Aspectos Estratégicos, Organizacionales y de Infraestructura en el Diseño de Laboratorios Judiciales de Informática Forense

Strategic, Organizational and Infrastructure Aspects in the Design of Judicial Digital Forensics Laboratories

Ana H. Di Iorio, Bruno Constanzo, Paula Vega, Sabrina B. Lamperti, Fernanda Giaccaglia, Pablo Cistoldi*, Luciano Nuñez
Univerisdad FASTA, Ministerio Público de la Provincia de Buenos Aires
Mar del Plata, Argentina
{diana, bconstanzo, fernandag, mpvega, slamperti, lnunez}@ufasta.edu.ar
* pcistoldi@mpba.gov.ar

***Resumo* — La informática forense es una disciplina nueva que se encuentra en constante crecimiento. En su proceso evolutivo, se ha detectado como una necesidad la creación de Laboratorios Forenses que brinden estándares mínimos de calidad para el desarrollo de las actividades periciales. Para ello, se propone elaborar una guía técnica que tenga en cuenta en su implementación determinadas pautas básicas, tales como: la infraestructura edilicia, los recursos humanos, el equipamiento adecuado a dichas tareas y los protocolos y procedimientos que aseguran la calidad de la labor pericial. En su desarrollo, se busca integrar el conocimiento de otras disciplinas de reconocida raigambre, procurando que el trabajo interdisciplinario coadyuve a la labor de los peritos informáticos lo que redundará en una mejora del servicio ofrecido, ya sea judicial o extrajudicial.**

Palabras Clave – informática forense; laboratorios periciales; protocolos; recursos humanos; estándares de calidad.

***Abstract* — Digital forensics is a new discipline in constant development. In its evolutionary process, it has been detected as a necessity the creation of Forensic Laboratories that give a minimum baseline of quality for the forensic activities. To that end, the development of a technical guide has been proposed, which will consider certain basic guidelines in its implementation, such as: buildings infrastructure, human resources, adequate technical equipment for the tasks, and protocols and procedures that ensure the quality of the experts work. In its development, we seek to integrate knowledge from other disciplines of recognized tradition, procuring the interdisciplinary work helps the digital forensics experts, which will result in a better service offering, whether judicial or extrajudicial..**

Keywords – digital forensics; judicial laboratories; protocols; human resources; quality assurance.

I. INTRODUCCIÓN

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 constituye una disciplina que surge para dar respuesta a una demanda cada vez mayor de especialización, en ámbitos tanto judiciales como extrajudiciales.

Sin embargo, las labores periciales suelen realizarse en espacios deficientes con falta de recursos humanos, con carencia de reglamentaciones y de equipamiento e infraestructura necesarias. En este aspecto la informática forense no se encuentra aún a la par de otras disciplinas como la medicina, balística, química, antropología, entomología, toxicología u otras ciencias forenses, y es tan necesario como en ellas el contar con un espacio de trabajo, equipo, instrumental y organización adecuados a la tarea.

El desarrollo de una guía para la implementación de laboratorios de informática forense brindará pautas para que la creación de los mismos sea adecuada. Incluso permitirá medir y evaluar la calidad de los procesos periciales, sentando las bases para la definición de programas de calidad en este tipo de laboratorios.

Es dable destacar que en la región se han llevado a cabo proyectos e investigaciones similares [1-3, 13] que brindan un soporte adicional a la tarea de nuestros investigadores. No obstante, su desarrollo se ha centrado en temáticas específicas del trabajo, como el análisis y tratamiento de la evidencia digital para la identificación, obtención, reconstrucción, análisis y presentación de la información que pueda ser válida dentro de un proceso legal; o bien en el abordaje de aspectos de infraestructura y equipamiento básico de un laboratorio.

Este trabajo, en cambio, pretende abarcar otros aspectos no considerados anteriormente, a través del estudio en conjunto con otras disciplinas, tales como la criminalística, la medicina legal, la arquitectura, la psicología y la abogacía.

En una publicación anterior [4], se ha definido el contexto en el cual se exponen las cuestiones relativas al marco teórico y estado del arte de la informática forense, los roles y niveles de actuación de los profesionales que intervienen, así como las problemáticas actuales y la misión, visión y objetivos institucionales en el diseño de un laboratorio judicial en informática forense.

Como resultado del presente, se propone delinear los aspectos relativos a la planificación estratégica, la organización y gestión, los vinculados a los recursos humanos necesarios para las diferentes tareas que desarrollan los informáticos forenses de acuerdo a sus roles, así como la capacitación y asesoramiento que puedan recibir y brindar; las cuestiones inherentes a infraestructura tecnológica y los protocolos y procedimientos que permiten asegurar estándares de calidad en la actuación dentro de un laboratorio forense..

Las conclusiones de la investigación resultan, de esta forma, una propuesta de un modelo que pueda servir como referencia en estas áreas, constituyendo un avance del desarrollo final de la *Guía Técnica para la implantación de Laboratorios de Informática Forense (GT-LIF).*

II. METODOLOGÍA

El Proyecto de Investigación para la elaboración de una Guía Técnica para implantación de Laboratorios de Informática Forense (GT-LIF) prevé el trabajo conjunto del Grupo de Informática Forense de la Facultad de Ingeniería de la Universidad FASTA con los agentes fiscales e instructores puestos a disposición por parte del Ministerio Público de la provincia de Buenos Aires, en el ámbito del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense [5].

El proyecto se caracteriza por su trabajo interdisciplinario, y de esta manera hace uso de conocimientos científicos y tecnológicos propios de la Informática Forense, recurriendo también a otras disciplinas como el derecho, la medicina forense, la arquitectura, la psicología y la criminalística. Este trabajo conjunto permite una continua retroalimentación y enriquecimiento mutuo, que da como resultado nuevos conocimientos, productos u objetos científicos.

Es por este motivo, que el equipo de investigación se encuentra compuesto de la siguiente manera: seis (6) ingenieros informáticos (dos de los cuales se desempeñan en el Ministerio Público del Departamento Judicial de Mar del Plata), una (1) médica forense (Directora del Instituto de Ciencias Forenses del Departamento Judicial Junín), un (1) arquitecto, una (1) psicóloga, un (1) estudiante de la Licenciatura en Criminalística y tres (3) abogados (2 de los cuales se desempeñan en el Ministerio Público de la provincia de Buenos Aires).

Para arribar al resultado esperado, es decir, la confección de la Guía Técnica para la Implementación de un Laboratorio de Informática Forense Judicial, se dividió el trabajo en 5 etapas:

1. Determinación de los instrumentos e instancias formales necesarias para la elaboración de una guía técnica de implantación de un laboratorio de informática forense.
2. Diseño de Aspectos Estratégicos e Institucionales.
3. Diseño de Aspectos Edilicios y Estructurales.
4. Diseño de Aspectos Tecnológicos.
5. Definición de instrumentos particulares basados en las guías de diseño para caso modelo.

Con relación a la metodología de trabajo, en primer lugar se realizó una recopilación de documentación y trabajos existentes en otras disciplinas forenses, así como en la propia de la informática, que fueron compartidos por medio de una plataforma virtual para ser analizados y puestos en común en las reuniones semanales del equipo, las cuales se encuentran destinadas principalmente al intercambio de ideas aprovechando los distintos puntos de vista de los investigadores. Esta exploración documental se complementa con la experiencia práctica de los informáticos forenses en sus lugares de trabajo, tanto desde el plano netamente laboral como el académico, generando de esta forma un enriquecimiento en los resultados de la investigación, al poseer características propias que la distinguen de otros aportes intelectuales.

Por otra parte, a la fecha se está trabajando en la confección de una encuesta que colaborará en la determinación de las necesidades y realidades de los laboratorios forenses existentes en Argentina. Sus resultados permitirán trabajar sobre los puntos críticos y proponer mejoras para la solución de tales carencias.

III. DISCUSIÓN Y RESULTADOS

A. Laboratorios Forenses

Cuando se habla de análisis de evidencia forense, ya sea física o digital, automáticamente asociamos la palabra laboratorio a la representación de un laboratorio de ciencias forenses, que no es ni más ni menos que el ámbito propicio para la realización de las pruebas científicas y tecnológicas sobre esa evidencia. Es un lugar dotado de los medios necesarios para efectuar investigaciones, experimentos, prácticas y trabajos de carácter científico, tecnológico y técnico que serán realizadas por personal capacitado y especializado al servicio de la justicia, del derecho y de la detección y esclarecimiento de delitos.

En el caso de la creación de un Laboratorio de Informática Forense presupone nuevos desafíos; en cuanto debe contemplar la particular naturaleza de su objeto de estudio. Puesto que la evidencia digital es esencialmente virtual, pero reside o se aloja en medios físicos que la contienen, todo proceso sobre ella lleva la impronta híbrida, de tener que ser tratada mitad como evidencia física (en cuanto al soporte) y mitad como evidencia virtual (en cuanto al análisis intrínseco de la misma).

En un laboratorio de evidencia física, como puede ser uno donde se realice búsqueda y análisis de muestras de partículas

GSR [1] , su estructura, organización, y funcionamiento se ordenarán necesariamente para ser eficaz en el manejo de este tipo de evidencia (desde que ingresa la muestra hasta su egreso) y no será, en términos generales, muy diferente al resto de los laboratorios en donde se analizan evidencias de características físicas, como lo puede ser un laboratorio de análisis de rastros o un laboratorio de documentología[14].

En cambio, el Laboratorio de Informática Forense debe ser igual de cuidadoso y eficaz a la hora de manipular los soportes de su evidencia, los dispositivos electrónicos que la contienen, pero además, deberá estar preparado para el análisis y la preservación de esa prueba digital teniendo especial cuidado en poseer los medios necesarios para realizar y resguardar la labor pericial en condiciones de seguridad adecuadas, teniendo en cuenta que esto implica no sólo la seguridad física, sino también la seguridad informática.

Un Instituto de Investigación Científica, especializado en Ciencias Forenses cumple además la función de promover y gestionar trabajos de investigación de sus integrantes a través de las diferentes ramas que abarque (balística, informática, comunicaciones, etc.) y difundir los resultados de dichas investigaciones, contribuyendo también así al desarrollo científico y tecnológico de la sociedad. Será un punto a considerar, entonces, si el laboratorio se encontrará inserto en un instituto de ciencias forenses, o sólo se contemplarán objetivos de servicios periciales.

B. Planificación Estratégica, Organización y Gestión

Ninguna actividad profesional puede ser desarrollada sin un mínimo de planificación y de gestión. Insistir sobre este punto es aún más importante cuando se trata de una actividad compleja desde varios puntos de vista, tal como sucede con la labor de los laboratorios de informática forense. En esta área confluyen los incesantes desafíos técnicos, los conflictos y dilemas jurídicos, y una complicada trama de interacciones entre actores que emplean distintos lenguajes y portan intereses diferentes. Asimismo, la diversidad de regímenes procesales, las variadas formas de inserción de los laboratorios en el ámbito forense y la creciente necesidad de servicios especializados no permiten modelar estructuras tipo con valor universal. Por ejemplo, debe ser muy diferente la planificación y organización del trabajo de un laboratorio que incluye dentro de sus servicios la realización de intervenciones rápidas o la cooperación en un rol investigativo, que el de otro que sólo lleva a cabo labores periciales. En el primer caso, será necesario organizar guardias, disponer de herramientas específicas, y consensuar procedimientos con otras dependencias. Las prácticas institucionales vinculadas con el manejo y gestión de efectos, o la conservación de copias de trabajo, pueden ser otras variaciones críticas que han de ser tenidas en cuenta. La existencia o inexistencia de una oficina orientada a la custodia de efectos digitales marcaría una diferencia significativa. Éstas son simples muestras de las posibles configuraciones que puede tener un laboratorio de informática forense.

En este contexto, cualquier modelo de dirección y gestión "llave en mano" parece destinado al fracaso. Los planes y los procesos de trabajo deben tener un cierto nivel de flexibilidad para responder adecuadamente a las exigencias y condicionamientos del entorno, lo que no impide encontrar algunos puntos comunes ni trazar lineamientos generales.

Para llevar a cabo eficazmente la planificación estratégica de un laboratorio, resulta necesario, en primer lugar, **clarificar su misión**. En el caso de laboratorios que pertenecen a una institución determinada o prestan colaboración casi exclusiva a ella, será importante definir interactivamente con sus autoridades cómo serán el alineamiento y articulación esperados. Todo ello exige realizar un esfuerzo para precisar, entre otras cosas:

A. Los intereses que dan motivo a los servicios demandados, y la contribución que se espera brinde el laboratorio para su satisfacción.

B. Los condicionamientos presupuestarios, de infraestructura y personal, los marcos institucionales y normativos.

C. La proyección a futuro de las dos variables precedentes.

Los intereses que demandan satisfacción pueden pertenecer a un destinatario final (cliente externo), o a un usuario intermedio (cliente interno). A su vez, un laboratorio informático forense es también cliente interno de otras oficinas o entidades. Si el laboratorio es estatal, debe partirse de una base ética y jurídica indiscutible: todo funcionario o empleado estatal está al servicio de la ciudadanía, es un servidor público. Las cadenas o redes de clientes y proveedores internos deben estar orientadas a brindar ese servicio en forma eficiente. Si desde una perspectiva conceptual tal exigencia es clara, la realidad del desempeño institucional suele mostrar contradicciones y ambigüedades. Lograr instaurar en una dependencia estatal la búsqueda constante de la excelencia es sólo un paso. En muchas ocasiones, la calidad de los productos o servicios que esa estructura brinda es medida en función de criterios puramente internos o, cuanto mucho, con base en estándares teóricos. Cuando el cauce de la excelencia no desemboca en el beneficiario final, muchas áreas de una institución se estancan, mientras que otras se desbordan, y en ningún caso ello redunda en un servicio de calidad. Un segundo cometido fundamental de la dirección y planeamiento estratégicos de una oficina es, entonces, el de **optimizar las relaciones con los otros eslabones de la cadena de valor**.

Siempre existirá la necesidad de una planificación y organización puramente interna, pero incluso esta dimensión está fuertemente influida por condicionantes institucionales. Algunos de estos factores son: el grado de descentralización y de autonomía; las políticas y procedimientos de compras; las reglas y prácticas de designación, capacitación y promoción de personal; los niveles de conocimiento acerca de la informática forense en los distintos clientes internos y proveedores internos; el clima organizacional.

---

[1] *Gun Shot Residue* en Inglés, Residuo de Disparo de Arma de Fuego: partícula característica de forma esférica y tamaño casi molecular, formada por plomo, bario y antimonio, procedente únicamente del disparo de un arma de fuego de la acción del fulminante o iniciador del cartucho [6].

Al trazar planes y diseñar procesos de trabajo, debe partirse de una línea de base (estado actual), la cual servirá para fijar metas específicas (estado deseado). Ambos extremos permitirán, a su vez, efectuar periódicas mediciones de avance. En sentido, la gestión de calidad de una oficina requiere una adecuada retroalimentación. A la luz de los objetivos fijados, es necesario conocer y medir los aspectos críticos del funcionamiento del laboratorio, de los flujos de trabajo y de las demás interacciones con el entorno. Esto no es sencillo, ya que ciertas modalidades tradicionales de control de gestión y de elaboración de estadísticas suelen conspirar contra la eficiencia del servicio a la sociedad. Cabe mencionar tres desvíos que es necesario evitar en esta cuestión. Primeramente, el modelo de registro inspirado en la contabilidad. Medir variables críticas para ajustar el desempeño no es contabilizar. En segundo lugar, el modelo de control disciplinario también es claramente ineficiente y conspira contra la motivación del personal. Lamentablemente, en el seno de muchas entidades suele verse una conjunción de ambos modelos. La resultante, con frecuencia, es la existencia de estadísticas obligatorias cuya confección distrae valioso tiempo de trabajo, pero que nunca redundan en mejoras. La construcción y uso de **indicadores** debe estar siempre alineada con las **metas de desempeño**.

Si se considera pertinente implementar en un laboratorio estatal algún modelo de auxilio a la gestión pensado para organizaciones privadas, debe desarrollarse un análisis detenido y una cuidadosa adaptación de dicha metodología. Además, el método a utilizar y los indicadores a construir deben ser articulables con los demás métodos e indicadores empleados en el entorno institucional. Una herramienta útil para explorar es el tablero de comando o **cuadro de mando integral**. A través del mismo es posible organizar y presentar datos, facilitando el control de gestión y la toma de decisiones. En el tablero de comando se mide el desempeño de una organización u oficina desde cuatro perspectivas, con sus respectivos conjuntos de indicadores: 1) resultados financieros, 2) clientes, 3) procesos internos y 4) recursos humanos. En un laboratorio estatal, debe hacerse un esfuerzo para definir las perspectivas de medición ya que las recién mencionadas no reflejan con exactitud la realidad de la gestión. Por ejemplo, la perspectiva financiera de un laboratorio que no tiene control sobre esta variable debería ser revisada y reformulada.

La planificación, la organización del trabajo, la gestión, la elaboración y empleo de indicadores deben ser contemplados en **distintos niveles o escalas**. El nivel que representa el punto de partida es el del propio laboratorio. Es allí donde pueden definirse, con cierto grado de autonomía, las metas de desempeño. Dichas metas deben estar alineadas con la planificación general de la oficina, y dicha planificación debe a su vez estar inspirada en la misión de la dependencia. Es además necesario compatibilizar planes y metas con los de las oficinas-cliente y las oficinas-proveedor. Esta compatibilización no se da en el vacío: a mayor escala, es menester la articulación y el alineamiento -de cada oficina y de cada modo de vinculación entre oficinas- con los planes, prioridades y misión de la institución, con miras a la mejor satisfacción del cliente final: la sociedad. A menor escala, es también importante armonizar estos planes y metas con los de cada agente o funcionario. Esta dimensión de la gestión, que no suele ser adecuadamente atendida en el interior de los organismos estatales, está vinculada con las condiciones de trabajo. Existen dos razones para otorgar a este tema la dedicación que merece. Por un lado, quien se desempeña como servidor público es, ante todo, una persona cuyos derechos deben ser respetados. Uno de sus derechos consiste en gozar de un espacio para planificar su propio aprendizaje y su carrera profesional. Por otro lado, desde una perspectiva crudamente utilitaria es fácil percibir cómo la calidad de vida laboral es uno de los principales factores reguladores del desempeño individual y grupal.

Es inevitable la existencia de conflictos y disonancias entre distintas instancias de cada uno de estos planos. La actividad estratégica de la dirección de una dependencia -en nuestro caso, un laboratorio informático forense- incluye la interacción constructiva para promover mejoras en todos los planos y facilitar la generación de sinergias. En ocasiones, los conflictos revelarán fallas del laboratorio. Ello es una oportunidad para detectar áreas o puntos de posible mejora. En otros casos, será necesario aliviar (o reforzar) el nivel de demandas y exigencias que pesa sobre un determinado profesional. En otras situaciones, será prudente plantear a los responsables de otras dependencias o a las autoridades jerárquicas la existencia de problemas ajenos al laboratorio que afectan el rendimiento de éste (por ejemplo: rigidez o falta de conocimiento del área de compras; prácticas de designación o promoción injustas y desmotivantes; sobreexigencia de tareas finalmente irrelevantes en el proceso judicial). En este marco, un desafío importante es el de contribuir a la elaboración y empleo de indicadores de productividad de los vínculos del laboratorio con las dependencias cliente y las dependencias proveedor, y de indicadores de alineamiento con la misión y las metas institucionales. Al respecto, resultaría útil **consensuar criterios para clasificar las tareas**, por ejemplo, según niveles de urgencia, complejidad, costos, importancia del caso y relevancia de la labor experta. El seguimiento de estos datos permitiría diseñar procesos de trabajo, asignar tareas y recursos, elaborar escenarios y planificar a corto, mediano y largo plazo.

Las consideraciones que siguen abordan cuestiones que, si bien podrían ser conceptualmente consideradas como parte de la planificación, tienen una particular relevancia, lo que torna aconsejable su tratamiento en forma específica.

C. Personal y Recursos Humanos

El ámbito forense es diverso y complejo, ya que los distintos espacios de inserción del perito en el mismo delimitan diferentes lugares de práctica profesional. Para seleccionar los integrantes del laboratorio no solo se debe tener en cuenta las funciones compuestas por las actividades, requerimientos y responsabilidades de cada uno de los roles, sino también el perfil profesional y el tipo de competencias que debe reunir la persona para poder asumir el reto tanto laboral como profesional, además del compromiso ético.

Por ejemplo, una faceta que debe tenerse en cuenta es la labor interdisciplinaria dentro del laboratorio. En este sentido, el ámbito médico-legal refleja un estándar a seguir para la Informática Forense. Así, se observa que para la identificación de las causas, mecanismos y maneras en que se produjo una

muerte se requiere la intervención de peritos en papiloscopía, odontología, radiología, antropología, inmunohematología, y ADN. El laboratorio médico-legal interviene en el examen tanatológico, traumatológico, y en toma de muestras para su análisis por áreas más específicas: laboratorio anatomo-patológico, toxicológico, serológico, balístico, entre otros.

Análogamente, se puede pensar para la Informática Forense las distintas áreas de intervención de quienes se especializan en esta disciplina, para así establecer de manera clara cuáles servicios debería brindar un laboratorio informático forense, atendiendo a que cada una de éstas requiere de un conocimiento especial y de una capacitación continua del personar ya que día a día se presentan nuevos desafíos determinados por su crecimiento exponencial.

Como se explicó en un trabajo anterior [4] los **niveles de actividad** de un informático forense se han definido así:

- Responsable de Identificación (que no correspondería al laboratorio)
- Especialista en Recolección
- Especialista en Adquisición
- Especialista en Evidencia Digital

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:

- Forensia en Equipos (*Computer Forensic*s)
- 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*)

Sin embargo, también es posible considerar que un informático forense puede profundizar su conocimiento con relación a una especialización temática, similar a la organización en que suelen dividirse las Unidades Fiscales de acuerdo a los delitos que investigan o su complejidad. De esta forma, podría diferenciarse la labor en las siguientes categorías, sin perjuicio de otras que no se hayan considerado:

- Ciberdelitos (*grooming*, distribución de pornografía infantil por internet, *ransomware*, *phishing*, accesos no permitidos a sistemas, etc.)
- Delitos Económicos (cometidos por medios informáticos)
- Análisis de teléfonos móviles (aplicable a todos los tipos de delito)
- Robos Calificados
- Usurpaciones
- Amenazas y Violencia de Género

No obstante, más allá de las posibles subdivisiones que pudieran realizarse, será necesario establecer un organigrama del laboratorio, que agrupe todas las especialidades y que permita conocer cómo se inserta dentro de la organización judicial, visualizando las funciones y responsabilidades de cada uno de los integrantes, así como las jerarquías y relaciones de poder entre ellos. También se debe tener en cuenta que la actividad forense dentro de la justicia es un trabajo en equipo, tanto de los integrantes de un laboratorio como de todos los intervinientes en el proceso judicial. En este sentido, se lo entiende como la colaboración y cooperación [7] que realizan todos los intervinientes en el proceso judicial para llegar a resolver un hecho de manera justa.

1) Capacitación

Por otra parte, el personal del laboratorio debe tener los conocimientos técnicos adecuados, e idealmente conocer cuestiones técnicas y procesales específicas de la Informática Forense. Es importante tener en cuenta que, debido al rápido progreso y cambio característico de la informática en general, la capacitación y aprendizaje debe ser una constante en todos los niveles de especialización de los investigadores informáticos. En este sentido, se plantea que deben considerarse al menos tres instancias de capacitación dentro de un Laboratorio de Informática Forense: Capacitación Interna, Actualización Profesional y Capacitación Externa.

En cuanto a la capacitación interna, el laboratorio debe proveer un ambiente propicio para el intercambio de conocimiento entre los distintos especialistas, fomentar la investigación (tanto científica como criminal) y el desarrollo profesional. Las metodologías para lograr estos objetivos pueden ser variadas, pero se sugiere:

- Realizar trabajo de a pares, especialmente para el caso de transferencia de conocimientos. Por ejemplo, un Especialista en Adquisición podría enseñar a un Especialista en Recolección sobre las tareas y herramientas adquisición de imágenes forenses al momento de realizar una imagen en el laboratorio.
- Conferencias internas, que brinden un espacio de consulta sobre la mejor forma de actuar, compartir experiencias, o permitan revisar la metodología aplicada y los resultados obtenidos en casos complejos.
- Talleres de estudio y aplicación práctica de herramientas y técnicas nuevas o desconocidas por integrantes del laboratorio.
- Documentación de metodologías aplicadas en hojas de datos.
- Fijar un día, hora y lugar para realizar encuentros de trabajo donde el objetivo sea el intercambio, la investigación, puesta en común y compartir experiencias, consultas y dudas, que permite el enriquecimiento y el avance de los profesionales en su actuar. De esta forma se van delineando las convenciones y criterios comunes a seguir dentro del laboratorio, y se da para generar nuevos conocimientos y procedimientos.

Esta es solo una lista de sugerencias y, en la medida que se vaya desarrollando la actividad del laboratorio, se podrá encontrar un conjunto de metodologías que obtengan los mejores resultados para realizar las capacitaciones. Se insiste en que la capacitación interna sea una actividad permanente, ya que el ritmo de cambio de la tecnología es capaz de anular rápidamente la capacidad de un profesional que no se capacita.

Además de la capacitación que pueden brindarse internamente los especialistas, es necesario que realicen actividades de **actualización y adquisición de nuevos conocimientos** y metodologías para aplicar en la labor pericial informática forense. El laboratorio debe proveer y facilitar los medios para que los profesionales realicen algunas de las siguientes actividades:

- Cursos de posgrado en tecnologías específicas y/o informática forense.
- Participación en congresos de informática forense o un área temática afín.
- Especializaciones, Maestrías y Doctorados en temas afines.
- Publicación del conocimiento adquirido.

El laboratorio también puede brindar **capacitaciones externas**, tanto para terceros ajenos al laboratorio, pero con quienes tenga un convenio o relación institucional (como podría ser en el caso de un laboratorio estatal que capacite a miembros de las fuerzas de seguridad), como a otros integrantes del Ministerio Público que se encuentren en otros departamentos judiciales.

El laboratorio, además de un instrumento para la resolución de las pericias informáticas es una herramienta de formación, tanto hacia su propio personal, como al personal de Ministerio Público y otras instituciones que, en el marco de convenios adecuados, necesitan recibir formación y conocimiento de informática forense.

Las capacitaciones externas pueden plantearse como modalidad de eventos especiales como talleres, cursos, congresos, o simplemente acompañando a las actividades propias de la capacitación interna con la incorporación al personal adicional que participará de ellas.

Si hubiere información sensible o reservada al laboratorio a la que fuera necesario acceder para la realización de las actividades de capacitación, se deberá consultar con las autoridades adecuadas al respecto de cómo se puede compartir o anonimizar la información, ya que es importante mantener el secreto profesional sobre determinadas acciones, conocimientos o métodos que, de difundirse de manera inadecuada, pudieran afectar a futuras investigaciones.

D. Infraestructura Tecnológica

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 informáticos puedan enfocarse plenamente en su trabajo. En esta sección se consideran las cuestiones tecnológicas, equipamiento, herramientas, e infraestructura de soporte a la actividad del informático forense.

1) Equipos de computación

Se sugiere contemplar las siguientes categorías dentro del Laboratorio: *workstations*, equipos portátiles, equipos de clonación, y servidores. Teniendo en cuenta que se debieran adquirir equipos nuevos para la realización de las tareas periciales, se desarrolla a continuación una serie de consideraciones para cada categoría.

Las ***workstations*** son los equipos de trabajo de los peritos informáticos dentro del laboratorio, y como tales deben ser computadoras de excelente rendimiento. Deben considerarse, en el siguiente orden de importancia, los siguientes aspectos del equipo: sistema de almacenamiento, memoria RAM, disponibilidad de puertos (USB, SATA, Thunderbolt, etc) y procesador. Dejando de lado el aspecto técnico por un momento, los equipos deben resultar cómodos de usar, y en ese sentido se recomienda que, además de contar con componentes internos adecuados, los monitores, mouses, teclados y demás periféricos auxiliares sean adecuados y se encuentren a la par en calidad con el resto del equipo. Considerando que estos componentes pueden tener una vida útil prolongada, la inversión monetaria que se realice sobre ellos se amortizará en calidad de vida y comodidad de los expertos del laboratorio durante años de trabajo.

El sistema de almacenamiento de los equipos es un componente crítico y debe ser de excelente rendimiento, ya sea en capacidad de almacenamiento, en velocidad o en ambos aspectos. El tamaño del sistema de almacenamiento condiciona si el perito puede trabajar sobre una copia local de la evidencia digital que debe analizar, o si deberá usar un complemento, como podría ser un disco externo, o el acceso a través de la red local a la evidencia almacenada en otro equipo. En cuanto a su rendimiento, al ser el componente más lento del equipo, el sistema de almacenamiento marcará el ritmo al que el perito irá obteniendo los resultados de sus tareas de análisis.

Entrando en consideraciones prácticas, al momento de presentar este trabajo se puede realizar la siguiente evaluación de las alternativas posibles:

- Los discos de platos clásicos brindan la mayor capacidad de almacenamiento por el menor costo, pero presentan una velocidad de lectura y escritura limitada frente a las otras alternativas.
- Los discos de estado sólido brindan mayor rendimiento en cuanto a velocidad de lectura y escritura, pero los modelos que cuentan con mayores capacidades de almacenamiento son caros.
- Una variante dentro de esta categoría son los dispositivos NVMe, diseñados para conectarse a través de la interfaz PCI Express, lo que les permite lograr mayores velocidades de lectura y escritura, a un costo incluso superior.
- La utilización de RAID, es un complemento que permite combinar medios de almacenamiento de cualquiera de las dos tecnologías vistas, brindando mayor velocidad y capacidad de almacenamiento.

Estos beneficios vienen con un costo económico y la complejidad adicional de armar y mantener esta configuración en el sistema.

- Independientemente de la elección de tecnologías, es conveniente que las workstations cuenten en primer lugar con un disco (ya sea de platos o de estado sólido) para almacenar el sistema operativo y las aplicaciones del perito, y uno o más discos adicionales en los cuales almacenar las imagenes forenses y la evidencia digital recuperada. De esta forma, la evidencia y la información privada de aquellos que se investigue quedan siempre alojadas en dispositivos fácilmente identificables, sobre los que se pueden realizar operaciones de borrado seguro cuando finalice la investigación correspondiente.

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. A futuro, las necesidades de los sistemas y la progresión tecnológica indicarán mayores capacidades de memoria y otra tecnología superior.

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 de los equipos debe tener un rendimiento que no limite al resto del sistema. Al año 2017, se deberían considerar procesadores *multicore* modernos, de al menos dos núcleos físicos y un TDP [2] de 65 W. 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, pero este tipo de actividades no suele ser determinantes en el tiempo de realización de pericias.

La decisión final sobre los componentes para armar las *workstations* debe realizarse teniendo en cuenta todas estas consideraciones y realizando un balance entre las necesidades del laboratorio, los expertos y el presupuesto disponible. Tampoco es necesario que todos los equipos cuenten con las mismas características, por ejemplo, puede plantearse un tipo de *workstation* con alta capacidad de almacenamiento y rendimiento normal, y otro con menor capacidad de almacenamiento y alta velocidad.

El Laboratorio puede contar con **equipos portátiles**, *notebooks* o *ultrabooks* que pueden servir para que el perito realice tareas de campo o presentaciones en juicios. Las tareas de campo pueden incluir allanamientos, capacitaciones o medidas de investigación para las cuales se requiera la utilización de equipos por parte del perito fuera del laboratorio. Se pueden realizar consideraciones similares a las *workstations*, pero teniendo en cuenta que se trata de equipos más caros, y que su rendimiento no es tan crítico en la función que se les asigna en el laboratorio.

Los **equipos de clonación** son computadoras o equipos especiales dedicados a la realización de imágenes forenses de los dispositivos que debe periciar 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 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 equipos de marcas específicas que proveen la capacidad de realizar copias forenses de distintos medios de almacenamiento, así como también de equipos especiales como pueden ser teléfonos inteligentes, GPS, *tablets* u otros. 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.

Es conveniente que los equipos de clonación puedan conectarse, a través de la red LAN, a los servidores de almacenamiento y automatizar el proceso de copia de la imagen forenses a los mismos. De esta manera, una vez que finaliza el proceso de imagen forense, la misma pasa a estar disponible para el acceso de los peritos a través de la red interna sin necesitar la interacción explícita de una persona.

Sobre los **servidores**, puede plantearse que en el Laboratorio se cuente con servidores de almacenamiento, o servidores de procesamiento. Los servidores de almacenamiento se plantean como servidores de muy alta capacidad de almacenamiento (en el orden de varios TiB, al año 2017) que se utilice para mantener copias maestras de las imágenes forenses realizadas por los equipos de clonación, sujeto a un protocolo para la administración de los procesos de resguardo de la copia maestra y su destino final (o un sistema que respete el protocolo).

2) Infraestructura de Red

El laboratorio deberá contar con una red local, Ethernet de Gigabit o 10 Gigabit idealmente, que conecte las *workstations* de los peritos entre sí, con los servidores del Laboratorio. Esta red, u otra dentro del laboratorio, debería permitir el acceso a internet de manera segura para los equipos.

La conectividad entre las *workstations* de los peritos y los servidores permite mover archivos e imágenes forenses dentro de la red, desde y hacia las computadoras donde sean necesarios. Esto permite, por ejemplo, que los peritos realicen una copia local de una imagen forense en su *workstation*, preservando en un servidor de almacenamiento una copia maestra, o eventualmente accedan de manera remota a una

[2] *Thermal Design Power* es un objetivo de consumo eléctrico de un procesador. En los procesadores modernos, es el punto que influye más fuertemente sobre el rendimiento, ya que estos ajustan su velocidad para cumplir con un determinado consumo.

imagen demasiado grande para ser copiada de manera local en su *workstation*.

La conexión a Internet disponible para los investigadores tiene que contar con el ancho de banda suficiente para que se puedan realizar videoconferencias sin que se degrade la calidad de imagen y sonido, ante la posibilidad de que participen de un juicio de manera remota, o se comuniquen con especialistas en otras zonas geográficas para capacitación o consulta. La utilización de un *firewall*, DMZ y otras soluciones de protección y seguridad en la red están sujetas a la organización de la misma, o la utilización de varias redes con distinto propósito. El objetivo final es que el laboratorio se encuentre lo menos expuesto posible a ataques informáticos que puedan comprometer su operación o la privacidad de la información que allí se maneja.

Dentro del laboratorio también puede instalarse *mirrors* de los repositorios de software utilizados por los peritos, tanto del sistema operativo como de aplicación. Esto permite que todos los peritos cuenten con la misma versión de los programas de aplicación, las últimas actualizaciones del sistema operativo utilizado, y optimizar el uso de ancho de banda a internet para estas tareas.

E. Protocolos y Procedimientos

Los estándares de calidad de los laboratorios periciales suelen medirse a través de una serie de indicadores que permiten generar confiabilidad en los resultados de las pericias requeridas por la autoridad judicial. Entre ellos se destacan: el manejo de la evidencia (manipulación y almacenamiento o resguardo), el procedimiento de cadena de custodia, la metodología empleada para el análisis, así como las técnicas y herramientas utilizadas a dicho fin. A ello pueden sumarse los controles de calidad y la participación en programas de comparación interlaboratorio[3]. A continuación, se desarrollarán solamente dos de estos estándares.

1) Metodología empleada para análisis, técnicas y herramientas

Tradicionalmente, las ciencias forenses han establecido *metodologías* tanto para la identificación, obtención, y recolección de los indicios de la comisión de un delito, como así también para su análisis y valoración, valiéndose para ello del *método científico*, al ser éste un modo objetivo y sistemático de resolver problemas, que permite fácilmente su observación y reproducción en caso de ser necesario. Se caracteriza por poseer cinco fases: planteamiento del problema, formulación de una hipótesis, obtención de lineamientos de la hipótesis, experimentación, interpretación y conclusiones.

Por su parte, el uso de una metodología adecuada reduce los niveles de deficiencia y de cuestionabilidad que pudieran realizar las partes en un proceso judicial, ya que se propugna la utilización de técnicas científicas cuyos resultados no deberían ser controvertidos al basarse en el conocimiento científico. Para ello, las ciencias forenses -en su desarrollo- han ido perfeccionando el método científico hasta volverlo imprescindible. Las características que lo conforman en cuanto resulta ser fáctico, objetivo, permite trascender los hechos, metódico, comprobable, y verificable [8], permiten ser tenidos en cuenta a la hora de implementarlos en la Informática Forense.

De esta forma, se busca que la labor que lleven a cabo los especialistas en informática forense, quede enmarcada en un método científico a la usanza tradicional que llevan a cabo colegas de otras ciencias forenses, para que de esta forma se pueda garantizar la correcta recuperación de las evidencias digitales relacionadas con el hecho de estudio. Para este propósito, entonces, se busca la aplicación de técnicas y herramientas que permitan garantizar un proceso reproducible de adquisición, examen, análisis, cotejo, preservación y presentación de la evidencia, basado en el conocimiento científico, que fortalezca su valor probatorio ante los órganos jurisdiccionales.

Con este norte, marcado por las ciencias forenses y la criminalística tradicional, investigadores de la Universidad FASTA elaboraron un Proceso Unificado de Recuperación de la Información (PURI®) [9], orientado a la identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva.

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. Adaptado a las necesidades e integrándolo a las regulaciones legales vigentes en materia penal, logró ser aprobado y recomendada su aplicación como *"Guía integral de empleo de la Informática Forense en el Proceso Penal"* [15] en el ámbito de la Provincia de Buenos Aires[4].

2) Controles de calidad

Los laboratorios ya existentes en las ciencias forenses tradicionales nos aportan estructuras de trabajo y metodologías ya consolidadas, de las cuales la Informática Forense debe aprehenderlas para así poder establecer servicios de calidad, acordes con estándares ya existentes en la materia.

Los sistemas de calidad brindan confiabilidad en los resultados por el cumplimiento de la normativa específica, por la garantía de los servicios ofrecidos y las técnicas y herramientas implementadas para la obtención de los objetivos, además de lo atinente al recurso humano: imparcialidad, objetividad, conocimiento, capacitación y confidencialidad en el manejo de la información con las consecuentes responsabilidades legales en cabeza del director y del equipo que lo conforma.

La calidad es una cualidad que permite una comparación contra un estándar. La calidad se logra mediante la **normalización**, esto es la redacción y aprobación de pautas

[3] Al respecto puede verse este documento sobre "Laboratorio de Toxicología y Química Legal" de la Suprema Corte de Justicia de Buenos Aires, disponible en: http://www.scba.gov.ar/pericial/laboratorios/labtq.pdf

[4] Mediante Resolución General 483/16 de la Procuración de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Copia disponible en http://www.info-lab.org.ar/images/pdf/Res48316.PDF

que se establecen para garantizar la calidad de los productos y servicios, con el fin de satisfacer las necesidades o los requerimientos de las personas que reciben el servicio. De este modo la normalización persigue tres propósitos fundamentales: *simplificar*, es decir reducir las diligencias y trámites, procediéndose con los necesarios para lograr una mayor eficiencia; *unificar*, esto es, permitir la estandarización a nivel internacional; y *especificar*, que implica crear un lenguaje claro y preciso acorde a la labor pericial [10].

En este sentido, la norma IRAM 301 - ISO/IEC 17025 [11] establece los requisitos generales para la competencia de los laboratorios de ensayo y calibración, fijando el objeto y campo de aplicación (punto 1), documentos de consulta (punto 2), términos y definiciones (punto 3), requisitos relativos a la gestión (punto 4) y los requisitos técnicos (punto 5).

Existe, a nivel legislativo, una propuesta de aplicar esta norma a los laboratorios forenses de la Provincia de Buenos Aires [12], que, de aprobarse, resultaría un avance importante en la estandarización de los procedimientos técnico–científicos, así como la efectiva aplicación de los protocolos ya existentes para algunas de las ciencias forenses, así como la necesidad de regular en aquellas disciplinas en las que aún no se hayan desarrollado.

IV. Conclusiones y Trabajo Futuro

Este trabajo tiene como fin exponer una serie de cuestiones a considerar a la hora de diseñar la implantación de un laboratorio de informática forense, el que, como toda dependencia destinada a brindar un servicio, está inserto en un contexto funcional, institucional y geográfico.

El producto "Laboratorio de Informática Forense" puede ser excelente de manera aislada, disponer del software apropiado, contar con el personal capacitado, cumplir con todas las previsiones arquitectónicas y de infraestructura, y, sin embargo, si no se adapta al contexto en el que está inserto desde el punto de vista estratégico e institucional, puede no resultar útil. Es decir, puede ser un "buen producto" pero una "mala solución" a las necesidades de la organización, y, en definitiva, de la ciudadanía.

Es por esto que debe tenerse especialmente en cuenta que servicios se brindarán, quiénes son los demandantes de los servicios y quiénes van a recibir los resultados.

La guía resultante del proyecto de investigación, no será un "kit" del cual surge mágicamente un laboratorio, sino una dirección sistémica y orgánica que da una visión general para guiar la implementación de un nuevo laboratorio. Esto será delineado como una serie de preguntas que guiarán al lector en los aspectos a considerar para su diseño.

Además, está previsto que en base a ciertos datos que se pueden obtener de las medidas de gestión del laboratorio, como por ej.: frecuencia de solicitud de ciertos servicios, tiempos de resolución, carga de trabajo, utilización de los recursos, entre otros, es posible utilizar sistemas de modelado y simulación para analizar cómo se comportaría un laboratorio particular ante distintas situaciones, o evaluar qué cambio tendría un mayor impacto en el funcionamiento del mismo. De esta manera, se pretende colaborar en el diseño de adaptaciones de laboratorios ya implantados, así como, en la mejora de los tiempos de respuesta. Dentro del *Proyecto GT-LIF* un equipo se encuentra trabajando en esta temática específica.

Se espera que este proyecto aliente a mejorar la calidad en el nivel de servicios de los laboratorios de informática forense, así como concientizar en la importancia de pensar en su diseño, en el convencimiento que constituye un aporte a una mejor calidad del servicio de justicia.

Agradecimientos

Agradecemos a la Universidad FASTA, el Ministerio Público de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon por fomentar la investigación en el espacio que es el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense InFo-Lab.

También queremos agradecer en especial a Fernando Greco, Santiago Trigo y Ariel Podestá por sus aportes a la redacción, revisión y mejora de este trabajo.

Referencias

[1] Calderón Valdiviezo R. G., Guzmán Reyes G. S., Salinas González J. M., Aranda A. (2012). *Diseño y Plan de Implementación de un Laboratorio De Ciencias Forenses Digitales*. Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral.

[2] Umaña Ramirez G., Mosquera Navarrete I. C. (2014). *Diseño e Implementación de un Centro de Informática Forense en la Universidad Autónoma de Occidente*. Departamento de Operaciones y Sistemas, Facultad de Ingeniería, Universidad Autónoma de Occidente.

[3] Semprini, G. (2016, Sep). *Lineamientos para la creación de laboratorios informáticos forenses*. Paper presentado en 45 JAIIO/SID 2016.

[4] Di Iorio, A. H., Mollo, M., Cistoldi, P., Lamperti, S., Giaccaglia, M. F., Malaret, P., Vega, P., Iturriaga, J., Constanzo, B. (2016, May). *Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense*. Paper presentado en VI CIIDDI 2016.

[5] Giordano Lerena, R., Di Iorio, A. H., Podestá, A., Constanzo, B. (2016, Sep). *InFo-Lab, un laboratorio mixto de investigación y desarrollo de tecnología en Informática Forense*. Paper presentado en III CADI 2016.

[6] Conclusiones del Primer Simposio Nacional sobre Análisis de Residuo de Disparo de Armas de Fuego (2012). La Plata, Buenos Aires, Argentina.

[7] Decenzo, D., Robbins, S. (2001). *Administración de Recursos Humanos*. México: Editorial Lumusa.

[8] Sotelo, Pachamé (2016). *Clase 1 - Método Científico 2016*. Material del Curso de Posgrado en Ciencias Forenses UNLP. 2° Cohorte 2016.

[9] Di Iorio A. H., Sansevero R., Castellote M., Podestá A., Greco F., Constanzo B., Waimann J. (2012) *La recuperación de la información y la informática forense: Una propuesta de proceso unificado*. Paper presentado en I Congreso Argentino de Ingeniería CADI 2012.

[10] Senado de la Provincia de Buenos Aires. Proyecto de Ley E 14 2014-2015. Disponible en: http://www.senado-ba.gov.ar/secleg_busqueda_acypro_detalle.aspx?expe=94752

[11] Norma IRAM 301 ISO/IEC 17025.

[12] Senado de la Provincia de Buenos Aires. Proyecto de Ley E 14 2014-2015. Disponible en: http://www.senado-ba.gov.ar/secleg_busqueda_acypro_detalle.aspx?expe=94752

[13] Appendino, S., Aprile, F., De Gallo, H. B. (2015, Oct). *Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense*. Paper presentado en CACIC 2015.

[14] *NISTIR 7941 - Forensic Science Laboratories: Handbook for Facility Planning, Design, Construction and Relocation*. (2013). National Institute of Standards and Technology, U.S. Department of Commerce.

[15] Di Iorio A. H. et al. (2015). *Guía Integral de Empleo de la Informática Forense en el Proceso Penal 1° edición*. Argentina, Editorial: Universidad FASTA.