a las normas técnicas y legales vigentes

A continuación, se presenta la MATRIZ DE TRIBUTACIÓN, que muestra la relación entre las competencias consideradas en el perfil profesional y las asignaturas que tributan al desarrollo de dichas competencias.

COMPETENCIA	ASIGNATURAS
Reconocer el fenómeno de inclusión de la TI en la sociedad y sus efectos, pudiendo analizarlos tanto desde la perspectiva técnica, legal y ética.	Introducción a la Ciberseguridad
	Introducción a la Informática Forense
	Seminario de Derecho Informático
	Ética de la Ciberseguridad
	Aspectos criminológicos y técnicos de la Ciberseguridad
	Ciberseguridad en la Nube y en Infraestructuras Críticas
	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas
Reconocer las técnicas y herramientas a aplicar en la implementación de medidas de ciberseguridad de una infraestructura tecnológica adecuada a su contexto.	Introducción a la Ciberseguridad
	Gestión de la Ciberseguridad
	Ciberseguridad en la Nube y en Infraestructuras Críticas

COMPETENCIA	ASIGNATURAS
Formular políticas de ciberseguridad en las organizaciones	Gestión de la Ciberseguridad
	Normas técnicas de la Ciberseguridad
	Derecho, Aspectos legales y de cumplimiento normativo de la Ciberseguridad
Formular planes de concientización y prevención con el objetivo de minimizar los riesgos y el impacto de posibles ataques a las organizaciones.	Gestión de la Ciberseguridad
	Derecho, Aspectos legales y de cumplimiento normativo de la Ciberseguridad
	Normas técnicas de la Ciberseguridad
Formular los planes de ciberseguridad y definir las estrategias de contención y primera respuesta ante un ataque.	Derecho, Aspectos legales y de cumplimiento normativo de la Ciberseguridad
	Normas técnicas de la Ciberseguridad
Colaborar en la implementación de planes de ciberseguridad en infraestructuras digitales de producción y de servicios, considerando su criticidad.	Gestión de la Ciberseguridad
	Ciberseguridad en la Nube y en Infraestructuras Críticas
	Normas técnicas de la Ciberseguridad
Identificar y analizar las vulnerabilidades y riesgos de una infraestructura tecnológica.	Aspectos criminológicos y técnicos de la Ciberseguridad
	Ciberseguridad en la Nube y en Infraestructuras Críticas
	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas
	Taller de Análisis de Riesgos de las Infraestructuras Tecnológicas
Mitigar y controlar riesgos de ciberseguridad mediante la elaboración y administración de planes para disminuir la probabilidad de ocurrencia de incidentes y el impacto que estos generan.	Gestión de la Ciberseguridad
	Ciberseguridad en la Nube y en Infraestructuras Críticas
	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas
	Taller de Análisis de Riesgos de las Infraestructuras Tecnológicas
	Normas técnicas de la Ciberseguridad
Aplicar las respuestas a incidentes de ciberseguridad acorde al alcance y profundidad del evento ocurrido.	Taller de análisis Forense de Redes y Dispositivos Móviles
	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas
	Ciberdefensa, Criptografía y Seguridad en Redes
	Gestión de la Ciberseguridad
Aplicar estrategias de investigación sobre casos reales e hipotéticos de ataques con el fin de evaluar los sistemas de seguridad informática de la organización.	Metodología de la Investigación
	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas
	Gestión de la Ciberseguridad
	Trabajo Final Integrador
Identificar a las partes interesadas ante un incidente de ciberseguridad.	Derecho, Aspectos legales y de Cumplimiento Normativo de la Ciberseguridad
	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas
	Normas técnicas de la Ciberseguridad
Elaborar esquemas y reportes de notificación de los	Derecho, Aspectos legales y de Cumplimiento

COMPETENCIA	ASIGNATURAS
incidentes ante las autoridades correspondientes	Normativo de la Ciberseguridad
	Actuación Forense, Criminalística e Investigación Judicial
	Normas técnicas de la Ciberseguridad
	Gestión de la Ciberseguridad
Obtener evidencias digitales residentes en equipos informáticos, en software de aplicación, en sistemas operativos, en sistemas de archivos y en las estructuras de administración de memoria.	Introducción a la Informática Forense
	Recuperación de Datos y Análisis de Archivos Multimedia
	Taller de Análisis Forense de Memoria
	Taller de Análisis Forense de Redes y Dispositivos Móviles
Extraer información de diferentes plataformas tecnológicas respetando los principios de las buenas prácticas forenses.	Introducción a la Informática Forense
	Recuperación de Datos y Análisis de Archivos Multimedia
	Actuación Forense, Criminalística e Investigación Judicial
	Taller de Análisis Forense de Memoria
	Taller de análisis Forense de Redes y Dispositivos Móviles
Analizar la información obrante en un sistema informático a partir de una secuencia temporal de hechos.	Recuperación de Datos y Análisis de Archivos Multimedia
	Actuación Forense, Criminalística e Investigación Judicial
	Auditoría y Seguridad Informática
	Taller de Análisis Forense de Memoria
	Taller de análisis Forense de Redes y Dispositivos Móviles
	Metodología de la Investigación
	Taller de Análisis de casos
Describir las tareas, métodos y técnicas utilizadas en una actividad forense.	Introducción a la Informática Forense
	Recuperación de Datos y Análisis de Archivos Multimedia
	Actuación Forense, Criminalística e Investigación Judicial
	Taller de Análisis de casos
Comunicar la actividad forense realizada, en un lenguaje acorde al público objetivo, respetando la terminología propia de la actividad.	Actuación Forense, Criminalística e Investigación Judicial
	Taller de Análisis de casos
Recuperar evidencia digital en entornos de redes y dispositivos móviles, mediante el uso de técnicas y herramientas específicas y adecuadas.	Recuperación de Datos y Análisis de Archivos Multimedia
	Ciberdefensa, Criptografía y Seguridad en Redes
	Taller de análisis Forense de Redes y Dispositivos Móviles
Realizar análisis forense de los incidentes de ciberseguridad para la obtención de evidencias digitales	Ciberdefensa, Criptografía y Seguridad en Redes
	Taller de Análisis Forense de Redes y Dispositivos Móviles
Procesar y analizar archivos multimedia con el objeto de obtener la información específica requerida.	Recuperación de Datos y Análisis de Archivos Multimedia

COMPETENCIA	ASIGNATURAS
Reconocer el marco de actuación de los informáticos forenses en términos legales, de criminalística y de investigación judicial.	Seminario de Derecho Informático
	Actuación Forense, Criminalística e Investigación Judicial
	Taller de Análisis de casos
Identificar el conjunto de técnicas y herramientas de seguridad informática y criptografía a utilizar de acuerdo al caso en el que se actuará.	Auditoría y Seguridad Informática
	Ciberdefensa, Criptografía y Seguridad en Redes
Diferenciar las actividades de respuesta a incidentes y de ciberdefensa respecto de las de informática forense y pericias informáticas.	Auditoría y Seguridad Informática
	Ciberdefensa, Criptografía y Seguridad en Redes
	Taller de análisis de Casos
	Gestión de la Ciberseguridad
Actuar con integridad ética y responsabilidad acorde a las normas técnicas y legales vigentes	Ética de la Ciberseguridad
	Normas técnicas de la Ciberseguridad
	Derecho, Aspectos legales y de Cumplimiento Normativo de la Ciberseguridad

11. **PERFIL DEL INGRESANTE**

La carrera está dirigida a profesionales de la informática, las ciencias de la computación y/o sistemas de información, u otros títulos asimilables de grado de al menos 4 años de duración, que estén implicados o interesados en la ciberseguridad y en la actuación forense y pretendan incorporar conocimientos específicos en la materia y desarrollar competencias para su aplicación en el campo profesional - laboral.

Excepcionalmente se contemplará el ingreso de postulantes que se encuentren fuera de los términos precedentes, siempre que demuestren, a través de las evaluaciones y los requisitos que la Comisión Académica de la carrera y la reglamentación vigente establezcan, poseer la preparación y experiencia laboral acorde con los estudios de posgrado que se proponen iniciar así como aptitudes y conocimientos suficientes para cursarlos satisfactoriamente. En cualquier caso, la admisión y la obtención del título de posgrado no acredita de manera alguna el título de grado anterior correspondiente al mismo (Art. 39 Bis LES).

12. **MARCO INSTITUCIONAL DE LA CARRERA**

12.1. **NORMATIVA INSTITUCIONAL**

La Universidad FASTA prevé la siguiente normativa en materia de posgrado en general y de la Maestría en Ciberseguridad e Informática Forense en particular:

- Resolución del Decano de la Facultad de Ingeniería Nº 258/24 por la cual se aprueba el Reglamento de la carrera de Maestría en Ciberseguridad e Informática Forense.
- Resolución del Rector Nº 443/24 por la cual se designa a los directores de la carrera de Maestría en Ciberseguridad e Informática Forense.
- Resolución del Rector Nº 444/24 por la cual se designa a los integrantes de la Comisión Académica de la carrera de Maestría en Ciberseguridad e Informática Forense.
- La presente Resolución del Rector por la cual se aprueba la creación de la carrera de Maestría en Ciberseguridad e Informática Forense.

La normativa citada *ut supra* se adjunta como Anexo de esta presentación.

12.2. **UBICACIÓN EN LA ESTRUCTURA INSTITUCIONAL**

La carrera de Maestría en Ciberseguridad e Informática Forense pertenece y se desarrolla en la Facultad de Ingeniería de la Universidad FASTA, en la órbita de la Secretaría Académica. Complementa la oferta de las carreras de grado de Ingeniería en Informática y Licenciatura en Ciberseguridad, y la carrera de posgrado de Especialización en Informática Forense. Tiene como marco académico e institucional al conjunto de actividades de docencia, extensión e investigación que se presentan como antecedentes, buscando la retroalimentación y enriquecimiento mutuo entre todas las funciones.

13. PLAN DE ESTUDIOS

13.1. **ESTRUCTURA CURRICULAR**

Asignatura	**Horas de Interacción Docente**			**Horas Semanales**	**Hs. Trabajo Autónomo**	**Hs. Totales**	**Créditos**
	Horas Teóricas	Horas Prácticas	**Total**				
PRIMER AÑO							
Introducción a la Informática Forense	25	5	30	10	70	100	4
Seminario de Derecho Informático	20	10	30	10	45	75	3
Recuperación de Datos y Análisis de Archivos Multimedia	20	40	60	10	190	250	10
Actuación Forense, Criminalística e Investigación Judicial	30	10	40	10	85	125	5
Taller de Análisis Forense de Memoria	10	25	35	10	215	250	10
Auditoría y Seguridad Informática	20	10	30	10	45	75	3
Ciberdefensa, Criptografía y Seguridad en Redes	30	20	50	10	75	125	5
Taller de Análisis Forense de Redes y Dispositivos Móviles	10	25	35	10	215	250	10
Taller de Análisis de Casos	10	40	50	10	200	250	10
SEGUNDO AÑO							
Introducción a la Ciberseguridad	30	10	40	10	85	125	5
Aspectos criminológicos y técnicos de la Ciberseguridad	20	20	40	10	85	125	5
Gestión de la Ciberseguridad	20	20	40	10	85	125	5
Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas	10	25	35	10	65	100	4
Derecho, Aspectos legales y de Cumplimiento Normativo de la Ciberseguridad	20	10	30	10	95	125	5
Metodología de la Investigación	20	10	30	10	20	50	2

Ciberseguridad en la Nube y en Infraestructuras Críticas	20	25	45	10	80	125	5
Taller de Análisis de Riesgos de las Infraestructuras Tecnológicas	10	25	35	10	65	100	4
Buenas Prácticas y Normas Técnicas de la Ciberseguridad	30	10	40	10	35	75	3
Ética de la Ciberseguridad	20	10	30	10	20	50	2
Trabajo Final Integrador	10	40	50	10	450	500	20
TOTALES	**385**	**390**	**775**		**2225**	**3000**	**120**

(*) Los créditos se calculan a razón de 25 horas cada uno, respetando lo dispuesto por la Resolución Ministerial N° 2598/23.

13.2. **DURACIÓN Y CARGA HORARIA**

La carrera de Maestría en Ciberseguridad e Informática Forense tiene una duración de 24 meses (4 semestres) para el cursado de todas las asignaturas. Tiene una carga horaria de 3.000 horas reloj equivalentes a 120 créditos académicos, distribuidas en 19 asignaturas teórico-prácticas que totalizan 2.500 horas equivalentes a 100 créditos académicos y un Trabajo Final Integrador de 500 horas equivalentes a 20 créditos académicos.

Dado el perfil de la carrera con acento en la investigación y práctica forense y en ciberseguridad, se promueve en los docentes el método de enseñanza por medio del estudio de casos prácticos con análisis de diferentes alternativas de resolución, posibilitando en el estudiante el aprendizaje basado en problemas.

Las actividades de formación práctica se realizarán en los espacios virtuales definidos por cada asignatura, en función de los contenidos y herramientas que se deban utilizar, y cada asignatura será responsable de implementar las acciones de seguimiento y acompañamiento necesarias que garanticen las habilidades y destrezas con que se intenta formar a los estudiantes, recurriendo para ello a la infraestructura tecnológica (hardware, software, servidores, máquinas virtuales, etc.) que la institución pone a disposición de la carrera.

13.3. **ESQUEMA DE CORRELATIVIDADES**

El cursado de cada asignatura está condicionado por el cursado de las asignaturas correlativas anteriores, conforme el siguiente esquema:

PRIMER AÑO		
#	**Asignatura**	**Correlativa Anterior (#)**
1	Introducción a la Informática Forense	--
2	Seminario de Derecho Informático	--
3	Recuperación de Datos y Análisis de Archivos Multimedia	1
4	Actuación Forense, Criminalística e Investigación Judicial	1

5	Taller de Análisis Forense de Memoria	3
6	Auditoría y Seguridad Informática	1
7	Ciberdefensa, Criptografía y Seguridad en Redes	3
8	Taller de Análisis Forense de Redes y Dispositivos Móviles	3 y 7
9	Taller de Análisis de Casos	3
SEGUNDO AÑO		
#	**Asignatura**	**Correlativa Anterior (#)**
10	Introducción a la Ciberseguridad	7 y 9
11	Aspectos criminológicos y técnicos de la Ciberseguridad	7 y 9
12	Gestión de la Ciberseguridad	10
13	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas	10 y 11
14	Derecho, Aspectos legales y de Cumplimiento Normativo de la Ciberseguridad	10 y 11
15	Metodología de la Investigación	9
16	Ciberseguridad en la Nube y en Infraestructuras Críticas	13
17	Taller de Análisis de Riesgos de las Infraestructuras Tecnológicas	16
18	Buenas Prácticas y Normas Técnicas de la Ciberseguridad	14 y 15
19	Ética de la Ciberseguridad	14 y 15
-	Trabajo Final Integrador	12, 17, 18 y 19

13.4. **ORGANIZACIÓN DEL DICTADO**

La carrera de Maestría en Ciberseguridad e Informática Forense se cursará en modalidad “a distancia”, soportada por la plataforma de educación a distancia de la Universidad FASTA. Las asignaturas se desarrollarán en sus respectivas aulas virtuales.

Cada asignatura está planteada para ser dictada en módulos, con contenidos teóricos y ejemplos, casos y ejercitación práctica que motivarán el debate e interacción virtual entre los estudiantes, y entre los estudiantes y docentes.

La ejercitación práctica se realizará sobre máquinas virtuales específicamente diseñadas para la docencia más otras herramientas definidas por los docentes en cada cátedra, montadas sobre servidores de propósito específico para la docencia. En estos servidores, los estudiantes podrán realizar sus prácticas simulando las condiciones reales de trabajo de un experto forense que opera sobre un dispositivo determinado. Asimismo, en esos mismos servidores, los estudiantes tendrán a su

disposición todas las herramientas de software libre disponibles en el mercado a efectos de su aplicación en cada caso a resolver, según corresponda. Esta plataforma y modalidad de desarrollo de los trabajos prácticos, siempre orientados a casos, es la misma que se viene utilizando con excelentes resultados en la carrera de Especialización en Informática Forense que dicta la Unidad Académica, en tanto significa la simulación de un entorno real de trabajo pericial.

13.5. **CONTENIDOS MÍNIMOS**

PRIMER AÑO

Introducción a la Informática Forense

Ciencia y Técnica. El método científico. Informática Forense. Pericias Informáticas. Evidencia Digital. Proceso Unificado de Recuperación de la Información: PURI. Conceptos básicos de Sistemas Operativos.

Seminario de Derecho Informático

Relaciones entre informática y derecho. Derecho informático. Informática Jurídica. Datos Personales. Protección de datos.

Recuperación de Datos y Análisis de Archivos Multimedia

La Imagen Forense: obtención, restauración, preservación, decomiso. Extracción de datos. Estructuras de Almacenamiento y de gestión de espacio libre. Estructuras de Arranque. RAID. File Carving. Data Carving. Técnicas y Herramientas de Recuperación de Archivos y de Datos. Análisis Forense. Procesamiento digital.

Actuación Forense, Criminalística e Investigación Judicial

Introducción a la Criminalística. Ciencias Forenses. Principios Forenses. El proceso de Investigación Criminal. Metodología de la Investigación. Cadena de Custodia. Estructura Judicial. Litigación. Protocolo de Actuación en Informática Forense. Delitos Informáticos. La Prueba. El dictamen pericial.

Taller de Análisis Forense de Memoria

Memoria Persistente y Volátil. Organización de la memoria. Estructuras de interés. Rootkits. Malware. Virus. Recuperación de Información en Memoria.

Auditoría y Seguridad Informática

Auditoría informática. Seguridad de la Información. Seguridad Informática. Ataques Informáticos.

Ciberdefensa, Criptografía y Seguridad en Redes

Criptografía. Sistemas de Cifrado. Protocolos y Esquemas Criptográficos. Certificados y Firmas Digitales. PKI. Políticas y Estándares de Certificación. Ciberataques y Ciberdefensa.

Taller de Análisis Forense de Redes y Dispositivos Móviles

Redes informáticas. Seguridad en comunicaciones inalámbricas, en redes de datos móviles y en comunicaciones de bajo alcance. VoIP. Recuperación de Información en Dispositivos Móviles. Recuperación de Información en Redes Informáticas.

Taller de Análisis de Casos

Análisis de casos reales e hipotéticos, utilizando herramientas y técnicas de recuperación de

información.

SEGUNDO AÑO

Introducción a la Ciberseguridad

Conceptos básicos de ciberseguridad. Introducción a la ciberseguridad en infraestructuras críticas digitales, industriales y de producción y servicios. Relación de la ciberseguridad con la seguridad informática, la seguridad de la información y la auditoría informática. Conceptos básicos de ciberdelitos, cibercrimen y escenarios delictivos digitales. Aspectos criminológicos.

Aspectos criminológicos y técnicos de la Ciberseguridad

Ingeniería Social. Amenazas pasivas, ataques y códigos maliciosos. Tipos de Malware. Clasificación. Ataques de denegación de servicio. Ciberataques masivos: ataques, defensa y prevención. Botnets. Sistemas de detección de intrusión. Inteligencia Artificial en ciberseguridad. Criptoactivos. Relación de la ciberseguridad con el ciberdelito, el cibercrimen y los escenarios delictivos digitales, crimen organizado, evolución histórica de los ataques y amenazas.

Gestión de la Ciberseguridad

Gestión de identidad y controles de acceso físico y lógico. Sistemas de autenticación. Planes y Gestión de incidentes. Planes de respuesta y contingencias. Planes, técnicas y normas de identificación, evaluación y control de riesgos y amenazas en el ciberespacio. Gestión integrada de la ciberseguridad. Elaboración del programa de ciberseguridad y Plan de Continuidad de Negocio. Políticas de ciberseguridad de la organización y Ciberresiliencia. Generación de la cultura de ciberseguridad: Comunicación interna y externa. La gestión de las cibercrisis en la empresa y en la administración pública. Impacto de la concientización de la ciberseguridad en las personas y las organizaciones.

Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas

Vulnerabilidad tecnológica de una organización. Tipos de vulnerabilidades. Aplicación, configuración e implementación de infraestructuras seguras. Diseño seguro. Pentesting y Hacking ético. Tipos de hacking según la infraestructura tecnológica

Derecho, Aspectos legales y de Cumplimiento Normativo de la Ciberseguridad

Organización y estructura del área de seguridad. Centro de Operaciones de Seguridad. Normas nacionales e internacionales sobre ciberseguridad. Delitos Informáticos: legislación nacional e internacional. Gobierno de las TIC y ciberseguridad. IT Compliance. Gobernanza de Internet. Instituciones que regulan el espacio digital.

Metodología de la Investigación

Conceptos fundamentales sobre la investigación científica y tecnológica. Los fines de la investigación. Publicaciones científicas, herramientas para la referenciación bibliográfica. Acceso y uso de las bibliotecas electrónicas. El equipo de investigación y la ética de los investigadores. Metodologías orientadas a la Investigación Aplicada y al Desarrollo Tecnológico

Ciberseguridad en la Nube y en Infraestructuras Críticas

Tipos de infraestructura en la nube y modelos de alta disponibilidad. Arquitecturas de seguridad en redes. Vulnerabilidad y Riesgos específicos de ciberseguridad en la nube y en infraestructuras críticas. Seguridad de infraestructuras críticas digitales, industriales y de producción y servicios.

Taller de Análisis de Riesgos de las Infraestructuras Tecnológicas

Relación de los sistemas de gestión de calidad y la gestión del riesgo. Gestión de Riesgos . Metodologías Ágiles para la Gestión de Riesgos. Herramientas. Mapas.

Buenas Prácticas y Normas técnicas de la Ciberseguridad

Estándares de seguridad informática: COBIT, ITIL, OWASP. La serie de normas ISO/IEC 27000. Normativas emanadas de instituciones técnicas reconocidas (IEEE, NIST, y otras.). Buenas prácticas: Desarrollo seguro de software. Metodologías.

Ética de la Ciberseguridad

Ética, responsabilidad profesional y responsabilidad social. Ética en la era digital. Inteligencia y sentido. Inteligencia humana e inteligencia artificial. Inteligencia y emociones. Importancia de la protección y privacidad de la información. La ética frente al acceso indebido a los datos. Impacto de la ciberseguridad en poblaciones vulnerables. Internet Sana.

Trabajo Final Integrador

El Trabajo Final Integrador se centrará en el tratamiento de una problemática acotada en el campo de la ciberseguridad y la informática forense.

Podrá optar por el formato de un proyecto, un estudio de casos, una obra, una tesis que dan cuenta de una aplicación innovadora o producción personal que, sostenida en marcos teóricos, evidencian resolución de problemáticas complejas, propuestas de mejora, desarrollo analítico de casos reales y que estén acompañadas de un informe escrito que permita evidenciar la integración de aprendizajes realizados en el proceso formativo. La presentación formal debe reunir las condiciones de un trabajo académico, conforme el reglamento ad hoc.

El estudiante debe presentar su propuesta de trabajo avalada por un especialista que lo dirija. La presentación de esta propuesta conforme a los requisitos solicitados es condición para la aprobación de la cursada de esta materia.

El Trabajo Final Integrador será individual y el estudiante deberá realizar una presentación y defensa oral virtual, mediante sistemas de telecomunicaciones multimedia.

Para la presentación del Trabajo Final Integrador, los estudiantes deberán haber cursado todas las asignaturas de la carrera para poder iniciar su trabajo final y deberán haber aprobado todas las asignaturas de la carrera para poder presentar su trabajo final.

Los estudiantes podrán convocar en carácter de director o tutor a los docentes de la carrera o bien a reconocidos profesionales de la disciplina, con título de posgrado y/o méritos suficientes en el campo científico o tecnológico que corresponda.

El estudiante dispone de 6 (seis) meses, a partir de la finalización y aprobación de la cursada, para la presentación de su Trabajo Final Integrador.

13.6. SISTEMA DE EVALUACIÓN

La evaluación está prevista para el seguimiento y desarrollo de las competencias explicitadas en el perfil del egresado con el fin de comprobar las habilidades que el estudiante vaya desarrollando. Se aplicará la evaluación de procesos, como así también la autoevaluación.

El sistema de educación a distancia de la Universidad FASTA incluye una importante innovación en lo

referente a evaluaciones en línea. Se trata de un completo desarrollo que cuenta con diferentes instrumentos de evaluación que gestiona el profesor responsable de cada asignatura. Partimos de un concepto de evaluación comprensiva e integral, convencidos de que el uso de las herramientas tecnológicas de comunicación sincrónica (chat, sala virtual de videoconferencia, audio conferencias) y asincrónicas (Web, foros de discusión, correo electrónico, sistema de mensajería por campus virtual, textos en línea y archivos de trabajo) favorecen los procesos de enseñanza y de aprendizaje. El Sistema de Evaluación en Línea cuenta con técnicas objetivas (valoración cuantitativa) y técnicas subjetivas (valoración cualitativa). En la Resolución Rectoral N° 402/17 de aprobación del SIED de la Universidad FASTA se describen detalladamente las características, técnicas e instrumentos de evaluación disponible para los procesos de enseñanza-aprendizaje de esta carrera. Algunos de los instrumentos de evaluación propuestos son el *múltiple choice*, resolución de casos, trabajos analíticos y de campo, trabajos de evaluación de procesos, productos y tecnologías, informe de desarrollo, participación en Wikis y foros como herramientas que proveen los entornos virtuales de aprendizaje, ajustándose al Reglamento de la carrera aprobado por Resolución del Decano de la Facultad de Ingeniería Nro. 258/24.

Para la obtención del título de Magister en Ciberseguridad e Informática Forense es condición que los estudiantes hayan aprobado todas las asignaturas, a partir de sistema de seguimiento y acreditación de las mismas y el correspondiente Trabajo Final Integrador.

13.7. **SEGUIMIENTO CURRICULAR**

Tal como prevé la normativa de la carrera de posgrado que se presenta, los mecanismos de seguimiento serán desarrollados en las diversas instancias por medio de distintas metodologías e indicadores que muestran el alcance y desarrollo de las competencias establecidas en el perfil.

La Comisión Académica de la carrera evaluará el desarrollo total de la carrera y sus actividades. La Dirección hará el seguimiento académico y administrativo de su desarrollo.

Toda la información necesaria será remitida a la Secretaría Académica de la Facultad para hacer el seguimiento formal del proceso formativo, asegurando y propendiendo al mejoramiento continuo de la calidad educativa.

Los mecanismos previstos son:

- Seguimiento de la adecuación de las actividades propuestas por los docentes, a partir de la planificación y secuenciación de contenidos en función del desarrollo de las competencias previstas en el perfil, favoreciendo el aprendizaje, mediante el registro en la plataforma.
- Seguimiento del desarrollo de actividad de los estudiantes, tendiente a la aplicación de las competencias previstas en el perfil, mediante el registro en la plataforma y de las producciones realizadas.
- Seguimiento de indicadores que miden el cumplimiento de las competencias en torno al perfil del egresado.
- Seguimiento de tasas de regularidad y aprobación de exámenes (aprobación, desaprobación, a cargo de la Comisión Académica sobre la base de los datos provistos por el Sistema Integrado de Información de la Universidad FASTA - SIUF)
- Seguimiento de tasas de graduación, deserción y desgranamiento del grupo de estudiantes que cumplieron con la cursada y le resta la realización del Trabajo Final Integrador correspondiente.
- Encuesta de satisfacción a los estudiantes, realizada luego de la finalización de la cursada.

Al finalizar el cursado el estudiante habrá alcanzado competencias y habilidades previstas en cada asignatura, habiendo sido supervisado por los docentes, quienes se convierten en tutores permanentes que aseguran la orientación y seguimiento del proceso de formación de los estudiantes.

13.8. **SEGUIMIENTO DE ESTUDIANTES Y EGRESADOS**

La Dirección Académica de la carrera, conjuntamente con la Dirección Ejecutiva y la Secretaría Administrativa de la carrera, tienen a su cargo la organización de los sistemas de control y registración académica y administrativa. La Universidad cuenta con el Sistema integrado de Información de la Universidad FASTA (SIUF) que administra los datos de estudiantes, docentes y actividades académicas de la Universidad. El sistema gestiona el ciclo completo de información de los estudiantes desde su ingreso y matriculación en la Universidad hasta su egreso de la misma.

El sistema de información involucra la gestión académico-administrativa desde los niveles operativos de atención al estudiante, formando un datawarehouse que brinda un panel de control gerencial para asistir en la toma de decisiones.

Asimismo, cuenta con un subsistema que atiende los requisitos para las carreras de posgrado que administre la Universidad. La funcionalidad más destacada del panel de control gerencial incluye el control y seguimiento de indicadores académicos generales y comparados por facultades y carreras (actividad docente, rendimiento académico, entre otros) y administrativos como el control presupuestario, seguimiento de cobranzas.

El SIUF brinda también información directa a los estudiantes y docentes en forma *on line* a través de internet. Para ello, pone a disposición el sistema SIUF Web donde los estudiantes consultan información personalizada sobre su situación académico-administrativa.

En cuanto a los aspectos formativos, la Plataforma de Educación a Distancia de la Universidad FASTA brinda todas las herramientas para facilitar el seguimiento académico de los estudiantes, permitiendo la consulta on line de su actividad y el diálogo permanente docente-estudiante y entre los mismos estudiantes (foros, chats, teleconferencias, videoconferencias, etc.). Toda la actividad queda registrada en la plataforma, incluso los mismos exámenes.

La Comisión Académica participa junto con las áreas institucionales de la Universidad FASTA en la definición de las políticas y procesos de seguimiento de estudiantes y es responsable junto con la dirección de la carrera de la aplicación de dichos procedimientos, especialmente en lo que respecta a la identificación y seguimiento de posibles casos de deserción y desgranamiento de los estudiantes.

En cuanto al seguimiento de egresados, cabe señalar que la Facultad de Ingeniería de la Universidad FASTA tiene una fluida relación con ellos, más allá del lugar de radicación de los mismos. Los egresados se nuclean en el Centro de Graduados de la Facultad de Ingeniería (CGI). La Unidad Académica lleva un archivo actualizado de la situación laboral de sus miembros y listas de distribución de correspondencia electrónica y trabaja en forma conjunta con el CGI en su mantenimiento. Por medio de las redes sociales también se generan canales de comunicación e información fluida con los graduados.

14. **NORMATIVA PARTICULAR DE LA CARRERA**

La Facultad de Ingeniería de la Universidad FASTA aprobó mediante Resolución del Decano Nº 258/214 el reglamento propio de la carrera, en el que se establecen los requisitos de ingreso y

permanencia en la carrera, la modalidad de cursado y evaluación de las asignaturas, las características específicas de los trabajos finales, las funciones de las autoridades de la carrera, etc.

15. **REQUISITOS DE INGRESO**

Son requisitos de ingreso a la carrera de Maestría en Ciberseguridad e Informática Forense:

- **a.** Poseer título profesional de informática, sistemas de información o ciencias de la computación, electrónica, tales como Ingeniero, Licenciado, u otro asimilable de grado universitario, con pertinencia al perfil de la carrera, de al menos 4 años de duración, expedido por universidades argentinas reconocidas por el Ministerio de Educación de la Nación Argentina o extranjeras.
- **b.** Presentar copia del Documento Nacional de Identidad, copia del título certificada o certificado analítico original del título de base a partir del cual solicita la inscripción, curriculum vitae y 2 fotografías 4x4 color. Los estudiantes extranjeros deben presentar copia del certificado analítico de estudios, copia de título universitario debidamente legalizado, copia del pasaporte, curriculum vitae y 2 fotografías 4x4 color.
- **c.** Abonar la matrícula correspondiente.

En el caso de los postulantes que no cuenten con un título de grado conforme lo expresado en (a.) la Comisión Académica de la carrera definirá las evaluaciones, requisitos y mecanismos administrativos para dictaminar respecto de su admisibilidad en base a la preparación y experiencia laboral debidamente respaldada y acorde con los estudios de posgrado que pretende cursar, en el marco de lo establecido por la reglamentación específica de la carrera.

16. **CUERPO ACADÉMICO**

Se considera como cuerpo académico a los directores de la carrera, los miembros de la comisión académica de la carrera, el cuerpo docente, los directores y codirectores de trabajos finales. Los integrantes del cuerpo académico poseen formación de posgrado equivalente a la ofrecida por la carrera y acorde con los objetivos de esta o una formación equivalente demostrada por sus trayectorias como profesionales, docentes e investigadores.

Tanto las funciones y responsabilidades de la Directora Académica, Director Ejecutivo y Comisión Académica de la carrera se enuncian en el Reglamento de Carrera que acompaña esta presentación.

16.1. **STAFF DE GESTIÓN DE LA CARRERA**

Directora Académica
Dra. Ing. H. Beatriz Parra de Gallo

Director Ejecutivo
Mg. Ing. Gonzalo Ruiz De Ángeli

Decano Facultad de Ingeniería
Esp. Ing. Roberto Giordano Lerena

Vicedecana Facultad de Ingeniería
Lic. Sandra Cirimelo

Secretario Académico Facultad de Ingeniería

Ing. Roberto Sotomayor

Secretaría Administrativa
Tec. Virginia Sebastián

16.2. **COMISIÓN ACADÉMICA DE LA CARRERA**

Dra. Ing. H. Beatriz Parra de Gallo (Directora Académica de la carrera - UFASTA)

Esp. Ing. Roberto Giordano Lerena (Decano de la Facultad de Ingeniería - UFASTA)

Mg. Ing. Hugo Curti (UFASTA)

Mg. Ing. Gerardo González (UFASTA)

Mg. Ing. Miguel Solinas (UNC)

Mg. Ing. Gonzalo Ruíz De Ángeli (UFASTA)

16.3. **STAFF DOCENTE DE LA CARRERA**

Profesores de la Universidad FASTA afectados

Dra. Lic. Fabiola BALTAR

Mg. Ing. Maximiliano BENDINELLI

Mg. Ing. Eduardo CASANOVAS

Esp. Abg. Pablo CISTOLDI

Esp. Ing. Pablo CROCI

Mg. Ing. Hugo CURTI

Esp. Ing. Ana DI IORIO

Mg. Ing. Gerardo GONZALEZ

Mg. Ing. Jorge KAMLOFSKY

Dra. Abg. Bibiana LUZ CLARA

Mg. Abg. Oscar MATO

Dr. Ing. Gustavo MESCHINO

Mg. Ing. Guillermina NIEVAS

Dra. Ing. Beatriz PARRA de GALLO

Mg. Abg. Hernán QUADRI

Pbro. Dr. Lic. Alejandro RAMOS

Mg. Ing. Gonzalo RUIZ DE ÁNGELI

Mg. Lic. Gustavo SAIN

Ing. Santiago TRIGO

Profesores invitados

Mg. Ing. Cintia GIOIA (UNLaM)

Dr. Ing. Adolfo ONAINE (UNMdP)

Dra. Ing. Lía OROSCO (UCASAL)

Mg. Ing. Hugo PÁGOLA (UBA)

Mg. Ing. Marcela PALLERO (UNTRES, UP)

Mg. CPN Patricia PRANDINI (UBA, UNSM)

Mg. Ing. Diego ROMERO (UBA)

Esp. Abg. Daniel SHURTJIN (UBA)

Mg. Ing. Miguel SOLINAS (UNC)

16.4. **DOCENTES POR ASIGNATURA**

PRIMER AÑO			
#	**Asignatura**	**Docente Responsable**	**Docentes Asociado**
1	Introducción a la Informática Forense	Mg. Ing. Maximiliano BENDINELLI	Esp. Ing. Ana DI IORIO
2	Seminario de Derecho Informático	Dra. Abg. Bibiana LUZ CLARA	Mg. Abg. Hernán QUADRI
3	Recuperación de Datos y Análisis de Archivos Multimedia	Mg. Ing. Hugo CURTI	Dr. Ing. Gustavo MESCHINO
4	Actuación Forense, Criminalística e Investigación Judicial	Mg. Lic. Gustavo SAIN	Esp. Abg. Sabrina Lamperti
5	Taller de Análisis Forense de Memoria	Mg. Ing. Gonzalo RUIZ DE ANGELI	Esp. Ing. Pablo CROCI
6	Auditoría y Seguridad Informática	Dra. Ing. Beatriz P. DE GALLO	Mg. Ing. Guillermina NIEVAS
7	Ciberdefensa, Criptografía y Seguridad en Redes	Mg. Ing. Eduardo CASANOVAS	Mg. Abg. Oscar MATO, Mg. Ing. Jorge KAMLOFSKY
8	Taller de Análisis Forense de Redes y Dispositivos Móviles	Mg. Ing. Hugo CURTI	Ing. Santiago TRIGO
9	Taller de Análisis de Casos	Mg. Ing. Maximiliano BENDINELLI	Esp. Abg. Pablo CISTOLDI
SEGUNDO AÑO			
10	Introducción a la Ciberseguridad	Mg. Ing. Cintia GIOIA	Mg. Lic. Gustavo SAIN
11	Aspectos criminológicos y técnicos de la Ciberseguridad	Mg. Ing. Hugo PÁGOLA	Mg. Ing. Eduardo CASANOVAS
12	Gestión de la Ciberseguridad	Mg. Ing. Gerardo GONZALEZ	Ing. Santiago TRIGO

13	Taller de Identificación de Vulnerabilidades de las Infraestructuras Tecnológicas	Mg. Ing. Miguel SOLINAS	Mg. Ing. Hugo CURTI
14	Derecho, Aspectos legales y de Cumplimiento Normativo de la Ciberseguridad	Mg. Ing. Marcela PALLERO	Esp. Abg. Daniel SHURTJIN
15	Metodología de la Investigación	Dra. Lic. Fabiola BALTAR	Dra. Ing. Lía OROSCO
16	Ciberseguridad en la Nube y en Infraestructuras Críticas	Mg. Ing. Gerardo GONZALEZ	Mg. Ing. Diego ROMERO
17	Taller de Análisis de Riesgos de las Infraestructuras Tecnológicas	Mg. CPN Patricia PRANDINI	Dr. Ing. Adolfo ONAINE
18	Buenas Prácticas y Normas técnicas de la Ciberseguridad	Mg. Ing. Guillermina NIEVAS	Mg. Ing. Pablo CROCI
19	Ética de la Ciberseguridad	Pbro. Dr. Lic. Alejandro RAMOS Dra. Ing. Beatriz P. DE GALLO	Mg. Ing. Gonzalo RUIZ DE ANGELI
-	Trabajo Final Integrador	Dra. Ing. Beatriz P. DE GALLO	Mg. CPN Patricia PRANDINI

16.5. **ANTECEDENTES DEL STAFF DOCENTE DE LA CARRERA**

Dra. Lic. Fabiola BALTAR

Licenciada en Economía (UNMdP). Master en Economía y Desarrollo Industrial con especialización en PYMES (UNGS). Master Oficial en Organización Industrial; mercado y empresas (Universitat Rovira i Virgili, Tarragona, España) Doctora en Economía y Empresa (Universitat Rovira i Virgili, Tarragona, España). Profesor investigador en Universidad Nacional de Mar del Plata

Mg. Ing. Maximiliano BENDINELLI

Ingeniero en Sistemas Informáticos (UAI), Especialista en Seguridad Informática (UBA) y Maestría, Seguridad Informática y de Sistemas de Información (UBA). Docente de la Maestría en Seguridad Informática (UBA). Líder de Informática Forense e Ingeniero en Seguridad Informática de la Corte Suprema de la República Argentina. Amplio conocimiento y experiencia en seguridad de redes, respuesta a gestión de incidentes, amenazas cibernéticas y computación en la nube.

Mg. Ing. Eduardo CASANOVAS

Ingeniero Electrónico (UNDEF), Especialista en Telecomunicaciones (UNC), Especialista en Criptografía, Seguridad Teleinformática, Seguridad Informática y de Sistemas (UNDEF); Magister en Ciencias de la Ingeniería (UNC). Es director de la carrera de Maestría en CIberdefensa de la IUA. Co-fundador & CTO en Capazeta.

Esp. Abog. Pablo CISTOLDI

Es Abogado y Procurador por la Facultad de Derecho de la Universidad de Buenos Aires y Especialista en Derecho Penal por la Universidad Nacional de Mar del Plata. Es Fiscal del Ministerio Público Fiscal del Departamento Judicial Mar del Plata desde el año 2003. Es Investigador del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredon y Universidad FASTA.

Fue docente de las cátedras de Derecho Penal II y Criminología en la Universidad Atlántida Argentina, es docente del Curso de Formación de Instructores Judiciales para el Ministerio Público Fiscal. Es coautor del libro "Justicia de Garantías, de Ejecución y Ministerio Público" (Riquert, Cistoldi, Celsi) y de la "Guía Integral de Empleo de la Informática Forense en el Proceso Penal basada en el Proceso Unificado de Recuperación de Información (PAIF-PURI)". Universidad FASTA, 2015. Tiene una activa participación en actividades de extensión universitaria del InFo-Lab y del Grupo de Investigación en Sistemas Operativos e Informática Forense.

Esp. Ing. Pablo CROCI

Ingeniero Electrónico (UBA), Especialista en Seguridad Informática y Criptografia (UNDEF) y Maestrando en Ciberdefensa (UNDEF). Analista Investigador en Informática Forense. Perito Judicial Informático. Consultor Técnico Judicial. Consultor de Seguridad en la Información. Docente e Investigador Universitario. Profesor de la cátedra de Taller de Análisis Forense de Memoria", en la Especialización de Informática Forense (UFASTA). Docente de la Especialización de Cibercrimen (USIGLO21). Docente de coordinación de talleres de investigación en el Instituto de Ciberdefensa de las Fuerzas Armadas. Miembro de la Comisión de Informática Forense del Instituto Argentino de Normalización y Certificación (IRAM).

Mg. Ing. Hugo CURTI

Ingeniero de Sistemas (UNICEN) y Magíster en Ingeniería de Sistemas (UNICEN) Profesor Adjunto en la Facultad de Ciencias Exactas de la misma Universidad. Es Profesor Adjunto en la asignatura de Sistemas Distribuidos de la Facultad de Ingeniería de la Universidad FASTA.

Es Consultor de Sistemas Informáticos y participa como investigador en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA.

Enfocado principalmente en la formación de Recursos Humanos de alta calidad en el área de Sistemas, tanto a nivel técnico como humano. La experiencia obtenida se centra en dictado de cursos, participación en proyectos de investigación y desarrollo, dirección de proyectos de desarrollo, y la formación de equipos de trabajo.

Esp. Ing. Ana DI IORIO

Es Ingeniera en Informática de la Universidad FASTA y Especialista en Gestión de la Tecnología y la Innovación de la Universidad Nacional de Mar del Plata. Ha realizado y aprobado el curso de Posgrado Capacitación en Ciencias Forenses de la Universidad Nacional de La Plata y tiene pos-título de Formación Docente para Profesionales y Técnicos. Es Instructor Informático en el Ministerio Público de la provincia de Buenos Aires. Es docente en la carrera de posgrado Especialización en Criminalidad Económica de la Facultad de Derecho de la Universidad de Castilla La Mancha y de la Universidad Nacionalidad de Mar del Plata, del Curso de posgrado de Actualización en Derecho Informático de la Universidad de Buenos Aires y del Curso de posgrado en Forensia Digital de la Universidad Católica de Salta. Es director del Programa de Actualización Profesional en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Es director del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab, integrado por la Universidad FASTA, el Ministerio Público de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon, donde dirige, además, los siguientes proyectos acreditados como Proyectos de Desarrollo Tecnológico y Social: INVESTIGA “Ambiente Integrado de Análisis y Visualización de Datos”, PAIF-PURI “Protocolo de Actuación en Informática Forense basado en PURI”, FOMO “Plataforma de Análisis Forense para Dispositivos Móviles”, GT-LIF “Guía Técnica para la

Implementación de Laboratorios de Informática Forense" y BIG DATA INVESTIGA "Sistema de exploración y selección de "Grandes Datos" relacionados a Investigaciones Judiciales". En la Universidad FASTA es Profesor Asociado con dedicación afectada a docencia e investigación. Se desempeña como Profesor en las materias Informática y Derecho y Sistemas Operativos de la Facultad de Ingeniería, y en la materia Derecho Informático de la Facultad de Ciencias Jurídicas y Sociales. En lo que hace a investigación, se desempeña como Directora del Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Actualmente dirige también el proyecto "Elaboración de Indicadores para la detección de Malware" y participa del proyecto "La reconfiguración del Estado en la Sociedad en red. Experiencias democráticas de promoción de inclusión digital, participación política y transparencia en América Latina y el Caribe – ALC en la Sociedad en Red" con la Universidad Federal de Santa María de Brasil. Trabaja e investiga en el área de informática y derecho desde hace más de diez años, habiendo participado en varios proyectos relacionados con la temática, entre ellos, el Proyecto "Ontojuris", con el I3G de Brasil y la Universidad Politécnica de Madrid y el proyecto "Diseño de un Centro de Resolución Electrónica de Conflictos" realizado en conjunto con la Universidad UNIANDES de Ecuador. Ha dirigido, entre otros, los Proyectos "Proceso Unificado de Recuperación de la Información – PURI", "PURI en Dispositivos Móviles" realizado en conjunto con la Universidad UNIANDES de Ecuador y "Análisis de Consistencia de la Legislación de Defensa del Consumidor por Métodos Formales", realizado en conjunto con el Grupo de Investigación FORMALEX de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. En la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata es Jefe de Trabajos Prácticos de las cátedras de Sistemas Operativos y Diseño de Sistemas Operativos. Es Coordinadora de la Comisión Asesora de la Red de Laboratorios Forenses del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación. Fue integrante de la Mesa de Trabajo de la Red de Laboratorios Forenses del Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación durante el año 2014/2015. Ha presentado y publicado trabajos en numerosos congresos nacionales e Internacionales. Ha presidido el III Congreso Iberoamericano de Investigadores y Docentes en Derecho e Informática (2014), el Simposio de Derecho e Informática de la Jornada Argentina de Informática (2007 y 2009) y ha sido Secretaria General del Congreso Iberoamericano de Investigadores y Docentes en Derecho e Informática (2012). Es co-autora del libro Defensa del consumidor en la contratación de bienes y servicios informáticos, editado por la Universidad FASTA (2013). Integra el Consejo Editorial de la Revista Argentina de Ingeniería – RADI de Argentina (ISSN 2314-0925), el Consejo Editorial de la Revista Direitos Emergentes na Sociedade Global – REDESG de la Universidad Federal de Santa María de Brasil (ISSN 2316-3054), el Comité Evaluador de la Revista Ingeniería Solidaria de la Universidad Cooperativa de Colombia (ISSN 1900-3102/e-ISSN 2357-6014), el Comité Evaluador de la Revista Democracia Digital e Governo Eletrônico de la Universidad Federal de Santa Catarina de Brasil (ISSN 2175-9391), y el Comité Científico de Arbitraje de la Revista Ventana Informática de la Universidad de Manizales. Es integrante del Comité Técnico de Tecnología de la Información – Subcomité de Seguridad, del Instituto Argentino de Normalización y Certificación – IRAM. Es Secretaria Permanente de la Red Iberoamericana de Universidades e Institutos con Investigación en Derecho e Informática - Red CIIDDI.

Mg. Ing. Cintia V. GIOIA

Magister en Informática (UNLaM).Ing. en Informática (UNLaM). Especialista en Criptografía y Seguridad Teleinformática (EST). Especialista en Informática Forense. Coordinadora de las carreras de Tecnicatura Web y para Móviles (UNLaM). Gerente de proyectos de Desarrollo de Sistemas, Seguridad de la Información, Calidad y Auditoría de Sistemas. Perito Informática.

Mg. Ing. Gerardo GONZALEZ

Es Ingeniero en Sistemas de información (UTN), posgrado en UADE “Management Executive Program” y “Marketing Digital” (UB). Más de 18 años como Docente en distintas disciplinas y Universidades: Universidad Tecnológica Nacional (UTN FRBA), en la actualidad de la materia "Ciberseguridad Industrial“, en la carrera Ing. en Sistemas de Información. Ha dictado también Habilitación Profesional, Planeamiento y Ctrl de Gestión y Algoritmos y modelos de datos; Universidad de la Defensa (UNDEF), Facultad de ingeniería del Ejército (FIE) e Instituto Universitario Aeronáutico de Córdoba, dictando la materia "Infraestructuras Críticas" en la Maestría de Ciberdefensa; ESAN Perú – Diplomatura Ciberseguridad para empresas de Sector Energético. Módulo 2: Ciberseguridad Industrial e IICC y UNSTA – Universidad del Norte Santo Tomas de Aquino – Diplomatura Ciberseguridad en Sistemas Industriales. Más de 30 años de trayectoria en Telecomunicaciones, Sistemas y Ciberseguridad IT y OT. Certificado por ISA en todos los módulos (4) de la Norma internacional IEC62443. Ha escrito libros de divulgación tecnológica acerca de “Internet de las cosas” y el uso de “Energías renovables” (Discovery (2021). España y Argentina. ISBN: 978-84-18267-28-4-00018 y 978-84-17472-59-7-00012). Desempeñó cargos de diversa responsabilidad en empresas de gran envergadura de Argentina como FiberTel, AESA e YPF entre otras. Hoy se desempeña como consultor externo experto en Ciberseguridad Industrial, en forma independiente, asesorando, realizando distintos assessment y dictando cursos de concientización y capacitación a empresas privadas y gubernamentales, principalmente en Latinoamérica.

Mg. Ing. Jorge KAMLOFSKY

Ingeniero Electrónico (UTN), Licenciado en Matemáticas (UAI), Especialista en Criptografía y Seguridad Teleinformática (IESE), Magister en Tecnología Informática (UAI) y Doctorando en Ingeniería (UNLZ). Investigador en el área de Ciberseguridad, criptografía e Inteligencia Artificial (UAI). Es Especialista en ciberseguridad: Criptógrafo (Proyecto: INCIBE) y fue Científico de datos (NLP - Proyecto BBVA). Profesor de Defensa de Sistemas Distribuidos de la Maestría en Ciberdefensa (UNDEF). Profesor de Criptografía de la Especialización en Informática Forense (UFASTA).

Esp. Abg. Sabrina LAMPERTI

Abogada, Especialista en Criminalidad Económica. Prosecretaria del Dpto de Ciberdelitos y Tecnologías aplicadas de la Secretaría de Política Criminal de la Procuración de la Provincia de Buenos Aires e integra el equipo de Referentes en Investigaciones Digitales del Ministerio Público de la Provincia de Buenos Aires. Docente de la Universidad FASTA, Universidad de Buenos Aires, UNNOBA, entre otras. Investigadora del InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. Coautora de varios libros entre los que se destaca “El rastro digital del delito” – Universidad FASTA 2017.

Dra. Abg. Bibiana LUZ CLARA

Es Abogada de la Universidad Nacional de Mar del Plata y Magister en Derecho de Internet y las Nuevas Tecnologías de la Información y las Comunicaciones con certificación internacional del Instituto Europeo Campus Stellae de Santiago de Compostela, España. Además, es Árbitro de Comercio Internacional por la Florida Supreme Court. Ha realizado el posgrado de Negociación de la Universidad de Belgrano, y los posgrados de Mediación de la Universidad Nacional de Mar del Plata y de la Fundación Libra. Ha realizado la formación de posgrado en Arbitraje Internacional y Training de la Florida Supreme Court. En la Universidad FASTA es Profesor titular con dedicación parcial

afectada a docencia e investigación. Se desempeña como Profesor en las cátedras de Informática y Derecho de la Facultad de Ingeniería de la Universidad FASTA y en la cátedra de Derecho Informático de la Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA. Es Directora Ejecutiva de la carrera de Especialización en Gestión Legal de la Tecnología de la Información de la Universidad FASTA. En lo que hace a investigación, se desempeña como Directora del Grupo de Investigación en Informática y Derecho de la Universidad FASTA. Dirige el Proyecto "Diseño de un Centro de Resolución Electrónica de Conflictos", realizado en conjunto con la Universidad UNIANDES de Ecuador, y participa como investigadora del Proyecto "Análisis de Consistencia de la Legislación de Defensa del Consumidor por Métodos Formales", realizado en conjunto con el Grupo de Investigación FORMALEX de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. Es docente en el posgrado de Actualización en Derecho Informático de la Universidad de Buenos Aires y en las cátedras de grado de Aspectos Profesionales para la Ingeniería, y Derecho en la Carrera de Publicidad de la en la UCAECE. Como investigadora ha dirigido varios proyectos en la temática de Informática y Derecho, por más de 10 años, entre ellos, el Proyecto "Ontojuris", con el I3G de Brasil y la Universidad Politécnica de Madrid. Su dedicación al campo del derecho informático la ha llevado a escribir los libros "Manual de Derecho Informático" (2001) y "Ley de Firma Digital Comentada" (2006), ambos de Editorial Nova Tesis. Además, es co-autora del "Tratado de Doctrina y Jurisprudencia sobre Derecho Informático de LA LEY", publicado por Ed. La Ley (2011), y del libro "Defensa del consumidor en la contratación de bienes y servicios informáticos", editado por la Universidad FASTA (2013). Dirige el Instituto de Derecho Informático del Colegio de Abogados de Mar del Plata desde el año 2000. Ha presentado y publicado trabajos en numerosos congresos nacionales e Internacionales y ha presidido las Primeras Jornadas Latinoamericanas de Derecho Informático (2001), el Simposio de Derecho e Informática (2007 y 2009) y el Congreso Iberoamericano de Investigadores y Docentes en Derecho e Informática (2012). Fue árbitro del Tribunal Arbitral del Colegio de Abogados de Mar del Plata durante el periodo 2003- 2012 y es mediadora prejudicial.

Mg. Abg. Oscar MATO

Abogado (UBA) y Master of Business Administration en Dirección de Sistemas de Información (USAL). Es Analista de Seguridad y Vulnerabilidad en Redes, Seguridad en redes informáticas y seguridad de la información (IESE). Realizó cursos de posgrado en Actualización en Control y Auditoría de la Tecnología de la Información, Auditoría de Tecnología de la Información y en Derecho Aeronáutico y Espacial. Integró el Comando Conjunto de Ciberdefensa - EMCFFAA. Profesor de Ciberdefensa, Criptografía y Seguridad en Redes en la FI-UFASTA: Es Asesor en Derecho en el Ciberespacio y en Ciberseguridad.

Dr. Ing. Gustavo MESCHINO

Ingeniero Electrónico (1997). Doctor en Ingeniería, Orientación Electrónica (2008). Títulos otorgados por la Universidad Nacional de Mar del Plata (UNMDP). Profesor Asociado en la UNMDP. Investigador Categoría II de la Secretaría de Políticas Universitarias, otorgada desde 2018. Director del Laboratorio de Bioingeniería, perteneciente al Dpto. de Ingeniería Electrónica y Computación y al Instituto de investigaciones Científicas y Tecnológicas en Electrónica (ICYTE, UNMDP/ CONICET). Director del Doctorado en Ingeniería, Orientación Electrónica. Integrante de la Comisión Directiva de la Sociedad Argentina de Bioingeniería SABI (Tesorero, 2017-2025). Integrante de la Comisión Directiva del ICYTE (consejero investigador, 2021-2025). Profesor Titular de la Universidad FASTA. Codirector del grupo Informática y Salud. Docente de grado y posgrado en temas de Ingeniería

Electrónica e Inteligencia Artificial. Ha dirigido y dirige tesis de grado, doctorado y posdoctorado en esas áreas. Dirige proyectos de investigación. Sus áreas de investigación abarcan técnicas de Inteligencia Artificial aplicadas al procesamiento de imágenes y señales biomédicas, en conjunto con la coordinación de proyectos de diseño de dispositivos biomédicos de adquisición y procesamiento de señales.

Mg. Ing. Guillermina NIEVAS

Doctoranda en Informática (UAI), Magister en Ingeniería de Software y Sistemas de Información (UTECH, España), Magíster en Administración de Negocios (UCASAL), Ing. en Sistemas de Información (UTN). Docente de grado y posgrado en la Universidad Católica de Salta, docente de posgrado en UFASTA. Actualmente se desempeña como Secretaria Académica de la Facultad de Ingeniería de la UCASAL y es Directora Especialización en Gestión de TICs (UCASAL).

Dr. Ing. Adolfo ONAINE

Ingeniero Electricista (UNMdP), Master of Business Administration (USAL) y Doctor en Ingeniería mención Ingeniería Industrial (UNLZ). Es Profesor Titular en la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata.

Dra. Ing. Lía OROSCO

Doctora en Ingeniería por la Universidad Politécnica de Cataluña, Magister en Ingeniería Estructural y Consultora Ambiental por la Universidad Politécnica de Cataluña. Magister en Ingeniería Estructural (UNT). Investigadora en Riesgo Sísmico de UCASAL, profesora titular de "Dinámica Estructural" y "Construcciones de Hormigón Armado" en UCASAL y profesora adjunta de "estructuras laminares"y "Geoctenia II" en la Universidad Nacional de Salta. Coordinadora del Departamento de I+D de la Facultad de Ingeniería de UCASAL. Docente de la cátedra de Taller de Tesis I de la Maestria en Gestión de Proyectos, Obras y Desarrollos Inmobiliarios de la UCASAL.

Mg. Ing. Hugo PÁGOLA

Ingeniero Electrónico (UBA), Especialista en Seguridad Informática (UBA), Master en Seguridad Informática (UBA). Profesor de Criptografía y Seguridad Informática (UBA). Integrante de la Comisión de Posgrado de la Maestría en Seguridad Informática (UBA). Director de Tecnopro SA.

Mg. Ing. Marcela PALLERO

Ing. Sistemas de Información (UTN), Especialista, Criptografía y Seguridad Teleinformática (UNDEF). Profesora en Disciplinas Industriales (UTN). Docente de ciberseguridad del Programa IA y Sociedad (UNTREF). Docente de la materia Auditoría y Seguridad de Sistemas (UP). Responsable del Programa Seguridad en TIC en la Fundación Sadosky.

Dra. Ing. Beatriz PARRA DE GALLO

Dra. Ingeniería Mención Sistemas de Información, Master en Administración de Negocios, Especialista en Informática Forense, Ingeniería en Computación. Con una extensa carrera académica como docente e investigadora en la UCASAL reviste la categoría de investigador independiente “B” (CI-UCASAL), y es Directora del Grupo de I+D+i de Forensia Digital y Ciberseguridad de esa institución, grupo abocado al desarrollo de proyectos de i+d interinstitucionales con universidades nacionales y latinoamericanas. Es además, Directora del Instituto de Estudios Interdisciplinarios de Ingeniería de la Facultad de Ingeniería de la UCASAL y Directora de la carrera de Especialización en Administración de Bases de Datos. Participa en la formación de recursos humanos impartiendo cursos

de posgrado y como docente de carreras de grado y posgrado en UFASTA (Argentina), UTN-FRSF (Argentina), UTN-FRC (Argentina), UNIVA (México), UNISANGIL (Colombia), Universidad Católica de Colombia (Colombia), UniTECH (España). Es miembro de la Comisión de Informática Forense del Instituto Argentino de Normalización y Certificación (IRAM), y representante de la UCASAL en la Red Iberoamericana de Blockchain y Ciberseguridad (RIBCi), Red Iberoamericana de Docentes e investigadores de Informática y Derecho (CIIDDI), Red Argentina de Posgrados en Ingeniería (RADoI), Red Red Universitaria de Informática Forense (Red UNIF). Perito Informático de Parte, es consultora en Proyectos Tecnológicos Críticos y sus temáticas de interés son: Forensia Digital, Educación en Ingeniería y Ética en la Ingeniería.

Mg. CPN Patricia PRANDINI

Contadora Pública, Especialista en Seguridad Informática y Magister en Seguridad Informática (UBA) y Master of Accounting Science con especialización en Sistemas de Información (Universidad de Illinois, EEUU). Tiene certificaciones internacionales en Auditoría de Sistemas (CISA) y en Riesgo y Control (CRISC), otorgadas por ISACA. Se ha desempeñado en el Ministerio de Modernización de la Nación y en la Dirección Nacional de Ciberseguridad. Ha participado entre otros proyectos, en la implementación de la Infraestructura de Firma Digital de la República Argentina, en la creación de la Coordinación de Emergencias en Redes Teleinformáticas (ArCERT) y en el desarrollo del primer portal de Estado argentino. Es docente de Auditoría y Seguridad Informática en la UBA y en la Universidad Nacional de San Martín. Fue presidente del Capítulo Buenos Aires de ISACA. Es coautora del libro "Normas Internacionales y Nacionales vinculadas a la Seguridad de la Información" y ha publicado varios artículos sobre temas de seguridad informática en revistas técnicas.

Mg. Abg. Hernán QUADRI

Abogado (UM), Dr. en Ciencias Jurídicas (UMSA), fue Secretario de Redacción de la revista La Ley Buenos Aires. Director Honorario del Instituto de Derecho Procesal Civil del Colegio de Abogados de Morón (BsAs). Coordinador Revista Temas de Derecho Procesal (Erreius). Coordinador Revista Temas de Derecho Procesal (Erreius) del Poder Judicial de la Provincia de Buenos Aires.

Mg. Ing. Diego ROMERO

Ingeniero en Electrónica (UBA) y Especialista en Ingeniería Sanitaria (UBA). Docente de ciberseguridad industrial en cursos de posgrado de la Escuela de Graduados en Ingeniería Electrónica y Telecomunicaciones de la Facultad de Ingeniería (UBA). Cuenta con una certificación ISA/IEC 62443 Cybersecurity Certificate Program. Consultor independiente e instructor en automatización, informática y ciberseguridad industrial. Instructor Técnico de Schneider Electric.

Mg. Ing. Gonzalo RUIZ DE ANGELI

Ingeniero en Informática (UFASTA), Mg. en Dirección Estratégica en TI (Universidad Europea del Atlántico). Líder de Pronóstico, Planificación y Programación en Movistar. Investigador en UFASTA. Field Services Forecasting, Planning and Scheduling Leader. Researcher. Es el responsable de Planificación Estratégica en el InFo-Lab (UFASTA).

Mg. Lic. Gustavo SAIN

Licenciado en Ciencias de la Comunicación Social, Políticas y Planificación de la Comunicación (UBA). Master en Sociología y Ciencias Políticas, Ciencias sociales · (FLACSO). Docente en UFASTA, USIGLO21, UNQ, UNLZ, IUPFA y UB. Director Nacional de Ciberseguridad. Asesor en ciberseguridad y cibercriminalidad de la Dirección Nacional de Política Criminal. Investigador del

Observatorio de Seguridad del Instituto de Investigaciones Gino Germani. Director de la Diplomatura en Cibercrimen.

Esp. Abg. Daniel SHURTJIN

Abogado (UBA). + Especialista en Administración de Justicia (UBA). Especializado en Ministerio Público (UBA) y en Derecho Informático (CEDI-UBA). + Graduado del Programa Argentino de Capacitación para la Reforma Procesal Penal (CEJA-INECIP). Formación en Análisis Económico del Derecho (Escuela Complutense Latinoamericana) y en Género, Sexualidad y Diversidad (Escuela Complutense Latinoamericana y CSJN). + Docente del Departamento de Derecho Penal de la Facultad de Derecho, UBA. Docente de posgrado en el Programa de Actualización en Ciberseguridad y Delitos Informáticos (UBA) y en el Diplomado en Cibercrimen de la Universidad Nacional de Quilmes. + Subsecretario letrado de la Procuración General de la Nación. + Ex cotitular de la Dirección General de Capacitación y Escuela del Ministerio Público Fiscal de la Nación. + Asesor de la Comisión para la Reforma del Código Penal (creada por Decreto PEN 103/2017). + Primer premio en el Concurso de Investigaciones de Derecho Penal Económico organizado por ITEPSUR (2018). Premio "mención académica" del Rectorado de la UBA (2019). + Conferencista y formador en Red de Capacitación del Ministerio Público Iberoamericano, H. Senado de la Nación, Ministerio Público Fiscal de la Nación, AFIP, entre otros.

Mg. Ing. Miguel SOLINAS

Ingeniero Electricista Electrónico (UNC), Magister en Ingeniería de Software, (UNLP), Ingeniero Especialista en Calidad (UTN) e Instructor CCNA Security, Seguridad en Redes (UTN). Es Sub Director Departamento de Computación, FCEFyN (UNC) y Sub Director del Laboratorio de Redes y Ciberseguridad, FCEFyN (UNC).). Es Profesor Adjunto con Dedicación Exclusiva de la FCEFyN (UNC).

Ing. Santiago TRIGO

Ingeniero en Informática. Perito en Departamento Judicial Mar del Plata. Ministerio Público Provincia de Buenos Aires (MPBA). Docente Investigador FI-UFASTA y Jefe de carrera de Licenciatura en CIberseguridad.

17. **INFRAESTRUCTURA Y EQUIPAMIENTO**

17.1. **Espacios físicos**

En términos de espacios físicos, la Universidad FASTA desarrolla sus actividades con recursos edilicios propios, tanto los espacios de oficinas, aulas y recursos didácticos. La Facultad de Ingeniería cuenta con la infraestructura física y edilicia adecuada y suficiente para el desarrollo de las carreras presenciales, así como, para la gestión académica y administrativa de todas las carreras, sean éstas presenciales o a distancia.

17.2. **Unidades de Apoyo Académico**

El SIED –UFASTA cuenta con Unidades de Apoyo Académico (UAA) donde, fuera del ámbito físico de la sede universitaria se llevan adelante las actividades académicas que se requieren para el desarrollo de las carreras (por ejemplo, toma de exámenes finales, defensa de trabajos finales de graduación o tesis de licenciatura), además de ser soporte para distintas actividades de investigación y extensión.

La decisión de constituir UAA en diversas ciudades del país se funda en:

- La decisión académica de realizar exámenes finales en forma presencial, con el objeto de asegurar las condiciones de identidad y seguridad en estas instancias evaluativas de alto impacto, pues tienen su correlato en la registración de la aprobación de la asignatura en el Plan Analítico de Estudios del estudiante.
- La importancia que también se le otorga a la expresión escrita del estudiante y a la competencia buscada del desarrollo de ideas o conceptos, resolución de problemas, análisis de casos, en los que el estudiante demuestra la comprensión e incorporación de aprendizajes y habilidades.
- Sin perjuicio de la intencionalidad de que el estudiante sea capaz de autogestionar sus procesos administrativos y académicos, la UAA brinda también la posibilidad de ofrecer en la ciudad de residencia del estudiante, un ámbito de promoción de la Universidad, su oferta académica y sus actividades y de información y atención administrativa al estudiante, para canalizar adecuadamente sus trámites y sus consultas en las áreas correspondientes de la sede central de la Universidad.

Un colegio, institución de educación superior, organización profesional u otra organización local, gubernamental o no gubernamental, podrá conformarse como Unidad de Apoyo Académica (UAA) de la Universidad FASTA, para el dictado de carreras y/o cursos en la modalidad a distancia, en el marco del Convenio que se firma a tal efecto y de las funciones que se establecen para la misma, siempre que cumplan con los requerimientos de infraestructura edilicia y tecnológica requeridos.

17.3. **Infraestructura Tecnológica disponible para la carrera**

El equipamiento informático de uso académico depende del área de Soporte Técnico de la Universidad FASTA, integrado por un coordinador y un equipo de 5 técnicos que garantizan el correcto y continuo funcionamiento de la infraestructura tecnológica para docencia.

Dentro de la infraestructura tecnológica disponible para la Facultad de Ingeniería, interesa describir aquellos requeridos para las carreras de modalidad a distancia.

Para la carrera de Maestría en Ciberseguridad e Informática Forense la Facultad cuenta con herramientas licenciadas para la comunicación sincrónica (ZOOM ®), así como de herramientas para la gestión de las aulas virtuales requeridas (Moodle).

En cuanto al equipamiento informático y sistemas de soporte a la administración y gestión de la Universidad FASTA, su instalación y mantenimiento depende de la Dirección de IT y dispone de un equipo de 28 personas (la mayoría profesionales) organizados en distintas divisiones que garantizan el correcto y continuo desempeño de la infraestructura tecnológica y el diseño, implantación y mantenimiento de los servicios de IT necesarios para todos los actores involucrados en las tareas de docencia, investigación, extensión y gestión que lleva adelante la Universidad FASTA.

La infraestructura de IT de la Universidad FASTA se soporta en un datacenter propio con tecnología de última generación que dispone la institución en sus instalaciones, desde donde se disponen las conexiones a la red de área local y a Internet. Así, se puede dar acceso a los servicios y sistemas a cualquier usuario sin importar su ubicación geográfica, y se mantienen los accesos de los edificios remotos, sedes y centros asociados de todo el país.

En cuanto al soporte para la gestión y administración de las distintas unidades académicas y de servicio, la infraestructura informática dispuesta es suficiente y adecuada. En este sentido, la disponibilidad de PCs para todos y cada uno de los integrantes del personal administrativo, técnico y

de gestión facilita y garantiza el trabajo cotidiano.

17.4. **Infraestructura para la Gestión y Registro de la Información y Servicios**

La infraestructura de los sistemas informáticos que dispone hoy en día la Universidad FASTA ofrece simultáneamente a las áreas de gestión, unidades académicas (sin importar las ubicaciones físicas de todas ellas), el acceso, la disponibilidad y uso para toda la comunidad universitaria. Es decir, los estudiantes, los docentes, el personal de gestión, los directivos, etc., tienen la posibilidad de acceder a los servicios informáticos que la Universidad FASTA les ofrece para el desarrollo de sus actividades.

El amplio conjunto de sistemas informáticos, con la gran cantidad de funcionalidades y servicios que ofrecen por medio de los diferentes módulos que poseen, permiten realizar un gran número de operaciones en forma digital e informatizada.

Un breve resumen de las funcionalidades del Sistema Integrado de la Universidad FASTA (SIUF) se muestra a continuación:

- Permite gestionar, registrar y mantener, de manera unificada, controlada y segura, toda la información relativa a la trayectoria académica de los estudiantes de todas las carreras. El sistema académico permite incorporar toda la información de una persona que cursa una carrera en la Universidad FASTA, desde el momento de su ingreso, hasta su finalización como graduado: datos personales, materias que cursa, comisiones, materias regularizadas, materias rendidas, etc.
- Dispone de un sistema de gestión administrativa de toda la parte arancelaria y contable, que permite seguir el desarrollo arancelario de cada estudiante.
- El sistema académico dispone, además, de un módulo de consultas y estadísticas para llevar los indicadores más relevantes en tiempo real, e históricos. Desde esta herramienta, también se obtienen los resultados a informar al Ministerio de Educación por medio del sistema SIU, en el cual la Universidad FASTA, siempre ha volcado toda la información requerida.
- El sistema de personal permite registrar y mantener toda la información referida a los legajos del personal administrativo y docente. Desde este sistema se organiza la composición de cátedras, se administran las designaciones, se registran las novedades, licencias y suplencias, etc.
- También, se dispone de un conjunto de subsistemas relacionados a actividades de gestión y administrativas internas, como pueden ser los subsistemas de seguridad y permisos, el subsistema de gestión de expedientes, subsistema estadístico para la toma de decisiones, servicio de correo electrónico propio, entre otros.
- MediatecaWeb: Es un subsistema para la gestión de la Biblioteca, pero que a la vez permite a los usuarios (estudiantes, docentes, etc.) consultar el material disponible, hacer reservas, etc. Este servicio se encuentra disponible también vía Internet.

Departamento de Ingreso: Es un subsistema para la gestión del área de ingreso, con información y servicios para los potenciales estudiantes, con material e información sobre toda la oferta académica de la Universidad FASTA.

El sitio web de la Universidad FASTA disponible en www.ufasta.edu.ar es un portal sumamente completo donde se puede encontrar mucha información institucional, datos de las áreas de gestión, secciones por cada unidad académica con toda la información referida a las carreras, planes de estudio, correlatividades, contenidos mínimos, áreas de noticias, carteleras virtuales, etc. Es muy importante aclarar que mucha de la información mostrada en este sitio se obtiene directamente de los otros sistemas nombrados anteriormente, lo que permite mantener esta información unificada, actualizada y

disponible mediante acceso público o privado, según corresponda.

El SIUFWeb es la plataforma de Internet al que pueden acceder estudiantes y docentes (sitio de acceso privado), por medio del cual pueden realizar diferentes trámites y consultas respecto de toda la información que les concierne. Este sistema, además se encuentra conectado con la plataforma de educación a distancia con el fin de disponer de la herramienta de aula virtual utilizada en este tipo de enseñanza.

La Universidad FASTA para el dictado de las carreras con modalidad a distancia cuenta con una Plataforma Moodle, personalizada y vinculada con SIUFWeb. Moodle es una aplicación web de tipo Ambiente Educativo Virtual de distribución libre, una plataforma de aprendizaje diseñada para proporcionarle a docentes, administradores y alumnos un sistema integrado único, robusto y seguro que ayuda a crear comunidades de aprendizaje en línea. Moodle está instalada en servidores contratados que garantizan la disponibilidad, estabilidad y calidad del servicio, y la escalabilidad cualquiera sea la demanda.

También, dentro de la plataforma Moodle las materias disponen de salas de chat, foros, mensajería, y la posibilidad de subir TPs y evaluarlos, subir archivos de clases, bibliografía, reglamento de cátedra, etc. Además, se dispone de una herramienta de aula virtual en la que un docente vía Internet (con Webcam y micrófono) puede dar clase a grupos de hasta 50 estudiantes, con la posibilidad de que los estudiantes puedan interactuar con sus compañeros y docentes.

Toda área de gestión de la Universidad FASTA (cada grupo de investigación, cátedra docente, o docente particular) dispone de un servicio de blog que permite mantener y publicar de contenido público en Internet sobre las actividades que cada uno de ellos realizan: artículos sobre trabajos, temarios y trabajos prácticos, etc.

En síntesis, la suficiencia, rapidez y seguridad de los sistemas de registro está garantizada. Prueba de ello es que llevan 15 años en régimen sin incidentes ni inconvenientes. Los registros constituyen fuentes únicas de información. Las redes permiten el acceso a toda la información y carga, a todos los tipos de usuarios de la comunidad universitaria, desde cualquier lugar físico donde se encuentren. Las constancias de la actuación académica y las actas de examen de los estudiantes se resguardan en la Secretaría General, bajo estrictas normas de seguridad. El SIUF permite el registro de los antecedentes académicos y profesionales del personal docente, su mantenimiento actualizado y su consulta en forma inmediata, aún a distancia.

17.5. **Sistema Institucional de Educación a Distancia de la Universidad FASTA**

17.5.1. **Modelo Educativo**

La Universidad FASTA, mediante Resolución del Rectorado Nro. 402/17, formaliza el Sistema Institucional de Educación a Distancia de la Universidad FASTA (SIED-UFASTA), evaluado luego por CONEAU y con validez oficial otorgada por el Ministerio de Educación (RM 206/2019), que establece un marco pedagógico, tecnológico y comunicacional de referencia para el desarrollo de ambientes de enseñanza y aprendizaje "en línea", dirigido especialmente a optimizar las prácticas docentes en ambientes virtuales, a fin de que los estudiantes alcancen las competencias formativas y profesionales buscadas, teniendo en cuenta los principios de la identidad institucional y las perspectivas de innovación metodológica, tecnológica y comunicacional

El modelo de educación en línea de la UFASTA ha sido concebido bajo la premisa de la comunicación

sincrónica y asincrónica, no como excluyentes una de la otra; por el contrario, son concebidos como procesos que se complementan y que potencian la acción comunicativa dentro del entorno virtual. Los docentes son debidamente capacitados y asistidos mediante el equipo de Asistencia Docente y están en condiciones de determinar los tipos de comunicación y las herramientas que utilizarán en acuerdo a sus prácticas educativas y a los objetivos planteados desde sus cátedras, con la colaboración del Departamento de Educación a Distancia para un mejor abordaje de las competencias buscadas en la formación del estudiante.

17.5.2. **Tecnologías previstas**

La Universidad FASTA posee una plataforma de iniciativa propia que interconectada a Moodle permite a la institución personalizar los sistemas de acuerdo a sus necesidades, logrando de ese modo una herramienta que se adapta a los requerimientos propios de las unidades académicas y que además permite trabajar de manera interdisciplinaria con sus propios equipos. La plataforma facilita la interacción en el ambiente virtual, proporcionando una serie de herramientas educativas para facilitar el aprendizaje, la comunicación y la colaboración (correo electrónico, foros de discusión, chat, aula virtual, videoconferencia, etc.), y una serie de herramientas administrativas y de gestión. La carrera dispondrá de un campus específico en versión de Moodle actualizada (superior a 4.2).

La Universidad FASTA, por medio de su SIUFWeb -que opera como un Campus Virtual-, propone una alternativa que atiende a las diferentes realidades de cada estudiante, buscando fomentar la igualdad de oportunidades de acceder a la capacitación independientemente de la ubicación geográfica y la distancia a centros de formación. Para el desarrollo del SIUFWeb se han tomado una serie de requisitos esenciales que posibilitan que dicha herramienta se comporte como un excelente nexo entre el estudiante y la Universidad. El modelo comunicacional es el denominado Aprendizaje en Ámbitos Colaborativos (AAC), donde existe una interacción permanente entre todos los actores del proceso educativo.

La plataforma además tiene incorporadas herramientas tecnológicas que promueven la integridad académica integrados a Moodle: sistema antiplagio y *proctoring*.

El **aula virtual para videoconferencias** se utiliza para encuentros sincrónicos del docente con un grupo de estudiantes (clase, clase de consulta, etc.); y también–para la presentación y defensa del Trabajo Final Integrador específico del título de Magister en Ciberseguridad e Informática Forense. También se puede utilizar para exámenes finales que deben ser realizados en forma oral y sincrónica. De ser necesario, el encuentro sincrónico puede grabarse y luego subirse a la plataforma a fin de que aquellos estudiantes que no hayan podido participar del encuentro puedan verlo de manera asincrónica.

La Universidad FASTA incorpora al sistema de Educación a Distancia una **plataforma de comunicación web** segura con el que se pueden realizar reuniones, seminarios, defensas de trabajos, tutorías, clases virtuales, evaluaciones, independiente de la ubicación de los participantes. Este sistema es una herramienta que facilita la comunicación entre profesor y estudiante permitiendo una interacción en tiempo real, ya que cuenta con elementos como el chat, videoconferencias, transferencia de archivos y la pizarra, que permiten el dictado o recepción de la clase. La impartición de una clase a través del aula se realiza de forma online y en tiempo real entre el docente y los participantes, la cual puede ser grabada para una futura descarga o reproducción. Cabe destacar que para administrar o utilizar la plataforma sólo se requiere de un navegador Web actualizado y una conexión a Internet aceptable (25 Mb como mínimo). Además del navegador es necesario de los componentes básicos de una videoconferencia, cámara Web, micrófono y salida de audio.

Por último, para el desarrollo de actividades prácticas específicas de Ciberseguridad e Informática Forense, la Facultad de Ingeniería pone a disposición de los estudiantes y docentes, servidores y servicios de uso exclusivo que permiten la instalación de máquinas virtuales, herramientas de propósito específico, resguardo de imágenes de almacenamiento para la simulación de casos, etc.

Es importante destacar que se ha diseñado un **plan permanente de formación docente** para la actualización continua de los profesores del sistema a distancia, con contenidos actualizados sobre el uso de los recursos tecnológicos y didácticos disponibles para esa modalidad. Este plan forma parte de la PROGRAMA GENERAL DE CAPACITACIÓN DOCENTE, aprobado por Resolución Rectoral N° 059/24, que tiene por objetivo la generación de recursos que favorezcan de modo permanente y articulado el fortalecimiento de propuestas de formación y capacitación, tanto de los docentes estables como también para favorecer la inducción de nuevos docentes.

17.5.3. **Plataforma para Ejercitación en Actividades Propias de la Ciberseguridad y la Informática Forense**

La Facultad de Ingeniería dispone de una plataforma de servidores donde se instalan máquinas virtuales para cada estudiante que permiten el desarrollo y seguimiento de las actividades prácticas, de investigación y de resolución de casos de pericias informáticas, en entornos simulados que representan escenarios reales o hipotéticos.

Estos servidores, además, cuentan con un repositorio digital de material bibliográfico y de herramientas de software libre de utilidad para el desarrollo de las actividades prácticas, de investigación y de resolución de casos de pericias informáticas. Los estudiantes acceden a estos servidores con su usuario y contraseña y tienen a su alcance la bibliografía y herramientas necesarias, los casos que deben resolver y los escenarios simulados de práctica, donde trabajan en la resolución y dejan los resultados alcanzados para la supervisión por parte de los docentes.

Esto permite y garantiza que los estudiantes, más allá del lugar geográfico donde se encuentren, puedan realizar sus prácticas en escenarios homogéneos y complejos, solamente con una computadora y acceso a Internet.

La administración de estos servidores y la gestión de los repositorios digitales está a cargo de los docentes de la carrera que los configuran conforme los fines previstos de todas y cada una de las actividades prácticas que los estudiantes deban realizar.

17.6. **Biblioteca**

La Biblioteca se encuentra en la planta baja del edificio de San Vicente de Paul y a ella puede acceder cualquier estudiante, docente o graduado de la Universidad FASTA para retirar libros y consultar información durante todo el año. Los horarios de atención son de 7:40 a 20 hs. de lunes a viernes y de 9 a 13 hs. los sábados.

La Biblioteca de la Universidad FASTA cuenta con sistema de catalogación AACR2 y clasificación CDD21 en español.

La cantidad del personal de biblioteca cubre adecuadamente la demanda y su nivel de capacitación es por demás adecuado. Dispone de 2 personas en carácter permanente una bibliotecaria documentalista y una estudiante de biblioteca escolar. El equipamiento informático disponible en biblioteca es suficiente para la demanda y permite el acceso a la intranet y a Internet vía LAN y WI-FI. Además, los docentes pueden acceder también desde las salas de profesores.

La Universidad FASTA cuenta con un repositorio digital denominado REDI que fue generado como un espacio para facilitar y mejorar la visibilidad de la producción científica y académica de la institución, permitiendo el acceso abierto a sus contenidos y garantizando su preservación en el tiempo.

La búsqueda de material existente en la biblioteca está disponible desde la web, es decir que los estudiantes y docentes pueden verificar la existencia de algún material o de los materiales de determinado tópico por internet y hacer las consultas correspondientes.

Respecto del acceso a redes de información y sitios o bibliotecas científicas, la biblioteca dispone de una cantidad importante de estos recursos con acceso pleno para estudiantes, docentes e investigadores. Entre las más relevantes está el acceso libre a la biblioteca electrónica de la Secyt, y por su intermedio a todas las bibliotecas virtuales que con ella tienen convenio. Distintos tipos de documentos en texto completo pueden ser consultados desde 1988 hasta el presente: revistas científicas y de divulgación, actas de conferencias, estándares internacionales, entre otros.

En síntesis, la calidad de la prestación de los servicios de la biblioteca es adecuada y suficiente para la demanda de la carrera. Los sistemas de consulta vía web o correo electrónico y la suscripción a bases de datos on line y conexiones a otras bibliotecas son servicios de alta calidad que la biblioteca pone a disposición de los estudiantes y docentes, en particular, de las carreras a distancia.

17.7. **Bibliografía específica**

La Universidad FASTA dispone de la bibliografía específica para el apoyo al dictado de la carrera. A su vez, y a efectos del dictado de la carrera, está prevista la incorporación de los títulos que los profesores invitados soliciten.

Como bibliográfica básica se indica el siguiente listado no excluyente, que deberá actualizarse debidamente al momento de implementar la carrera:

- Andress J., (2019), Foundations of Information Security
- Ararat, P. A. P., Ortiz, Z. X. R., Hernández, F. A. C., &
- Pantoja, A. H. (2023). Perfil profesional en ciberseguridad y ciberdefensa: un ejercicio exploratorio de conceptualización. Revista da UNIFA, 36, 1-15.
- Candel, J. M. O. (2024). Ciberseguridad: manual práctico. Ecoe Ediciones.
- Deutsch V., (2022), CIBERSEGURIDAD PARA DIRECTIVOS. RIESGOS, CONTROL Y EFICIENCIA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
- Dudley R. y Golden D. (2022) THE RANSOMWARE HUNTING TEAM, Editorial: Farrar, Straus and Giroux
- García, F. X. M., & Martínez, J. L. Z. (2023). Revisión de la literatura de las metodologías de ciberseguridad en plataformas bancarias. Polo del Conocimiento: Revista científico-profesional, 8(3), 2618-2634.
- García, J. A. C. Economía de defensa, ciberseguridad y ciberdefensa. ECONOMÍA DE DEFENSA, 145.
- Global Cybersecurity Outlook 2024, https://www.weforum.org/publications/global-cybersecurity-outlook-2024/?gad_source=1
- Grubb S., (2021) How Cybersecurity Really Works
- Hubbard D. y Seiersen R. (2022), HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK, Editorial: John Wiley & Sons Inc
- Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos, ciberseguridad e insurtech.

Dykinson.
- Kinosita, J. G. (2022). Amenazas y desafíos a la política de seguridad del siglo XXI. Pensamiento Conjunto, 10(2), 15-15.
- Montes, J. F. O. (2020). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Revista de Ciencia e Investigación en Defensa, 1(4), 36-48.
- Moya, J. G. (2023). Revolución de la ciberseguridad en la cuarta revolución industrial. Revista Ingeniería e Innovación del Futuro, 2(2), 6-20.
- Pardo Gato, J. R. (2019). La ciberseguridad como deber deontológico del abogado: el secreto profesional y la protección de datos. Wolters Kluwer España.
- Wolff J., (2022) CYBERINSURANCE POLICY, The MIT Press

18. **INFORMES**

Para informes se ha dispuesto una cuenta de correo electrónico de consulta que permite el acceso a la dirección de la carrera.

Mail: **posgrado.ciberseguridad.ead@ufasta.edu.ar**
Contactos: Dra. Ing. Beatriz H. Parra de Gallo, Mg. Ing. Gonzalo Ruiz De Ángeli