Trabajo Final Integrador

# Titulo: Diseño del Laboratorio de Informática Forense del COPROCIER

Autor: Silvia Mónica Aranguren

POSGRADO ESPECIALIZACIÓN EN INFORMÁTICA FORENSE

Directores:

Mg. Ing. Gonzalo Matías Ruiz De Angeli

Dr. Pablo Adrián Cistoldi

Fecha de publicación: 18/08/2022

UNIVERSIDAD FASTA

FACULTAD DE INGENIERÍA

## Resumen:

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.

## Palabras Clave:

Informática Forense; Laboratorio Pericial Informático; Pericias Informáticas; Perito Judicial; Protocolos.

## Agradecimientos

Un agradecimiento muy especial al grupo de peritos del COPROCIER, quienes han colaborado de manera inestimable, disponiendo de su valioso tiempo, para la concreción de este trabajo.

# INDICE

## Contenido

## Anexos

**I - Planos COPROCIER**

**II- Fotos COPROCIER**

**III- Instrumentos utilizados para consultar a los peritos**

**IV - Formulario online**

**V- Presupuesto Hardware**

**VI- Glosario**

# INDICE de Imágenes

## Introducción

En la provincia de Entre Ríos, los peritos informáticos matriculados realizan pericias de oficio, de parte y pruebas anticipadas en todos los fueros (laboral, civil y comercial, familia, etc.) menos en el ámbito penal que se realiza dentro de los laboratorios forenses del MPF[2].

Nuestro interés es contar con un Laboratorio Forense y procedimientos de calidad para que los peritos que conforman el grupo o equipo de peritos del COPROCIER [3] Colegio de Profesionales de Ciencias Informáticas de Entre Ríos, actúen de manera metódica y utilizando 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.

Hoy en día los peritos cuentan con muchos desafíos; como ser las diferentes y dinámicas modalidades de los delitos informáticos, el explosivo aumento de la cantidad de información y de variedad de fuentes de evidencia digital (ej.: almacenamiento en la nube; teléfonos inteligentes, cámaras, smartwatches, drones, computadoras de vehículos, IoT -Internet de las Cosas, entre otros), la incesante evolución tecnológica, el conflicto entre privacidad y seguridad, etc. Para representar un aporte eficaz, la labor informático forense no debe dejarse librada a la improvisación ni a la rutina. Al contrario, se requiere disponer de una infraestructura flexible y suficiente, procesos de trabajo adecuados, formación y actualización profesional, todo ello en el marco de un escenario sumamente cambiante y frecuentemente imprevisible (Di Iorio, Cistoldi et al., 2019).

**COPROCIER** es la institución que representa a los profesionales de la informática de la provincia de Entre Ríos, a través de su matriculación. La entidad nuclea a los profesionales que poseen título de grado en carreras de Ciencias Informáticas que se dictan en las universidades de nuestro país. El Colegio fue creado por Ley Provincial Nº 9498[4], sancionada en el año 2003, que regula las condiciones para el ejercicio de la profesión en Entre Ríos, y asume como

[2] https://mpf.jusentrerios.gov.ar/
[3] https://coprocier.org.ar/web/
[4] https://coprocier.org.ar/web/?page_id=33

función principal la de representar y proteger los derechos de los matriculados en sus diversos ámbitos de actuación, promoviendo el ejercicio legal de la profesión.

"En la actualidad, el desarrollo de las tecnologías de la información y las comunicaciones ha traído como consecuencia un incremento en la cantidad de información digital, y la necesidad de utilizarla como evidencia es un reto creciente. La Informática Forense, como aplicación forense de las ciencias informáticas, constituye una disciplina que surge para dar respuesta a una demanda cada vez mayor de especialización, tanto en ámbitos judiciales como extrajudiciales" (Di Iorio, Cistoldi et al., 2019).

Debo manifestar, que justamente en estos momentos, se presentó un anteproyecto de modificatoria de la Ley provincial Nº 9498 a fin de contener al segmento de técnicos informáticos que son actores reales en nuestra sociedad y cuyas funciones no se encuentran reguladas ni controladas en nuestra provincia. Considerando que desde hace casi veinte años el COPROCIER es la entidad madre de los profesionales de la informática en nuestra provincia es que resulta necesario incorporar en nuestro colegio a las personas con títulos en tecnicaturas informáticas y títulos intermedios de pregrado expedidos por Universidades Públicas y/o Privadas para ejercer su profesión en el ámbito de la Provincia de Entre Ríos; y que, consecuentemente, tengan el respaldo necesario y el contralor indispensable para actuar en las diferentes ramas de la informática.

Ante esa gran demanda en la provincia de Entre Ríos, esta propuesta de creación del Laboratorio de Informática Forense en el ámbito del COPROCIER, en adelante Lab-InFo COPROCIER, pretende contribuir a la concreción del mismo; en su implementación inicial, para que los peritos cuenten con herramientas de vanguardia, procedimientos y software especializado para el trabajo pericial. Esta propuesta ha sido elaborada en permanente diálogo con los peritos del COPROCIER, a efectos de su validación.

Es hoy, sin dudas, una necesidad la creación de Laboratorios Forenses que brinden estándares mínimos de calidad para el desarrollo de las actividades periciales (Di Iorio, Constanzo et al., 2017).

Implementar el Lab-InFo COPROCIER permitirá, sin dudas, brindar un nuevo y mejor servicio de calidad a los ciudadanos de la provincia de Entre Ríos.

## El Laboratorio de Informática Forense del COPROCIER

En primer lugar, la gestión del COPROCIER junto a sus matriculados en su conjunto, deberá delinear y explicitar la misión, visión y objetivos del Colegio, para de esta manera visualizar su razón de ser. En realidad hoy se rige por el estatuto de la institución Ley Nº 9498[5].

La definición de la misión, visión y objetivos, y la delimitación de los servicios y funciones constituyen la base y el punto de referencia imprescindible para el diseño y gestión de cualquier laboratorio. Por lo que el equipo de peritos definió en su conjunto estos puntos de referencia importantes para el Lab-InFo COPROCIER, debiendo presentarlo formalmente a la gestión para su consenso y posterior resolución de creación del Laboratorio de Informática Forense del COPROCIER.

Declarar la Misión Institucional significa responder a la pregunta ¿Qué nos hace "ser"? ¿Cuáles son las características esenciales que nos distinguen de otros? La Visión Estratégica permite identificar ¿Cómo queremos cumplir nuestra misión? (Appendino et al., 2015).

**Misión**

Colaborar con la justicia contribuyendo con la labor de investigación y asesoramiento como auxiliares de la justicia, mediante la realización de tareas técnico-periciales de la especialidad informático forense, que resulten útiles y relevantes para esclarecer delitos y/o probar hechos delictivos.

**Visión**

Nuestro "futuro deseado" es el ser reconocidos y referentes para la justicia, por la calidad profesional de nuestros servicios, por el actuar científico y metodológico, en pos del desarrollo de la Informática Forense y la permanente actualización.

[5] https://coprocier.org.ar/web/?page_id=33

**Objetivos:**

- La obtención de equipamiento de hardware.

- Proporcionar de herramientas de vanguardia para la resolución de pericias.

- Contar con procedimientos estandarizados y homogéneos para efectuar pericias.

- Colaborar y propiciar resultados útiles en las pericias informáticas realizadas por profesionales informáticos matriculados en el colegio.

- Implementar un sistema de análisis de demandas y tendencias de uso de los servicios del laboratorio.

¿Qué objetivos debe cumplir el laboratorio?

Definir los objetivos del laboratorio de informática forense, y frecuencia de medición (trimestral/ semestral/ anual). Estos deberían presentarse a la comisión directiva luego que se apruebe la creación del laboratorio de informática forense del colegio profesional por resolución.

Tener presente la misión que se busca y mantener una visión estratégica permitirá identificar el camino a recorrer para cumplir con la misión (Rivetti et al., 2020).

¿Cuáles son las contribuciones específicas que se esperan de un laboratorio de informática forense, para que la institución a la que pertenece ofrezca un producto o servicio de calidad a sus usuarios? El valor del aporte debería quedar reflejado, no tanto en la satisfacción de los "clientes internos" ni en estándares autorreferenciales de la oficina, sino en la satisfacción de los derechos y necesidades de los destinatarios finales del producto en el que influye el servicio prestado (Di Iorio, Cistoldi et al., 2019).

**Conceptos básicos de la actividad pericial**

- Perito Informático

El Perito Judicial Informático es aquel profesional que, en su carácter de auxiliar de la justicia, tiene la función de asesorar al juez y/o a las partes respecto a temas informáticos.

Las carreras vinculadas a las ciencias informáticas, Ingeniería en Sistemas de Información, Licenciatura en Sistemas y afines, en la Provincia de Entre Ríos se rigen bajo la

ley 9498, que da creación al Colegio de Profesionales de Ciencias Informáticas de Entre Ríos (COPROCIER). Sin embargo, aquellos profesionales de ciencias informáticas que sean ingenieros, pueden matricularse en el Colegio de Ingenieros Especialistas de Entre Ríos (CIEER[6]), creado por ley 8815.

Los peritos que actúan en la justicia provincial se capacitan regularmente a través del Instituto "Dr. Juan Bautista Alberdi"[7]. "La capacitación judicial es una valiosa herramienta para el crecimiento personal, para el desarrollo funcional y el fortalecimiento institucional, de allí que junto al staff del Instituto ponemos diariamente nuestro trabajo, esfuerzo y conocimientos al servicio de la misma." palabras de la Directora Dra. Susana Medina.

Además se cuenta con capacitación interna permanente ya que el grupo de peritos se reúne mensualmente donde se intercambian experiencias, se ayuda a los peritos noveles, se intercambian ideas y herramientas de uso libre, etc.; donde generalmente participa activamente nuestra asesora legal.

Se realizan actividades de capacitación y actualización continua (a través de reuniones virtuales, webinarios, jornadas, cursos, participación en congresos; así como fomentar y motivar a la participación en investigaciones académicas) haciendo vínculos con profesionales de trayectoria de otras provincias, de otros colegios o consejos profesionales como CPCIBA[8] Consejo Profesional de Ciencias Informáticas de la Provincia de Buenos Aires, CPCIPC [9] Consejo Profesional de Ciencias Informáticas de la Provincia de Córdoba, CPCi [10] Consejo Profesional en Ciencias Informáticas Ciudad Autónoma de Buenos Aires, C.G.C.T.I.[11] Colegio de Graduados en Ciencia y Tecnología Informática de Tucumán, entre otros, y de otros laboratorios con más experiencia como Info-Lab[12] de UFASTA, DigiLab[13] de UCASAL, etc.

[6] https://www.cieer.org.ar/release/index.php
[7] https://institutoalberdi.jusentrerios.gov.ar/
[8] https://www.cpciba.org.ar/
[9] https://www.cpcipc.org.ar/
[10] https://www.cpci.org.ar/inicio
[11] http://www.colegioinfotuc.com.ar/
[12] https://info-lab.org.ar/
[13] https://digilab.ucasal.edu.ar/

PROYECTO DE REGLAMENTO DEL CUERPO PERICIAL DEL STJER[14]

Todos los peritos que actúan desde el COPROCIER son Peritos Judiciales (Ley Orgánica del Poder Judicial de Entre Ríos[15]) peritos de oficio y peritos de parte. Todos son profesionales independientes, que realizan un análisis basado en sus conocimientos científicos, del cual se obtendrán conclusiones que permitirán elaborar un dictamen.

CAPITULO III DE LOS PERITOS Art. 130.- [Ley Orgánica del Poder Judicial N° 6902 ratificada por Ley N° 7504 y actualizada al 27/08/13] Requisitos. Los jueces y tribunales harán las designaciones de oficio de Peritos según el orden de una lista especial que deberán confeccionar antes de la finalización del año. Para inscribirse en dicha lista se exigir título a nivel terciario o universitario. Únicamente en los casos en que no hubiere en el medio Peritos del mencionado nivel se aceptarán inscripciones de expertos o idóneos en la materia.

En el año 2018 el Superior Tribunal de Justicia, mediante el Acuerdo General N° 35/18 estableció el "Reglamento para Peritos Oficiales, Eventuales y demás Auxiliares de Justicia" (Acuerdo General N° 35/18, 2018).

El perito, con el método, garantiza una forma de observar, pensar y resolver problemas de manera objetiva y sistemática. El método es un procedimiento de trabajo que permite descubrir las circunstancias en que se presentan hechos concretos y se caracteriza por ser: verificable, de observación objetiva y de razonamiento riguroso.

Parte pertinente del acuerdo general Nº 35/18 del 13-11-18. Proyecto de reglamento del cuerpo pericial del Superior Tribunal de Justicia de Entre Ríos.

En su Art. 4 dice: Los Peritos y demás auxiliares de justicia deberán analizar y dictaminar sobre aspectos técnicos y/o científicos relativos al objeto del proceso que escapan a los conocimientos exigibles al Juzgador teniendo en cuenta la diversidad de las pretensiones que se deducen ante los jueces. Dichos profesionales en el ejercicio de su función deben a través

[14] https://www.coper.org.ar/images/2018/Punto_8%C2%BA_Reglam._Peritos.pdf
[15] https://www.entrerios.gov.ar/secjusticia/userfiles/files/otros_archivos/Ley%20Org%C3%A1nica%20del%20Poder%20Judicial%20de%20Entre%20R%C3%ADos(1).pdf

del dictamen pertinente la no paralización o demora injustificada del proceso oral y por audiencias.

Los peritos, es decir, aquellos expertos designados de oficio por los jueces, en virtud de su saber específico, son sujetos auxiliares de la administración pública de justicia, cuya actividad en el proceso se desarrolla con autonomía, sin subordinación jerárquica y en base a la idoneidad técnica que deriva su título profesional para asegurar un mejor funcionamiento de la administración de justicia.

Así, el perito es un tercero ajeno a la causa, que auxilia al Juez sobre hechos controvertidos que requieren conocimientos especiales en alguna ciencia, arte, industria o actividad técnica especializada. Los dictámenes periciales deben realizarse en el plazo acordado y suministrar los antecedentes y explicaciones técnicas que justifiquen convicción sobre la materia que se expiden, en tanto su finalidad de prestar asesoramiento al órgano decisor, quien ha de valorar el acierto de sus conclusiones.

- Evidencia digital

Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático (computadoras, celulares, aparatos de video digital, etc.). Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales (Di Iorio et al., 2016).

La evidencia digital debe poseer cuatro características esenciales: relevancia, suficiencia, validez legal y confiabilidad.

Para asegurar la confiabilidad, el proceso de manejo de evidencia digital debe ser justificable, auditable, repetible y reproducible.

**Actividades previstas en la etapa inicial del Lab-InFo COPROCIER**

Considero que el laboratorio de informática forense del COPROCIER irá tomando forma respecto a qué servicios genéricos (descripciones generales de un servicio a solicitar) puede

ofrecer luego de su implementación efectiva y a medida que las estadísticas de uso y la práctica que se genere en el mismo posibiliten definir esto.

Estos servicios genéricos tienen en común una técnica, un objetivo, un objeto de estudio o una prestación, sin indicar una tecnología particular. Por ej.: "Adquisición de Imagen Forense (copia forense)".

Los servicios específicos, en cambio, se aplican a una tecnología precisa y limitada a un área de estudio. Son las capacidades específicas que tiene el laboratorio en una determinada categoría. Por ej., dentro del Servicio Genérico "Extracción de evidencia digital", estaría el específico "Extracción de evidencia en Dispositivos Móviles". Para esto se necesita hardware y software acorde y también peritos capacitados en la materia (Di Iorio, Cistoldi et al., 2019).

Para la implementación del laboratorio de Informática Forense del COPROCIER se necesita una inversión de la cual el mayor porcentaje, en nuestro caso, corresponde a la adquisición del hardware; ya que se decidió en una primera etapa trabajar con software libre y/o de código abierto (open source) y además considerando que el inmueble del colegio ya cuenta con seguridad, sistemas de alarma y de climatización.

Se deberá definir qué servicios específicos puede o debe brindar (ya sea por sus recursos en equipamiento, como por las capacidades de sus recursos humanos) o, a la inversa, dependiendo de las demandas a satisfacer, determinar el equipo requerido a tal fin, tanto tecnológico como humano. Una exigencia ineludible es la capacitación permanente y la actualización continua.

Dado que el laboratorio no existe, es complejo estimar la frecuencia de uso que tendrá el laboratorio o cantidad de pedidos, la demanda real que tendrá el laboratorio, por lo que esto se podrá conocer a partir de las estadísticas de uso cuando se lo implemente.

Se detallan a continuación algunas actividades involucradas en la función pericial (Di Iorio, Cistoldi et al., 2019), las cuales se consensuaron con el grupo de peritos que se realizan:

- Adquisición
  - ✓ Adquisición de imagen forense: implica la realización de tareas de generación de una imagen forense, acompañada de los hashes de validación de acuerdo a las necesidades del cliente.
  - ✓ Reconstrucción de un dispositivo (pocas veces): implica la realización de tareas para la obtención de una imagen a partir de un medio de almacenamiento que, por presentar fallas en su funcionamiento, no brinda garantías de continuar su operación luego de realizada la tarea, o que se pueda realizar una nueva adquisición del mismo que coincida con adquisiciones previamente realizadas.
- Extracción y Análisis
  - ✓ Extracción de evidencia - nivel aplicación: Implica la búsqueda de archivos o información contenida en archivos, utilizando el medio original o una imagen del mismo desde el punto de vista lógico (desde el propio sistema de archivos del dispositivo).
  - ✓ Extracción de evidencia - nivel plataforma: implica la búsqueda de archivos, información o metadatos por medio de mecanismos propios de la plataforma, pero a un nivel técnico más profundo que la recuperación lógica (accediendo a información específica del Sistema Operativo del dispositivo).
  - ✓ Extracción de evidencia - bajo nivel (rara vez): implica la búsqueda de archivos, información contenida en archivos o remanente sobre el dispositivo, utilizando el medio original o una imagen del mismo, desde el punto de vista físico (accediendo directamente al bloque de datos, independientemente del Sistema Operativo).

Análisis forense: es el servicio principal del laboratorio, orientado a la recuperación de información relevante para obtener evidencia y conclusiones sobre la investigación judicial. En este punto es difícil de especificar los servicios, debido a que éstos pueden ser muy variados; sin embargo, es importante destacar si el laboratorio pretende focalizarse en alguna especialidad.

Nuestro futuro Lab-InFo COPROCIER, con las estadísticas de uso y pasado un tiempo, podrá definir y especificar los diferentes servicios que ofrece; aunque considero que debemos estar abiertos y flexibles a nuevas demandas y desafíos.

El laboratorio no será responsable del resguardo de la información recuperada. Cada perito designado en una causa judicial será el responsable de esto usando sus propios recursos.

Elaboración del dictamen pericial: el aporte pericial escrito tiene la forma de dictamen, en el cual se presenta la evidencia encontrada y se responden los puntos periciales. Es recomendable que el laboratorio establezca un modelo o guía para estructurar el dictamen pericial, con el fin de asegurar que el mismo dispondrá de todos los aspectos esenciales. Este modelo deberá ser adaptado a las particularidades de cada caso.

Respecto a esto, el equipo de peritos cuenta con un Drive compartido donde se presentan diferentes modelos y demás información de interés, espacio colaborativo (Imagen Nº 1).

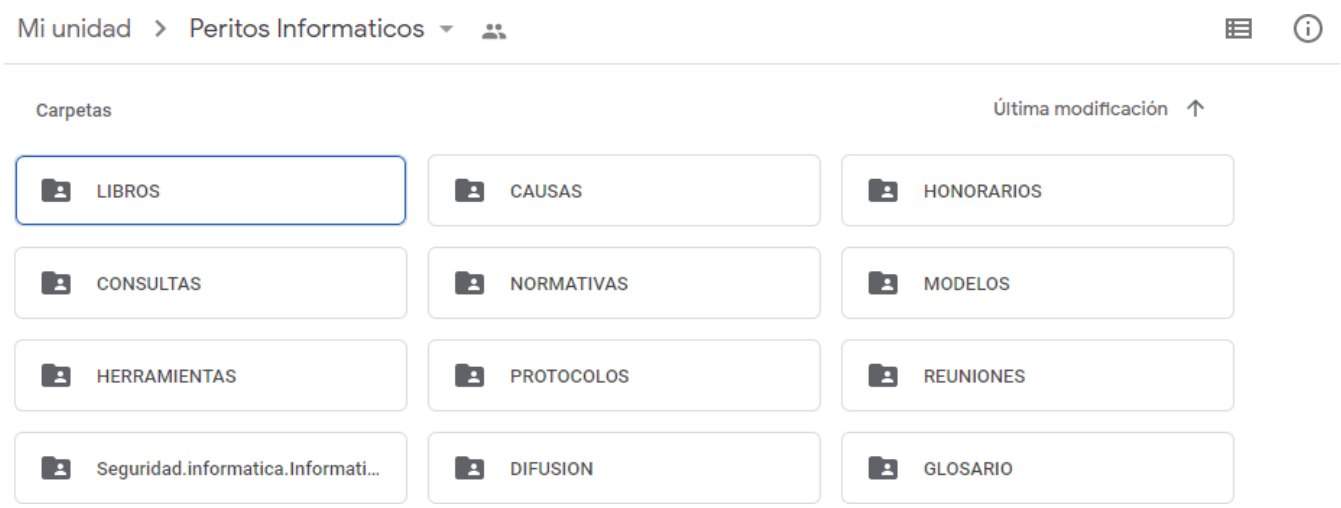


**Imagen 1 - Drive Peritos Informáticos**

En general, un dictamen de calidad debe demostrar que las labores periciales se basaron sobre evidencia o datos suficientes y confiables (o en caso contrario, formular las debidas advertencias y reservas); que las operaciones practicadas fueron realizadas utilizando herramientas y métodos fiables; que estos últimos fueron aplicados correctamente; y que las conclusiones se sustentan en el resultado de tales acciones.

Recursos humanos

El COPROCIER además de la Junta Directiva, del Directorio, del Tribunal Arbitral y de Disciplina, y del Órgano de Fiscalización cuenta con una Secretaria Administrativa, una Asesora Legal, una Asesora Contable-Impositiva y una Asesora de Comunicación y a futuro, cuando se implemente el Lab-InFo COPROCIER contará con el Director del laboratorio (Imagen N° 2).

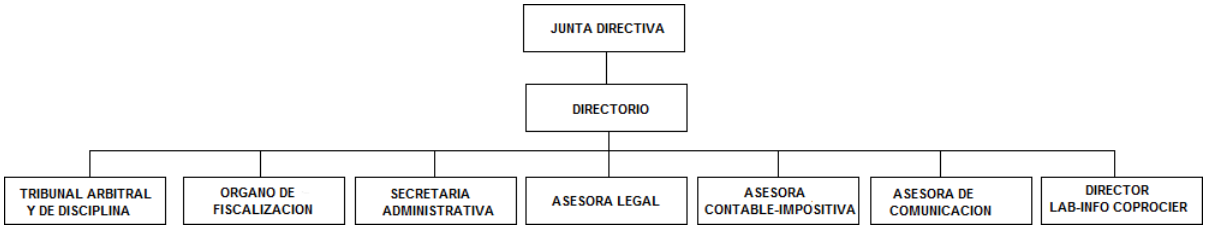


**Imagen 2 – Organigrama COPROCIER**

En nuestro caso tenemos dos tipos de personal del laboratorio, el Director del mismo y todo el equipo de peritos que conforman el registro actual y vigente y que va cambiando dinámicamente año a año, con altas nuevas y bajas.

Un laboratorio de informática forense, en líneas generales estará compuesto como estructura mínima del siguiente puesto: el Director que es el responsable máximo del laboratorio, quien firma junto al perito interviniente en el caso y avala las pericias, investigaciones e informes técnicos realizados en el mismo, organiza, gestiona y administra el laboratorio, además de identificar las necesidades de formación y capacitación de los peritos e investigadores como así también proponer al directorio la compra de nuevas herramientas o insumos necesarios. Bajo su responsabilidad se encuentran los Peritos e Investigadores.

- ✓ Director: a elección de sus pares.
- ✓ Peritos informáticos. Todos los profesionales matriculados y registrados como peritos en la provincia de Entre Ríos.

Personal de Apoyo:

- ✓ Administrativo - Secretaria Administrativa
- ✓ Asesora Legal

La secretaria administrativa se encarga de los procesos de soporte en lo que se refiere a la gestión y administración del laboratorio, asignando fechas y horarios a partir del formulario que debe completar el perito solicitante del uso del laboratorio.

El laboratorio dependerá orgánicamente del colegio, intermediando con la comisión a través del Director del mismo siendo su alcance provincial.

El equipo de peritos del COPROCIER, actualmente **34** peritos de toda la provincia de Entre Ríos. Hay peritos registrados en diferentes jurisdicciones. Se pretende y desea que este número crezca anualmente, durante el llamado al registro del año siguiente, que generalmente se realiza en el mes de noviembre (ver Imagen Nº 3).

Mapa de Entre Ríos donde se puede ver la relación entre Nº de matriculados (M) y Nº de peritos (P)
Total de matriculados activos: 438
**M: Matriculados** **P: Peritos**

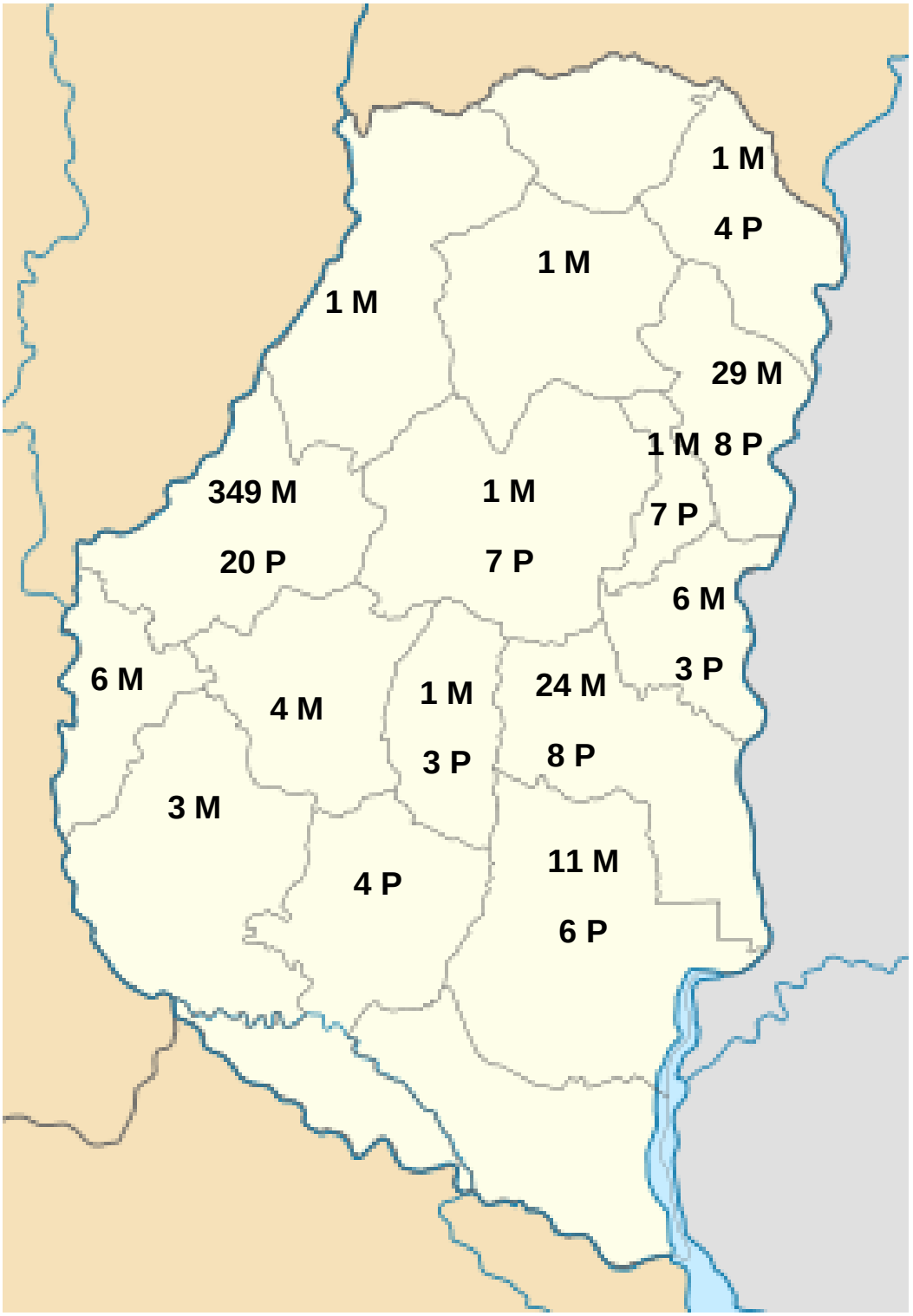


**Imagen 3 - Mapa de ER (matriculados/peritos)**

En las jurisdicciones que no aparecen peritos las mismas solicitan a la jurisdicción más cercana; por ejemplo, La Paz, Diamante, Nogoyá y Victoria solicita peritos a la MUI (Mesa Única Informatizada) del Poder Judicial de Entre Ríos de Paraná; mientras que Chajarí y Federación lo hace en Concordia.

Dentro de este gran equipo hay profesionales interesados en armar un equipo de investigación y desarrollo de herramientas propias; programando rutinas de análisis o que resuelva alguna problemática específica, utilizando Python o algún otro lenguaje de programación.

Respecto al equipo de peritos, ya se está trabajando en la gestión de conocimiento, la cooperación y colaboración entre pares para la implementación del laboratorio y se proyecta la cooperación académica con las universidades UADER, UNER y UTN. Con estas universidades el colegio ya cuenta con convenios marcos y de colaboración reciproca; ya que entre otras actividades se hacen prácticas académicas en el colegio.

**Futuras Actividades**

Los profesionales matriculados y registrados como peritos en el COPROCIER podrán hacer uso del laboratorio completando un **formulario online** previo (en Anexos se presenta). Esto permitirá llevar las estadísticas de uso y para qué se usa el laboratorio mayoritariamente.

El control de egresos e ingresos de objetos a peritar: el registro de todo objeto ingresante o saliente al laboratorio, susceptible de ser peritado o ser entregado al juzgado como evidencia es responsabilidad directa del perito que lleva la causa.

Cuando el perito fija la fecha de pericia en autos debe haber completado el formulario online reservando el uso del laboratorio forense. Espacio que pueden participar la parte que lleva el dispositivo a peritar como así los abogados de la parte actora y demandada.

Cada perito se hace responsable de su prueba pericial específica, realizando posteriormente el informe o dictamen pericial y respondiendo aclaraciones por escrito, si las hubiera, o de manera oral en la audiencia de vista de causa.

Para el correcto desempeño de las funciones, el laboratorio necesita contar con equipamiento e infraestructura tecnológica adecuada a las actividades que debe realizar, de manera que los peritos puedan enfocarse plenamente en su trabajo.

**Infraestructura edilicia**

El Lab-InFo COPROCIER se radicará en la Sede del Colegio, sito en calle Dr. Raúl Lucio Uranga Nº 3020 de la ciudad de Paraná, inmueble de 101,15 $m^2$ cubiertos que ya cuenta con alarma y con sistemas de cámara de seguridad como así también posee aires acondicionados en las distintas salas del mismo (Ver en Anexos I- Planos COPROCIER).

Contar con una infraestructura edilicia y una estructura organizativa en la cual implementar el laboratorio se considera una fortaleza y una oportunidad, ya que los costos de funcionamiento estarán amortizados por el propio colegio.

Se propone remodelar o readecuar un espacio físico del colegio para el área de procesamiento, para su implementación y puesta en marcha presentando un plan en etapas para asegurar la factibilidad del proyecto. Se presenta en Anexos una propuesta de diseño inicial, en una 2° etapa y en una final.

Se analiza el plano de la infraestructura vigente del colegio y se visualiza que presenta una única puerta de ingreso al área administrativa, donde se encuentra la secretaria administrativa. Para poder utilizar la sede del colegio hoy, ya sea para realizar una pericia o una reunión de trabajo, capacitación, taller o curso se debe; con el tiempo suficiente, reservar el espacio "sala de reuniones". Hoy esto se realiza por e-mail, teléfono o WhatsApp al celular institucional.

Pensando ya en el uso del laboratorio, el ingreso y egreso de objetos a peritar se realizará por los propios peritos del COPROCIER o por las partes que llevan sus dispositivos; serán los responsables del control; a partir del registro online de la pericia a realizar.

No se pensó en contar con un área de depósito destinado a guardar el material pericial ya que una vez finalizada la pericia; el perito, el abogado o las partes se lleva el dispositivo o se devuelve al juzgado.

En general las pericias que se realizan no dura la extracción más de un día; pero de requerir continuar al día siguiente con el trabajo pericial se podrá guardar –excepcionalmente- el o los dispositivos en un espacio de almacenamiento temporario con llave que se encuentra en el Área de Gestión. Una vez finalizado el trabajo se devuelve el dispositivo a quien corresponda.

Se diseñó un área de procesamiento dedicada a las actividades periciales propiamente dichas, donde los peritos informáticos realizan su actividad. Esta área pensada para hacer la pericia, soporta las tareas de extracción y posterior análisis. A este lugar, también pueden asistir los abogados y/o partes, para observar la realización de la pericia.

También el colegio cuenta hoy con un área administrativa, área de gestión y sala de reuniones y servicios y circulaciones que incluyen sanitarios, office y pasillos (Constanzo et al., 2018).

Dentro del área de procesamiento se propone en una primera etapa contar con 1 (un) box pericial o workstation (ver presupuesto hardware en Anexos).

Este proyecto particular se ajusta a cuestiones respecto a requerimientos, posibilidades, costumbres y presupuesto. Igualmente con las estadísticas de uso se evaluará para agregar nuevos boxes periciales en etapas futuras si es mayor y crece la demanda de requerimientos de uso del laboratorio.

Considero que el Lab-InFo COPROCIER es de todos los peritos de la provincia de Entre Ríos. Aunque igualmente considero que debe haber un director, que debería ser un profesional matriculado y perito con más de 10 (diez) años de experiencia. El Director se encargará tanto de la dirección como de la gestión del mismo y también debe conocer de las técnicas para poder asesorar a los profesionales y garantizar la capacitación y actualización continua.

El Director del Lab-InFo COPROCIER será elegido por sus pares matriculados y durará 4 años en su cargo, pudiendo ser reelecto en una segunda oportunidad.

**Funciones del Laboratorio**

La Guía Integral de Empleo de la Informática Forense en el Proceso Penal de la Provincia de Buenos Aires, Res PG SCBA 483/16 (Di Iorio et al., 2016), distingue tres roles básicos a desempeñar por los informáticos forenses: rol de asesoramiento, de investigación o pericial, cada uno de los cuales incluye un conjunto de servicios.

Un Laboratorio de Informática Forense puede cumplir con tres funciones principales y sus profesionales especialistas cumplir diferentes roles:

• Función o Rol de Asesoramiento: En ocasiones, el abogado suele necesitar la opinión de un experto para desarrollar tareas investigativas o probatorias. Por ejemplo, planificar una prueba anticipada con respecto a las fuentes de evidencia digital que se presenten en el caso, precisar los datos que han de requerirse a un proveedor de servicios, fijar puntos de pericia o interrogar al perito de la contraparte, son actividades que requieren contar con asesoramiento técnico.

• Función o Rol de Investigación: En algunos casos y/o momentos de un proceso, suele requerirse la intervención de un especialista informático para ejecutar medidas de investigación, por ejemplo: secuestro de equipos informáticos, volcado de datos de la memoria física de un equipo, obtención de la duplicación de un disco (imagen).

• Función o Rol Pericial: Bajo este rol, el experto aporta sus conocimientos especiales para conocer o apreciar algún hecho o circunstancia pertinentes a la causa, en la cual efectivamente se realiza una pericia sobre soportes de evidencia digital para obtener pruebas válidas, pasibles de ser presentadas en juicio.

La función pericial y los servicios asociados se corresponden con las tareas que el laboratorio tiene capacidad y potestad de realizar. El resultado de este servicio será el dictamen pericial que cada perito perteneciente al colegio efectúe y la correspondiente declaración del experto en el juicio oral, de ser convocado.

Un Laboratorio de Informática Forense debe tener un esquema de servicios acorde con alguna, o todas estas funciones, dependiendo las necesidades del departamento judicial y los objetivos que se buscan cumplir con la implantación de un laboratorio.

En el caso del COPROCIER, se detectó la necesidad de contar con un laboratorio forense capaz de brindar garantías de la aplicación de procesos estandarizados, permitiendo así la obtención de evidencias digitales y aportes expertos válidos, pertinentes y confiables. Para este propósito debe aplicar las técnicas y herramientas existentes, garantizando la realización de sus actividades mediante un proceso reproducible, repetible y auditable, basado en un conocimiento técnico-científico que fortalezca su valor probatorio ante los órganos jurisdiccionales.

El laboratorio debe satisfacer los intereses, en primer lugar, de los propios peritos del Colegio como así también, de los abogados de la provincia de Entre Ríos que requieran de los servicios periciales, y en definitiva la sociedad completa.

Proceso del perito de oficio[16]

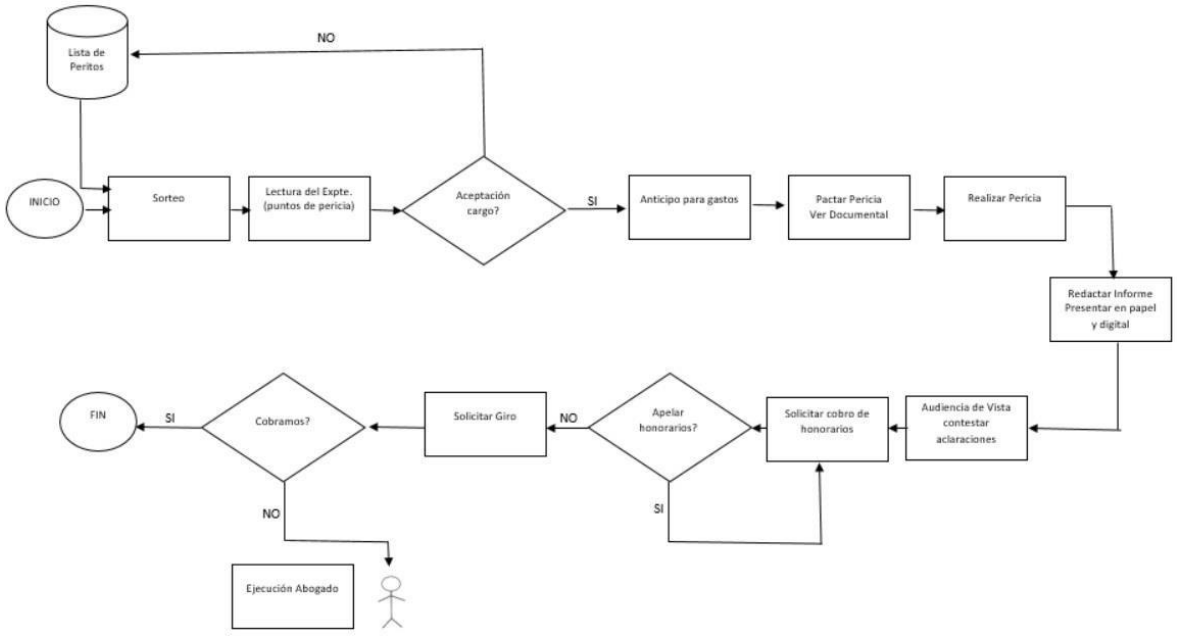


**Imagen 4 - Proceso del perito de oficio**

[16] Fuente artículo "Importancia del Perito Informático en el Ámbito Judicial de la Prov. de ER"

**Infraestructura Tecnológica**

**Hardware**

Se sugiere contemplar las siguientes categorías dentro del laboratorio: workstations, equipos portátiles, equipos de clonación y servidores (Di Iorio, Cistoldi et al., 2019).

Independientemente de la elección de tecnologías, es conveniente que las workstations cuenten en primer lugar con un disco para almacenar el sistema operativo y las aplicaciones del perito, y uno o más discos adicionales en los cuales almacenar las imágenes forenses y la evidencia digital recuperada.

Con respecto a la memoria RAM, las workstations deberían tener una buena cantidad, idealmente de la tecnología más moderna disponible. En la actualidad, estaríamos hablando de sistemas con (al menos) 16 GiB de RAM y tecnología DDR4.

En cuanto a los otros componentes, el procesador y la disponibilidad de puertos, debe tenerse en cuenta que el actuar de la informática forense suele requerir que se conecten discos (externo e internos), a través de múltiples interfaces (Serial ATA, USB 3, Firewire, Thunderbolt). Los equipos, en la medida de lo posible, no deberían ver limitado su acceso a dispositivos por los puertos e interfaces.

El procesador del equipo debe tener un rendimiento que no limite al resto del sistema. Se deberían considerar procesadores multinúcleo modernos, de al menos cuatro núcleos físicos y un TDP superior a 65 W, y cache L3 superior a 6MB. La utilización de procesadores más potentes, ya sea por contar con mayor cantidad de núcleos, o tener un TDP más elevado, permitirá acelerar operaciones de alta complejidad computacional como puede ser el crackeo de contraseñas o el análisis de información por medio de técnicas de Inteligencia Artificial.

Los equipos de clonación son computadoras o equipos especiales dedicados a la realización de imágenes forenses de los dispositivos que debe peritar el laboratorio. Si se van a utilizar computadoras para esta función, para estos equipos solamente debe considerarse que cuenten con un sistema de almacenamiento adecuado, en capacidad y rendimiento, pero no necesitan procesadores muy potentes ni grandes cantidades de memoria. Son equipos importantes en el proceso pericial en informática forense (dado que éste comienza por

la realización de una imagen), pero no requieren de un rendimiento excepcional como las workstations.

En cuanto a equipos especiales para clonación, pueden considerarse dispositivos de marcas específicas que proveen la capacidad de realizar copias forenses de distintos medios de almacenamiento, así como también de equipos que cuentan con la capacidad de realizar copia forense del contenido de teléfonos inteligentes, GPS, tablets u otros dispositivos smart. La adquisición para el laboratorio de este tipo de equipos debe estar sujeta a una evaluación de necesidad y utilidad del equipo, para justificar su alto costo. Esta propuesta no considera necesario contar con un equipo para clonación por nuestro actuar como peritos judiciales en la primera etapa del laboratorio.

Las workstations son los equipos de trabajo de los peritos informáticos dentro del laboratorio, y como tales deben ser computadoras de excelente rendimiento.

Se propone una workstation para la primera etapa con las siguientes características:

Memoria Patriot Viper DDR4 16GB 3200MHz Steel
Gabinete Thermaltake V200 Tempered Glass Ryzen Edition Sin fuente
Discos Sólido SSD M.2 ADATA 512GB FALCON 3100MB/s NVMe PCI-E x4
Procesador AMD Ryzen 7 5800X 4.7GHz Turbo AM4 - No incluye Cooler
Fuente Cooler Master MWE 650W 80 Plus Bronze
Disco Rígido Toshiba 4TB N300 NAS 7200rpm 128MB
Placa de Video XFX Radeon RX 6500 XT Black 4GB GDDR6 Speedster QICK210
Mother ASUS TUF GAMING B550-PLUS WIFI II AM4
Monitor Lenovo 22" HDMI VGA S22E

Este hardware, que está disponible, es suficiente para las prestaciones previstas en la primera etapa del Lab-InFo COPROCIER.

También se consultaron otras posibilidades (https://digitalintelligence.com/) de estaciones de trabajo forenses Fred. Los sistemas FRED establecen el estándar para las estaciones de trabajo de análisis y adquisición forense.

Esta propuesta no prevé, en su primera etapa, la incorporación de un equipo de clonación ni de equipos portátiles (que todos tienen) ni servidores de almacenamiento ya que el resguardo de la evidencia es responsabilidad de cada perito.

Esta propuesta tampoco prevé la incorporación de servidores de almacenamiento ya que no se resguardan las copias forenses en el propio laboratorio, en esta primera etapa, luego se evaluará.

**Infraestructura de Red**

El Colegio solo cuenta con red WIFI por lo que habría que instalar una red local, Ethernet de 100 Gigabit idealmente, que conecte la workstation con la PC administrativa. En otra etapa esta red no debería permitir el acceso a Internet de los servidores y equipos de clonación si los hubiere. Sólo deberán tener acceso a Internet aquellos equipos que sean estrictamente necesarios, como es el caso de las workstations o equipos para uso administrativo.

La utilización de un firewall es fundamental, ya que en el mismo se definirán las reglas de acceso a las diferentes redes dentro del laboratorio y acceso a Internet para los equipos que lo necesiten. Tomando como referencia el gráfico "Esquema Básico de Red de un Laboratorio de Informática Forense" (Di Iorio, Cistoldi et al., 2019).

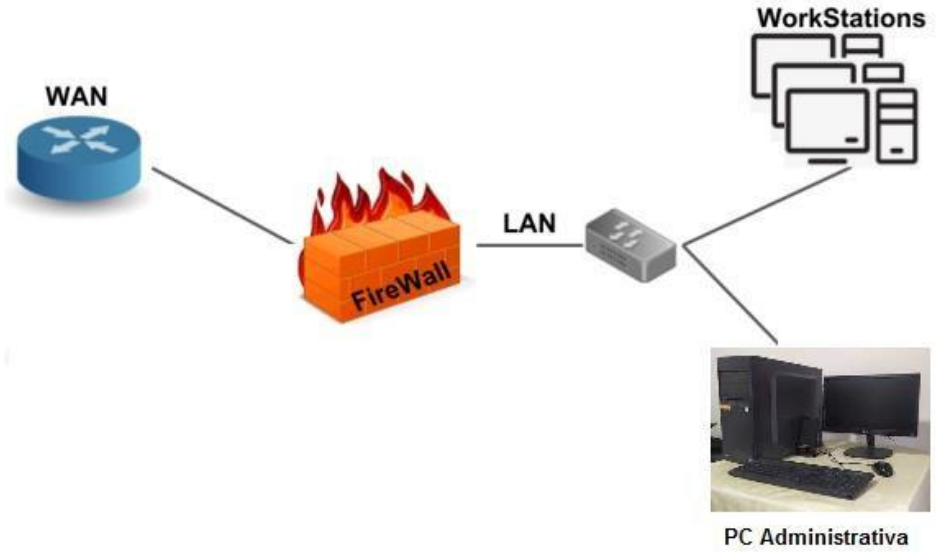


**Imagen 5 - Esquema básico de red del Laboratorio de Informática Forense del COPROCIER**

**Equipamiento Especial**

● Celulares o Tablets UFED o Equipamiento de extracción: Para el caso de los dispositivos móviles, es necesario equipamiento como software específico para realizar dicha tarea. Es por eso que las empresas Cellebrite UFED[17] o MSAB[18] o Mobile Forensics[19], por ejemplo, tienen soluciones para este tipo de tareas.

● Cámaras Fotográficas o de filmación: El COPROCIER cuenta con una cámara fotográfica y además cada perito tiene este recurso como la mayoría cuentan con una notebook.

● Equipo para proyección: El colegio cuenta con un sistema de proyección y un equipo de audio.

● Adaptadores de conexión para diferentes tecnologías (discos M.2, MicroSata, IDE, SSD, etc.)

**Software**

La idea es contar con diferentes plataformas de Sistema Operativo; Windows y Linux, que son las que habitualmente se utilizan.

Esta propuesta prevé, con el acuerdo del grupo de peritos del COPROCIER, que en la primera etapa se utilizará software libre y/o de código abierto (open source) para el trabajo pericial. Esta decisión se toma no solo por una cuestión económica sino porque al contar con el código fuente, es más seguro, hay más control y se puede contribuir al desarrollo de mejoras de las mismas. Además actualmente hay un amplio abanico de software forense libres actualizados.

Se debe contar con una herramienta que permita la correcta obtención de las imágenes forenses. Existen diversas aplicaciones para este tipo de tareas. Lo importante es que cuando se realice esta tarea, la imagen forense obtenida como resultado, sea una copia fiel y exacta

[17] https://cellebrite.com/es/ufed-ultimate-2/
[18] https://www.msab.com/products/
[19] https://www.mobiledit.com/online-store/forensic-express

al dispositivo original. Un ejemplo es la herramienta "dc3dd", de uso totalmente libre y funcionamiento en Linux.

Con respecto al análisis de estas imágenes forenses, se debe contar con una herramienta que permita la correcta gestión de las mismas. Lo que se debe contemplar son herramientas para búsquedas por palabras claves, búsqueda por hashes, archivos recientes, extracción de datos dentro de la imagen forense, búsqueda en los navegadores de Internet, en el registro del sistema operativo y todo lo relacionado a las actividades de un usuario dentro de un dispositivo informático.

Un ejemplo de paquete de software para este proceso es "Autopsy"[20], una suite muy potente, de uso libre, para realizar las actividades antes descriptas. Funciona tanto para Windows como Linux.

También utilizan algunas herramientas de CAINE[21] (entorno de investigación asistido por computadora) es una distribución en vivo italiana GNU/ Linux creada como un proyecto de análisis forense digital.

Viendo las técnicas y herramientas de informática forense en las diferentes fases mencionadas (Di Iorio et al., 2016), el equipo de peritos manifestó que ya utilizan hace bastante tiempo Autopsy, Phantom, FotoForensics, ExifTool[22], entre otras.

Siempre y en lo posible se sugiere el uso de herramientas Open Source, es decir, de código abierto, dado que éstas permiten conocer y validar los resultados que brindan, así como realizar modificaciones en su funcionamiento de ser necesario.

Considero que los peritos del colegio, profesionales muchos de ellos con carreras de posgrados, están capacitados o tienen el conocimiento de los SO para usar por consola o terminal los comandos que muchas veces te ayudan a resolver conflictos que las propias

[20] https://www.autopsy.com/
[21] https://www.caine-live.net/
[22] https://www.exiftool.org/

herramientas no resuelven. Como así también, poder desarrollar las propias herramientas del laboratorio.

**Protocolos y procedimientos que aseguran la calidad de la labor pericial**

**Proceso Unificado de Recuperación de la Información (PURI)[23]**

"En una especialidad científica como lo es la informática forense, es importante que un laboratorio pericial informático realice su trabajo mediante normas estándares, procedimientos de buenas prácticas desarrollados por entidades de gobierno y autores reconocidos" (Semprini, 2016).

El Modelo PURI® (Di Iorio, Castellote et al., 2017). (Proceso Unificado de Recuperación de la Información) establece una guía de labores a desempeñar desde el área técnico-informático forense, organizándolas en fases, actividades y tareas.


**Imagen 6 - Fases que intervienen en el Modelo PURI**

Luego el método PURI fue tomado como base para el proyecto de elaboración de un Protocolo de Actuación en Informática Forense (PAIF) por el Laboratorio de Investigación y Desarrollo en Informática Forense, en el año 2014.

[23] Modelo PURI - PAIF

El "Protocolo de Actuación en Informática Forense a partir del Proceso Unificado de Recuperación de Información - PAIF-PURI" fue acreditado por el Ministerio de Ciencia, Tecnología e Innovación Productiva de la Nación e incorporado al Banco Nacional de Proyectos de Desarrollo Tecnológico y Social de la República Argentina, mediante Res. 062/14 de la Secretaría de Articulación Científico-Tecnológica.[24]

Aunque el PURI fue pensado para el fuero penal se lo aplica a los demás fueros.

Este protocolo se basa en el Proceso Unificado de Recuperación de Información, en adelante PURI, desarrollado por el grupo de investigación en Sistemas Operativos e Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. PURI se nutre de procesos y guías de buenas prácticas en informática forense nacionales e internacionales, adaptándolas e integrándolas en un esquema de fases, etapas, tareas, técnicas y herramientas recomendadas. Se contemplan, de este modo, la planificación previa, identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva.

Respecto a equipos de telefonía celular el equipo de peritos está elaborando un procedimiento para llevar a cabo, que una vez revisado y consensuado se aprobará por resolución formal. Hoy en día de cada 10 (diez) pericias, entre 7/8 son referidas a equipos móviles. Por lo que consideramos de suma necesidad contar con este procedimiento.

Procedimiento utilizando como guía el protocolo PURI:

**1- Relevamiento**

Buscar, reconocer y documentar potencial evidencia.

Identificación de la evidencia (Peritos de parte).

Ejemplos: correos electrónicos, imágenes, videos, mensajes, llamadas, etc.

[24] Guía Integral de Empleo de la Informática Forense en el Proceso Penal

**2- Recolección y Adquisición**

Tener presente principios básicos de lo que significa una cadena de custodia.

La cadena de custodia es una secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que ésta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria[25].

Se adoptarán los principios de cadena de custodia al soporte de la información adquirida. Se sugiere obtener un hash para posterior validación, que será consignado en el acta de una prueba anticipada o en el informe pericial, con mención de la fecha, hora, lugar y dispositivo de origen.

Muchas veces los peritos de oficio se encuentran que los dispositivos se guardan en el juzgado hasta que se fija fecha de la pericia y se han encontrado, en algunas ocasiones, que los dispositivos o celulares no se encuentran debidamente rotulados ni sellados; no se resguarda la cadena de custodia ni tienen una planilla que chequee quienes recibieron el dispositivo ni en qué fecha, el estado del mismo, etc.

En tales casos, es recomendable documentar la condición en que se encuentran los dispositivos, precisando, en su caso, si ello tiene alguna clase de incidencia concreta sobre el desarrollo y conclusiones de la labor pericial.

Recolección y clasificación de evidencias según los elementos sometidos en los puntos de peritaje solicitados en los autos.

La fase de adquisición es una tarea especializada con conocimientos, habilidades y aptitudes que permitan un manejo responsable de la documental, pudiendo distinguir tres grandes grupos PC, Móviles y las nubes. Ejemplo en PC y Móviles, bloqueo del medio de almacenamiento, captura de memoria volátil y de memoria extraíble. Captura y resguardo de la imagen binaria y por último validación del original vs copia binaria.

[25] PAIF

La finalidad de esta fase es la de asegurar la confiabilidad de la evidencia digital, ya sea que se la considere en sí misma o como insumo para la labor pericial o la prueba testimonial. Se sugiere a los peritos realizar réplicas o copias forenses para efectuar análisis y pericia correspondiente sin alterar la evidencia original; siempre que sea posible.

**3- Preparación y Análisis**

Preparación del análisis, restauración de la imagen y validación.

Selección de la herramienta forense más apropiada de acuerdo a los sistemas operativos, programas, tipos de archivos y situaciones particulares presentes.

Análisis e interpretación de los resultados obtenidos.

**4- Presentación**

Armado del informe pericial con todos los pasos anteriormente documentados y en caso de ser necesario una presentación oral explicativa. Todo perito debe actuar con solvencia técnica, objetividad y veracidad. La comparecencia del perito en la audiencia de vista de causa es crucial, ya sea para ampliar o aclarar cualquier aspecto del informe y contestar a las preguntas que le hagan las partes y el tribunal.

Todos los procesos operativos que se llevan a cabo en el laboratorio, como por ejemplo la adquisición de imagen forense son bajo la responsabilidad del Perito Informático que está designado en la causa.

Los peritos y especialistas en informática deben conocer no sólo los procedimientos y herramientas técnicas recomendadas vinculadas con su función. Es necesario que conozcan también las exigencias y límites legales de su desempeño.

“Toda esa serie de obstáculos que tiene que enfrentar un informático forense (diversidad de tecnologías, métodos de ocultamiento de información, etc.) determina que el éxito de la tarea dependa de su habilidad profesional guiada por su criterio y no por un proceso formal.” Esto da cuenta de la necesidad de la existencia de un PURI que valide la labor del

perito y contemple tal diversidad de dificultades permitiendo tener una guía orientadora en la tarea de la obtención de evidencias (Podestá et al., 2013).

Queda pendiente en esta propuesta, la elaboración de un Reglamento interno de uso del Lab-InFo COPROCIER, que deberá ser propuesto por el Director y aprobado por el Colegio.

El laboratorio en una primera etapa se dedicará solo a atender los roles de asesoramiento y pericial para que luego en una segunda etapa incluya el rol investigativo.

En nuestro laboratorio el equipo de peritos profesionales tienen a su cargo todos los roles o responsabilidades ER (Responsable de Recolección - en pruebas anticipadas o pericias de parte generalmente), EA (Especialista en Adquisición), EED (Especialista en Evidencia Digital).

El perito debe garantizar la cadena de custodia (Resolución PG SCBA 889/15, 2015) si es que retira del juzgado el dispositivo a peritar, o efectúa una copia del mismo o bien si las partes junto a sus abogados traen el dispositivo al laboratorio a fin de realizar la pericia solicitada.

En una prueba anticipada o mandamiento de aseguramiento de prueba, junto al Oficial de Justicia, al abogado que la solicita y al Defensor de Ausentes el perito debe responder lo solicitado en el mandamiento haciendo trabajo de campo y peritando en el lugar. Esto presenta similitudes con lo que puede suceder en algunos allanamientos.

El Oficial de Justicia labra un acta donde informa todo lo que el perito realiza y deja constancia de lo actuado en el lugar; la cual firman todos los presentes.

El perito judicial como perito de oficio recibe siempre los puntos de pericia; pero en el rol de asesoramiento como perito de parte podemos colaborar con los abogados en elaborar los puntos de pericia. Como así también asesorar o solicitar al juez, si para realizar la tarea pericial se considera necesario contar previamente con determinados informes, como por ejemplo: reportes de proveedores de servicios de internet, o de empresas de telefonía, etc.

Respecto a solicitar al juez libre oficios para obtener cierta información, que los peritos no podemos acceder, se usa "Información para requerimientos a empresas y servicios en Internet" del Ministerio Público de la provincia de Buenos Aires (UAID Unidad de Análisis e Investigación Digital, 2021).

Para ello un perito de oficio debe responder de manera objetiva los puntos de pericias solicitados; sin extenderse más de lo pedido y dando respuesta taxativa y concreta de lo que se le pide. Si por alguna cuestión no se entienden estos puntos o son ambiguos o no claros debe comunicarse con el abogado de la parte y pedir a través de la mesa virtual o hablando con el juzgado se aclaren.

La labor pericial se realizará en el lugar, el día y hora fijados previamente por un escrito a través de la mesa virtual y proveído por el juzgado. A la misma pueden participar las partes y sus letrados.

Respecto al lugar, puede ser el juzgado, si lo autorizan, en el domicilio fijado por el perito o en el COPROCIER. Hoy en día, ya se usan las instalaciones del colegio cuando viene un perito de otra localidad de la provincia y reserva y avisa con tiempo el día y horario de realización de una pericia.

En la etapa de Análisis se analiza el contenido adquirido en busca de vestigios de lo que se pretende hallar. El Análisis Forense comprende las siguientes labores (Di Iorio et al., 2016):

**Extracción Lógica**. Se efectúa empleando el sistema operativo del equipo como intermediario para el acceso a los datos (las herramientas de extracción se comunican con el sistema operativo del equipo y es éste quien aporta los datos existentes en el sistema). La extracción lógica comprende las siguientes acciones:

- Recuperación de archivos eliminados.
- Extracción de Información a examinar por tipo de archivo.
- Extracción de metadatos del archivo en el Sistema de Archivos.
- Extracción de metadatos propios del archivo.
- Extracción de archivos protegidos con contraseña.
- Extracción de archivos comprimidos.
- Detección y extracción de archivos encriptados.
- Búsqueda de Información de Configuración.
- Búsqueda de Información de Procesos en Memoria.

**Extracción Física**. Implica la búsqueda a bajo nivel, directamente sobre los datos presentes crudos en el disco, sin contar con el sistema operativo como intermediario. Este método de extracción permite la adquisición de los datos tal como se presentan en el medio de almacenamiento persistente, posibilitando el hallazgo de archivos ocultos y eliminados parcial o totalmente y que el sistema operativo no haya podido detectar. Esta labor implica una fuerte carga de trabajo con gran cantidad de información. Se recomienda su uso sólo si no se ha podido resolver los puntos periciales con técnicas de extracción lógica. Comprende estas acciones:

- Búsqueda de información en disco.
- Búsqueda de información en el área de paginado.
- Extracción de archivos en espacio no asignado - File Carving.

Analizando los servicios que demandaron mayor atención del Gabinete de Informática Forense (Ministerio de Justicia y Derechos Humanos de la Nación, 2014). Respecto al trabajo pericial que se realiza y haciendo un análisis de las propias prácticas periciales; se valora de 1 a 10 (siendo 10 muy frecuente y 1 rara vez/casi nunca). Esta valoración fue realizada un una reunión virtual del equipo de peritos del COPROCIER.

Extracción y análisis de datos en dispositivos de almacenamiento magnéticos:

(10) Discos rígidos, (6) CD/DVD/BLU-RAY, (9) pendrives, (8) tarjetas de memoria, (6) unidades de estado sólido (SSD) y (2) GPS.

(10) Dispositivos móviles, incluidos los smartphones, dispositivos (4) PDA y (5) tablets PC (contactos, mensajes de texto SMS, mensajes de texto eliminados (SIM/ USIM), historial de llamadas (recibidas, realizadas, perdidas), audio, video, fotos e imágenes, melodías, datos del teléfono (IMEI/ESN, número de teléfono).

(5) Cámaras fotográficas, mp3, mp4, Ipods y otros dispositivos similares.

(4) Dispositivos de conectividad de redes de datos, como swith, router y pendrive de redes móviles.

(5) Recuperación de archivos borrados en medios magnéticos.

(8) Reconstrucción de actividades y operaciones ejecutadas en computadoras, relacionadas con archivos de datos, Internet, mensajería, correos electrónicos, imágenes y videos.

(9) Determinación de origen/destino de correos electrónicos y su ubicación aproximada geográficamente.

Lectura y análisis de registros activos y volátiles:

(3) Estado de las memorias RAM (capacidad, programas ocupados, bloqueos, porcentaje de uso).

(3) Procesos activos (uso de CPU, dependencias de procesos y componentes).

(3) Conexiones de red (conexiones actuales a otras pcs, servidores, etc.).

(2) Impresiones activas (cola de impresión local, documentos sin imprimir, estado y descripción de documentos que se están imprimiendo).

(1) Red individual, de la empresa u organización (características, tráfico, congestión, bloqueos, sniffers activos, virus de red, etc.).

De esta forma, se podría pensar en realizar una primera clasificación de áreas de intervención de los informáticos forenses, de acuerdo al medio del que se extrae la evidencia digital (Di Iorio, Constanzo et al., 2017):

- Forensia en Equipos (Computer Forensics)
- Forensia en Dispositivos Móviles (Mobile Devices Forensics)

- Forensia en Redes (Networking Forensics)
- Análisis de Datos Forenses (Forensic Data Analytics)
- Análisis Forense de Archivos Multimedia (audio, video y sonido)
- Forensia en Bases de Datos (Database Forensics)

Interpretación de la evidencia digital para elaborar el dictamen o informe pericial respondiendo a los puntos de pericias solicitados.

Un informe o dictamen pericial de calidad debe demostrar que las labores periciales se basaron sobre evidencia o datos suficientes y confiables que las operaciones practicadas fueron realizadas utilizando herramientas y métodos fiables.

Tomando como referencia una muestra compuesta por las últimas 30 (treinta) pericias del autor de la propuesta, se presenta a continuación una tabla indicando fuero, si fue pericia de parte o de oficio y tipo de tarea realizada.

| Fuero | Perito de Oficio/de Parte | Tipo de tarea |
|---|---|---|
| Familia | Oficio | Forensia Redes Sociales |
| Civil y Comercial | Oficio | Forensia en Dispositivos Móviles |
| Civil y Comercial | Oficio | Forensia de E-mail y sitios web |
| Laboral | Oficio | Forensia Redes Sociales - imágenes |
| Laboral | Oficio | Forensia en Dispositivos Móviles |
| Civil y Comercial | Oficio | Forensia de E-mail |
| Civil y Comercial | Oficio | Forensia en Dispositivos Móviles - imágenes |
| Laboral | Oficio | Forensia de videos - sistema de seguridad |
| Laboral | Oficio | Forensia en Dispositivos Móviles (WhatsApp) |
| Civil y Comercial | Oficio | Forensia en Dispositivos Móviles (WhatsApp) |
| Laboral | Oficio | Forensia de E-mail |
| Laboral | Oficio | Forensia en Dispositivos Móviles (WhatsApp) y Redes Sociales |
| Laboral - prueba anticipada | Oficio | Forensia en Dispositivos Móviles |
| Laboral - prueba anticipada | Oficio | Forensia en Equipos |

| | | |
|---|---|---|
| Laboral | Oficio | Forensia en Dispositivos Móviles |
| Laboral | Oficio | Forensia en Dispositivos Móviles |
| Laboral | Oficio | Forensia de E-mail |
| Laboral | Oficio | Forensia Redes Sociales |
| Laboral | Oficio | Forensia en Dispositivos Móviles (WhatsApp) |
| Laboral | Oficio | Forensia en Dispositivos Móviles (WhatsApp) |
| Laboral | Oficio | Forensia de E-mail y en Dispositivos Móviles (WhatsApp) |
| Civil y Comercial | Oficio | Forensia de E-mail |
| Civil y Comercial | Oficio | Forensia en Redes (Homebanking) |
| Laboral | Parte | Forensia en Dispositivos Móviles (WhatsApp) |
| Civil y Comercial | Oficio | Forensia en Dispositivos Móviles (WhatsApp) y Redes Sociales |
| Civil y Comercial y Laboral | Oficio | Forensia de videos - sistema de seguridad |
| Civil y Comercial y Laboral | Oficio | Forensia de E-mail |
| Laboral | Parte | Forensia en Dispositivos Móviles (WhatsApp) |
| Familia | Parte | Forensia en Dispositivos Móviles (Billetera virtual - bitcoins) |
| Laboral | Oficio | Forensia en Dispositivos Móviles (WhatsApp) - Audios |

Esto nos da un indicio de en qué tipos de dispositivos se está trabajando, en el 80% de los casos se trabaja con móviles, y qué se está haciendo y; en rara vez, dentro del 20% aparece una pericia más compleja e interesante que nos hace estudiar, investigar y consultar en algunas oportunidades a otros expertos profesionales en la temática del país y de otras provincias. Respecto a las prácticas periciales que se desarrollan, "Ley 80/20" que justamente hay "pocas vitales o novedosas/interesantes" respecto a "muchas triviales o ya conocidas".

Igual hay que destacar que aunque se trabaje mucho sobre dispositivos móviles, cada caso tiene sus particularidades; diferentes modelos y sistemas, si funcionan o no, si encienden o no, difieren los puntos de pericias, etc.

En Anexos se presenta un glosario alfabético de términos con el propósito de facilitar la lectura y consensuar dentro del laboratorio de los términos y conceptos específicos; igualmente deberá actualizarse a medida que se actualizan las tecnologías tanto de hardware como de software y por lo tanto surgen nuevas herramientas y conceptos.

## Conclusiones

El Lab-InFo COPROCIER pretende contribuir a uno de los objetivos del COPROCIER "Estimular el profesionalismo y prestigio de la profesión, así como promover las buenas prácticas profesionales", de calidad.

Los cambios en las tecnologías, plataformas, medios de almacenamiento, legislaciones y aplicaciones de software, hacen cada vez más necesario el uso de procesos, métodos, estándares y buenas prácticas, que brinden algún tipo de garantías en la recuperación de información almacenada digitalmente y, sobre todo, que permitan asegurar que se realizaron todas las tareas posibles con los mecanismos adecuados.

El grupo de peritos del COPROCIER requieren de procedimientos estandarizados y gracias a este laboratorio se pretende comenzar a estandarizar los procedimientos para la obtención de la información en celulares, tablets, computadoras, etc. La actuación pericial requiere el respeto de protocolos y guías de buenas prácticas que aseguren el trabajo metódico.

El equipo de peritos del COPROCIER, que actúan bajo este Laboratorio, tendrán que afianzar la relevancia, suficiencia, confiabilidad y validez legal de la evidencia analizada; la fiabilidad de los métodos y herramientas de análisis empleados; la correcta aplicación de dichos métodos y herramientas; y la solidez lógica y científica de los razonamientos que dan sustento a sus conclusiones.

Se considera vital continuar con los encuentros de trabajo donde el objetivo es el intercambio, la investigación, puesta en común y compartir experiencias sobre todo, hacer consultas a la Asesora Legal o a los pares y resolver inquietudes, esto permite el enriquecimiento y el crecimiento de todos. De esta manera también vamos delineando las convenciones y criterios comunes a seguir dentro del futuro laboratorio, y se da para generar nuevos conocimientos y procedimientos.

Se promueve y apoya la capacitación permanente de los peritos o auxiliares del Poder Judicial del COPROCIER, con el fin de tender a alcanzar mejores niveles de calidad en nuestro laboratorio y fomentar la interacción interdisciplinaria. Para ello se comunica y difunde de

carreras de posgrados vinculadas a la informática forense como así también de congresos y reuniones científico-académicas.

Además se fomenta la realización de actividades de actualización, de posgrados, participación en congresos; realización de publicaciones[26]; el COPROCIER da ayuda económica o beca o media beca todos los años a 2 (dos) profesionales matriculados para la realización de especializaciones, maestrías y/o doctorados.

Los peritos, matriculados del COPROCIER y su gestión concuerdan y defienden al profesional informático de la provincia de Entre Ríos; por lo que debido a diferentes situaciones y eventos se sacó una solicitada en el Diario de Paraná[27] página 7, en fecha 3 de abril de 2022.

"...desde el Colegio de Profesionales de Ciencias Informáticas de Entre Ríos (COPROCIER) exhortamos al Poder Judicial y al Estado provincial a garantizar el estricto cumplimiento de la Ley 9498, la cual regula el ejercicio profesional de los informáticos en Entre Ríos y la actividad misma, estableciendo específicamente las competencias exclusivas de los profesionales debidamente matriculados, siendo la actividad pericial una de ellas."

"Los tres poderes que conforman el Estado Provincial (Ejecutivo, Legislativo y Judicial) tienen el deber inquebrantable de respetar y hacer respetar las leyes que nos rigen."

"La Ley 9498 se encuentra vigente desde el año 2003 y establece los requisitos para el ejercicio profesional de los/as informáticos/as con título de grado, dentro de los que se incluye la matriculación obligatoria, determinando expresamente las incumbencias profesionales inmersas."

Un informe pericial de informática forense en la provincia de Entre Ríos, debe ser firmado por un profesional de Informática matriculado. Estoy a favor del trabajo

[26] Artículo en la revista académica Scientia Interfluvius de la UADER "Importancia del perito informático en el ámbito judicial de la provincia de Entre Ríos" https://drive.google.com/file/d/154mRvIMB22mCibCvd8pzcaB3NuzpCbU4/view

[27] https://www.eldiario.com.ar/193119-mira-la-edicion-impresa-de-el-diario-3-4-2022/

interdisciplinario y multidisciplinario pero por un tema de incumbencias y de ley estos informes DEBEN ser firmados por un profesional informático y matriculado.

Está prevista la realización de convenios entre las universidades presentes en la provincia que otorgan títulos de grado de informática (UADER, UTN, UNER, Universidad Adventista del Plata) y con la provincia de Entre Ríos a fin de capacitar al personal policial y del poder judicial. Como así también se ha firmado convenio con el CAER (Colegio de la Abogacía de Entre Ríos) y CAER Sección Paraná. Próximamente con otras Secciones.

Queda pendiente la vinculación o firma de convenio de colaboración con otros laboratorios forenses de la provincia; a saber con el Ministerio Público Fiscal - Gabinete de Informática Forense, la policía y gendarmería de la provincia de Entre Ríos.

La República Argentina cuenta con pocos laboratorios de Informática Forense, sobre todo en la esfera de la Justicia, aunque la demanda y necesidad de los mismos es cada vez mayor, en un escenario caracterizado por la alta y creciente demanda, pocos laboratorios, pocos peritos y ausencia de guías para la construcción de un laboratorio de Informática Forense (Di Iorio, Mollo et al., 2016).

Considero que la provincia de Entre Ríos cuenta con pocos laboratorios de informática forense; además en oportunidades se ha querido entablar relaciones con los laboratorios de la policía y de la gendarmería; sin lograr ningún resultado. Por lo que la creación, operación y organización de laboratorios dedicados a la realización de pericias informáticas es una temática en donde las instituciones y la sociedad en su conjunto aún demandan respuestas.

Vale la creación de herramientas forenses útiles para el ámbito de trabajo, generación de trabajos académicos presentados en congresos académicos que permita no solo acentuar los conocimientos adquiridos sino también su implementación. Profesionales expertos trabajando juntos para posicionar y lograr que la informática forense se ubique en un lugar desde el cual pueda brindar mayor confianza para la justicia y para la sociedad. La necesidad de crear un nuevo centro de apoyo.

El Lab-InFo COPROCIER de la ciudad de Paraná, provincia de Entre Ríos, estará compuesto por peritos informáticos encargados de realizar, como tarea principal, pericias informáticas de cualquier dispositivo que sea contenedor de evidencia digital (Resolución PGN Nº 756, 2016), así como también, tareas de asesoramiento e investigación.

La cultura de la calidad y la mejora continua representan una vía para que los servicios de un laboratorio de informática forense sean útiles, confiables, oportunos, eficientes y no se vuelvan obsoletos.

Pensar a futuro en el diseño de un Sistema de Gestión de Calidad (SGC) para los Laboratorios de Informática Forense requiere, en primer lugar, de un análisis de su situación actual, que identifique sus falencias y puntos de mejora, para luego poder contemplar de forma integrada todas sus características y necesidades; y desarrollar el SGC que aborde dicha situación (Di Iorio, Lamperti et al., 2019). Esto será otro proyecto sin dudas.

## Bibliografía

Acuerdo General Nº 35/18. (2018) Nuevo reglamento del cuerpo pericial aprobado por el Superior Tribunal de Justicia de la Provincia de Entre Ríos. 13 de noviembre de 2018. https://www.jusentrerios.gov.ar/institucionales/extracto-del-acuerdo-general-no-35-18-del-13-11-18/

Appendino S., Aprile F., Gallo B. (2015). *Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense.* CACIC 2015, Junín, Buenos Aires, Argentina.

Constanzo B., Malaret P., Vega P., Cistoldi P., Di Iorio A. (2018). *Arquitectura y Organización de Laboratorios de Informática Forense*. Red Congreso Iberoamericano de Docentes e Investigadores en Derecho e Informática. InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense Universidad FASTA, Ministerio Público de la Provincia de Buenos Aires, Municipalidad de General Pueyrredón.

Di Iorio A. H., Cistoldi P., Constanzo B., Giaccaglia M. F., Greco F., Iturriaga J., Lamperti S., Nuñez L., Malaret P., Mollo M., Podestá A., Trigo S., Vega P. (2019). *Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense*. InFo-Lab. Universidad FASTA.

Di Iorio A. H., Constanzo B., Vega P., Lamperti S. B., Giaccaglia M. F., Cistoldi P., Nuñez L. (2017). Aspectos Estratégicos, Organizacionales y de Infraestructura en el Diseño de Laboratorios Judiciales de Informática Forense. CIIDDI 2017, La Habana, Cuba. Recuperado de https://info-lab.org.ar/images/pdf/2017/VII-CIIDDI-Aspectos-Estrategicos-Organizacionales-Estructura-Diseo-LIF.pdf

Di Iorio A. H., Castellote M. A., Constanzo B., Curti, H., Waimann J., Alberdi J. I., Cistoldi P. A., Giaccaglia M. F., Greco F., Iturriaga J. I., Lamperti, S. B., Nuñez L., Podestá A., Ruiz De Angeli G. M., Trigo S. (2017). *El Rastro Digital del Delito. Aspectos Técnicos, Legales y Estratégicos de la Informática Forense*. Universidad FASTA Ediciones.

Di Iorio A. H. et al. (2016) *Guía Integral de Empleo de la Informática Forense en el Proceso Penal.* Segunda edición. InFo-Lab UFASTA. Recuperado de http://redi.ufasta.edu.ar:8082/jspui/bitstream/123456789/1592/2/PAIF.pdf

Di Iorio A. H., Lamperti S., Coppes L., Constanzo B. (2019). *Guía técnica para el diseño de laboratorios judiciales de informática forense.* InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense Universidad FASTA.

Di Iorio A. H., Mollo M., Cistoldi P., Lamperti S., Giaccaglia M. F., Malaret P., Vega P., Iturriaga J., Constanzo B. (2016). *Consideraciones para el diseño de un Laboratorio Judicial de Informática Forense.* CIIDDI 2016, Santa Fe, Argentina.

Ministerio de Justicia y Derechos Humanos de la Nación. (2014) *Laboratorios Regionales de Investigación Forense*. - 1a ed. - Ciudad Autónoma de Buenos Aires: Infojus. Recuperado de http://www.saij.gob.ar/docs-f/*ediciones*/libros/Laboratorios_Regionales_de_Invest._Forense.pdf

Podestá A., Constanzo B., Waimann J., Castellote M., Sansevero R. (2013) *PURI: Proceso Unificado de Recuperación de Información*.

Resolución PGN Nº 756/16. (2016). *Guía de obtención, preservación y tratamiento de evidencia digital* - https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

Resolución PG SCBA Nº 889/15. (2015). *Protocolo de Cadena de Custodia.* https://www.mpba.gov.ar/files/documents/889-15.pdf.

Rivetti E., Gamarra A., Parra de Gallo H. B. (2020). *Proyecto de Creación de un Laboratorio de Forensia de IoT.* Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza. Recuperado de https://reddi.unlam.edu.ar/index.php/ReDDi/article/download/114/242/

Semprini G. (2016). *Lineamientos para la creación de laboratorios informáticos forenses.* 45 JAIIO - SID 2016, Buenos Aires, Argentina.

UAID Unidad de Análisis e Investigación Digital. Ministerio Publico Provincia de Buenos Aires. (2021). *Información para requerimientos a empresas y servicios en internet*.

**Sitios Web**

COPROCIER – *Colegio de Profesionales de Ciencias Informáticas de Entre Ríos*. URL: https://coprocier.org.ar/web/

*Ministerio Público Fiscal de la Provincia de Entre Ríos* - https://mpf.jusentrerios.gov.ar.

**Videos**

Di Iorio A. H. (2020). *Laboratorio de Informática Forense. Buenas prácticas en el tratamiento de la evidencia digital*. https://www.youtube.com/watch?v=yblHvyHq9Co