

# Marco normativo para el desarrollo de pericias informáticas

Leopoldo Sebastián M. Gómez<sup>1</sup>  
gomezsebastian@yahoo.com

## Resumen

El desarrollo de pericias informáticas involucra un conjunto de conocimientos y pasos metodológicos que deben ser claramente establecidos. Se presenta un marco normativo en el que se establecen criterios y pautas de trabajo para la especialidad en cuestión. Mediante definiciones, taxonomías y metodologías de trabajo se obtiene un documento formal que proporciona un lenguaje común entre informáticos y operadores judiciales para el desarrollo de pericias informáticas y expone los criterios básicos a considerar durante la selección de recursos humanos para el desempeño de la función de Perito Informático.

Palabras Clave: análisis de datos, delitos informáticos, pericias informáticas.

### 1. La pericia informática. Definición.

La pericia informática consiste en la aplicación de técnicas de investigación y análisis a fin de determinar la existencia de evidencia legal almacenada en sistemas de computación, medios informáticos o responder consultas específicas en materia informática. El proceso finaliza con el dictamen del perito, que responde a los puntos de pericia solicitados por el juez en un determinado caso.

### 2. De la especificidad y competencia del Perito Informático.

Este es un tema de relevancia que debe ser considerado por los jueces durante la selección de un Perito Informático. Por otra parte, la ciencia informática tiene muchos campos de especialización, por lo que el perito deberá considerar minuciosamente si los puntos de pericia a resolver están dentro de su área de competencia.

Relacionado con la especificidad, hay que tener en cuenta los conocimientos y áreas que podrá abarcar un perito. Todo profesional, tiene una formación general o de base, a la que luego suma otros conocimientos específicos y la experiencia propia en el ejercicio de la profesión.

#### 2.1. De la formación en la ciencia informática.

A diferencia de otras ciencias, la experiencia en informática tiene un valor relativo, muy limitado por la evolución de los conocimientos, que hacen que metodologías, técnicas y herramientas queden obsoletas demasiado pronto.

En la ciencia informática existen diferentes niveles de conocimientos académicos, que implican perfiles con capacidades para asumir diferentes funciones dentro de la profesión. A tal fin, es importante conocer cómo se estructura la jerarquía académica en una carrera informática:

Nivel	Título	Duración
Posgrado	Doctor	4 años
Posgrado	Magister	2 a 3 años
Posgrado	Especialista	6 meses a 1 año

<sup>1</sup> Poder Judicial del Neuquen - Argentina

<b>Nivel</b>	<b>Título</b>	<b>Duración</b>
Grado	Licenciado	5 años
Grado	Ingeniero	5 años
Pregrado	Analista	2 a 3 años
Pregrado	Programador	1 a 2 años

Debe tenerse en cuenta que la preparación académica de un profesional en informática, puede variar de uno a más de nueve años de estudios. Los títulos a nivel de grado se diferencian principalmente por la orientación de la carrera. A nivel general, la mayor parte de las licenciaturas están orientadas a la formación de recursos humanos en el campo científico para promover el desarrollo de la ciencia, mientras que las ingenierías apuntan a la puesta en práctica de metodologías, técnicas y herramientas. Para acceder a los posgrados, generalmente es condición necesaria poseer un título de grado.

El nivel de pregrado –Programadores y Analistas- tiene por objeto formar profesionales con conocimientos de informática enfocados a realizar tareas puntuales en el mercado laboral: programación, análisis de sistemas, administración de sistemas operativos, bases de datos, etc. En general, en función del área donde el profesional deba desempeñarse, se requerirá el manejo de un conjunto de herramientas informáticas. La formación académica a este nivel tiene un alcance eminentemente práctico. Si bien la experiencia práctica en algún campo, puede otorgar cierto grado de autonomía en el desarrollo de sus funciones, el profesional de este nivel trabaja en equipo, bajo la dirección de un líder de proyecto, supervisor o gerente.

El nivel de grado –Licenciados e Ingenieros- profundiza en la formación teórica, a la vez que incorpora nuevas áreas de la ciencia, que permiten al futuro profesional tener un cuerpo más amplio de conocimientos en informática, para luego especializarse en algún tópico. El profesional de este nivel, está preparado para trabajar autónomamente, y a liderar grupos de trabajo.

El nivel de posgrado -Especialistas, Magisters y Doctores- tiene el objetivo de profundizar el conocimiento en un determinado campo de la ciencia, a fin de formar especialistas o investigadores. Las capacidades que se adquieren en este nivel son útiles en las siguientes áreas de competencia: dirigir proyectos de investigación, liderar equipos de desarrollo o gerenciar departamentos de informática.

En informática, la formación académica es un indicador de calidad del recurso humano, y determina las competencias de un profesional. A medida que se asciende en esta jerarquía, se incorporan principalmente nuevos conocimientos teóricos, metodologías y técnicas. Es por ello que debe tenerse en cuenta que este nivel será indicativo del grado de conocimientos profundos en la ciencia, y no de habilidades con herramientas informáticas. Los niveles superiores, establecen un perfil de profesional calificado en la aplicación de metodologías y técnicas informáticas, principalmente para el desarrollo de sistemas. Sin embargo, se requiere contar con personal auxiliar técnico para realizar tareas operativas que involucren el manejo de herramientas informáticas.

A partir de la formación académica puede establecerse un perfil profesional, definido no sólo por los conocimientos adquiridos, sino por motivaciones y expectativas de carrera. Es por ello, que al momento de establecer un plan de carrera, un llamado a concurso o el tipo de funciones que deba cumplir un profesional informático, uno de los aspectos más relevantes a considerar es la jerarquía académica.

De acuerdo con lo detallado, un parámetro relevante para determinar la calidad del recurso humano que realice funciones de perito informático, es la formación académica.

## 2.2. De las funciones del profesional informático.

Un aspecto a considerar para determinar la especialidad del perito son las funciones que haya desempeñado, principalmente en el último período de su carrera profesional. En el campo laboral de la informática, existen diversas funciones, de acuerdo al área de conocimiento involucrada. A lo largo una carrera profesional, el informático suele trabajar en diferentes áreas y al pasar de una a otra, los conocimientos prácticos dejan de ser de utilidad, quedando evidenciada la relevancia de la formación en la ciencia por sobre la función desarrollada.

Se detallan a continuación, las principales funciones que ejercen los profesionales informáticos:

<b>Area</b>	<b>Función</b>
Sistemas Operativos	Administrador de Sistemas
Bases de Datos	Administrador de Bases de Datos
Redes de Datos	Administrador de Red
Desarrollo	Analista Funcional Analista Programador Programador Testeador Documentador
Dirección	Director de Proyecto
Auditoría	Auditor Informático
Soporte Técnico	Helpdesk

Esta taxonomía no es exhaustiva, pero identifica las principales funciones del personal informático. En virtud de lo anteriormente expuesto, la especialidad del perito puede determinarse por las funciones informáticas que haya ejercido en el último período de su carrera profesional.

## 2.3. De la experiencia en un área informática.

En algunas áreas, de acuerdo con la experiencia obtenida, un profesional puede ser calificado como Junior, Semisenior o Senior. El profesional informático sólo podrá acumular experiencia práctica en determinadas herramientas, en función del área dónde se desempeñe. Puede tenerse en cuenta la experiencia como factor valorativo de un profesional, sin embargo, en general este criterio sólo tiene interés durante la búsqueda específica de un profesional informático con habilidades prácticas en determinadas herramientas.

Es imprescindible aclarar que los conocimientos adquiridos en el manejo de herramientas, son los más volátiles y susceptibles a quedar fuera de uso en poco tiempo. Por todo ello, no es posible mantener destreza en el uso de herramientas (aplicaciones, lenguajes, sistemas operativos, bases de datos, etc.) si no se hace un uso frecuente de los mismos. El conocimiento práctico de una herramienta no utilizada se convierte en conocimiento general acerca de características y posibilidades de explotación de la misma, pero se requerirá de un especialista en la herramienta para poder generar resultados concretos.

Si un profesional informático realiza funciones en diversas áreas, a lo largo de su carrera profesional, podrá adquirir una visión general que le permitirá a futuro ejercer funciones de dirección. En este caso, la experiencia tiene relevancia, pero no se refleja en las habilidades en el manejo de herramientas informáticas. El profesional informático que realice este plan de carrera, se convierte en Senior, reflejando su experiencia a través de sus habilidades para la conducción y interacción con el personal de cualquier área informática.

Lo expuesto precedentemente, la experiencia del perito puede ser calificada bajo estos dos enfoques: experiencia práctica, en el manejo de algunas herramientas informáticas o experiencia de dirección, mediante el dominio de metodologías y técnicas y manejo de relaciones humanas. Ninguno de estos tipos de experiencia es más relevante que el otro, pero determinan perfiles de profesionales diferentes.

En el caso de los peritos informáticos, la experiencia de dirección es la que le permite interactuar con profesionales informáticos de diferentes ámbitos, poder pautar cuáles serán los pasos a seguir para el desarrollo eficaz de una pericia y utilizar algunas herramientas informáticas para el trabajo pericial. Un perito informático con experiencia práctica, trabajará con eficiencia los casos en los que se utilicen las herramientas informáticas de su especialidad, pero no podrá actuar en otros.

#### 2.4. De los aspectos técnicos: hardware, software, comunicaciones.

La formación académica del profesional informático lo habilita a trabajar principalmente en cuestiones relacionadas con el software, es decir, la parte lógica de los sistemas informáticos. Si bien es importante el manejo del hardware y de dispositivos de comunicaciones, la destreza en la utilización de estos elementos no es una condición necesaria para el profesional. A tal fin, existen carreras terciarias o simplemente técnicas que capacitan en la instalación, configuración o mantenimiento de estos elementos. Es por ello que en el desarrollo de pericias informáticas, el perito debe contar con personal auxiliar técnico a fin de poder resolver temas relacionados con hardware o comunicaciones, así como otras tareas rutinarias (impresión, copia de datos, rotulado de material, etc.).

### 3. Metodología para el análisis de datos

El proceso para realizar una investigación, con el objeto de determinar si existe evidencia en medios informáticos, consta de cuatro pasos claramente definidos:

1. Identificar los elementos a periciar
2. Preservar los datos
3. Analizar los datos
4. Emitir un dictamen

En primer lugar, se deben identificar los sistemas de computación o medios de almacenamiento que puedan contener información digital que sea factible de ser presentada como evidencia. Debe informarse a los operadores judiciales de todos los aspectos claves a considerar para la preservación de la evidencia, como los recaudos en el transporte y/o almacenamiento de elementos informáticos y la prohibición de realizar operaciones sobre los sistemas informáticos, previas a la actuación del Perito Informático [Gom99a].

Una vez realizado el primer paso, se requiere analizar la posibilidad de preservar los datos mediante una copia para un posterior análisis. Este paso queda a criterio del perito informático, en función de las limitaciones que puedan existir [Gom99b]. Posteriormente, se debe proceder a realizar una investigación sobre los datos, a fin de localizar la información que sea relevante a la causa. Finalmente, el perito informático emitirá un dictamen, respondiendo a los puntos de pericia que le sean solicitados.

Debe tenerse en cuenta que este proceso, es exclusivo para pericias informáticas que involucren análisis de datos. Sin embargo, el perito informático podrá responder acerca de otras cuestiones en función de su especialidad.

#### 3.1. De los puntos de pericia.

Los puntos de pericias pueden dividirse en análisis de datos y consultas específicas. A modo de ejemplo, se sugiere una posible lista de actividades que estarían comprendidas de la primer categoría:

<b>Código</b>	<b>Tipo</b>	<b>Descripción</b>
AD001	Análisis de datos	Localización de archivos mediante palabras claves especificadas por el juez.
AD002	Análisis de datos	Localización de archivos mediante palabras claves extraídas de documentos.
AD003	Análisis de datos	Localización de imágenes especificadas por el juez.
AD004	Análisis de datos	Localización de imágenes extraídas de documentos.
AD005	Análisis cronológico de datos	Identificación de fechas de creación, acceso o modificación de archivos y documentos.
AD006	Análisis cronológico de datos	Identificación de fechas de creación, recepción o envío de e-mails.
AD007	Análisis cronológico de datos	Identificación de entradas y salidas de usuario sobre un sistema informático.
AD008	Análisis cronológico de datos	Identificación de accesos a páginas o sitios web.

De acuerdo a la especialidad del profesional, el perito informático podrá determinar, especificar o responder otros puntos de pericia específicos, como:

<b>Código</b>	<b>Tipo</b>	<b>Descripción</b>
CE001	Consulta específica	Especificar el tipo de equipamiento que se necesita para ejecutar un sistema informático.
CE002	Consulta específica	Especificar los tipos de dispositivos de almacenamiento utilizados por un sistema informático.
CE003	Consulta específica	Especificar la capacidad de un dispositivo de almacenamiento.
CE004	Consulta específica	Determinar similitudes y/o diferencias en los listados del código fuente de dos sistemas informáticos.
CE005	Consulta específica	Especificar qué módulos comprenden un sistema informático.
CE006	Consulta específica	Determinar si una sistema informático trabaja por lotes (batch) o en forma interactiva.
CE007	Consulta específica	Determinar cuándo dos sistemas son similares en base a la estructura de datos utilizada para el almacenamiento de información.
CE008	Consulta específica	Responder preguntas generales sobre la ejecución de un sistema informático.

### 3.2. De los allanamientos y procedimientos varios.

Durante los allanamientos y otros procedimientos para la identificación y recolección de evidencia informática, se deben tener en cuenta las siguientes limitaciones [Caf01]:

- Disponibilidad de equipos: debido a la variedad de marcas y modelos a veces se dificulta la investigación; dado que es imposible contar con todas las versiones o

elementos necesarios para la pericia. De la misma forma, no siempre es posible clonar (hacer una copia imagen) del sistema a periciar para un posterior análisis de datos por cuestiones de recursos, tiempo y lugar.

- Equipos compatibles: ídem anterior. En muchos casos, no se podrá prescindir del equipo sobre el cual se ejecuta el software. Si el sistema no puede ser clonado y ejecutado en otra plataforma, deberá evaluarse la posibilidad realizar la pericia sobre el sistema original, reduciéndose el alcance de la misma.
- Equipos antiguos: en la mayoría de los casos el tiempo que transcurre entre el allanamiento y el desarrollo pericial es extremadamente extenso. En estos casos; si no se logra reconstruir un equipo de similares características y/o prestaciones; no se puede realizar ningún tipo de investigación.
- Desconocimiento de las claves de seguridad: habrá que hacer uso de los servicios de algún hacker. El acceso y descifrado de archivos encriptados es virtualmente imposible con las herramientas que se utilizan en la actualidad, ya que en su mayor parte, utilizan mecanismos de fuerza bruta para el descifrado, cuyo tiempo de procesamiento llega a ser prohibitivo.
- Desconocimiento de aspectos técnicos específicos de hardware, software o comunicaciones. En virtud de lo explicado sobre el tema y el área de competencia del perito, pueden existir limitaciones en las habilidades prácticas sobre algunos elementos o herramientas específicas. En estos casos, se requerirá de personal técnico auxiliar para llevar a cabo la investigación.

### 3.3. De los procedimientos para el resguardo y el análisis de los datos.

Existen dificultades durante el desarrollo de las investigaciones, referidas al resguardo y análisis de datos.

Respecto al resguardo de datos:

- Los dispositivos son lentos.
- No siempre es importante realizar esta operación.
- No siempre es posible realizar la operación por cuestiones de recursos, tiempo o lugar.
- Requiere amplios conocimientos técnicos en el manejo de herramientas.
- No siempre se puede realizar sobre un único medio de almacenamiento.

Respecto al análisis de los datos:

- Se requieren herramientas específicas para la extracción de evidencia de archivos borrados, o espacios de disco reutilizables o áreas de memoria virtual, así como también para la visualización de la información a peritar.
- La búsqueda de datos es muy rudimentaria y consume mucho tiempo. No existen taxonomías de palabras estándares, formatos u organizaciones de datos que puedan ser aplicadas a la investigación de delitos específicos.
- No hay una forma automática de identificar a la información relevante, sin necesidad de leer los archivos. Las herramientas informáticas, sólo permiten acotar el espacio de búsqueda, sin embargo, dada la gran cantidad de información que puede almacenarse en un sistema informático, es prohibitivo realizar una investigación exhaustiva sobre todos los archivos localizados. En algunos casos, se deberá realizar un análisis de datos sobre un subconjunto de ellos.
- No existe una técnica informática para identificar a los posibles autores de la información localizada, en base a su vocabulario, gramática o estilo de escritura.

- Existen algunas herramientas informáticas que permiten descifrar datos, pero se basan en prueba y error, con lo cual, los tiempos de procesamiento son prohibitivos.
- No hay disponibles herramientas informáticas que correlacionen la información almacenada en los sistemas informáticos analizados. En algunos casos, se deben desarrollar bases de datos específicas para el procesamiento de la información.

#### 4. Capacitación para el Perito Informático

Existen ciertas capacidades que debe adquirir un perito informático para realizar un análisis de datos sobre medios informáticos. Para ello se requiere una capacitación específica en el uso de técnicas y herramientas informáticas utilizadas para pericias informáticas.

En el país no existen cursos de relevancia en materia de pericias informáticas, sin embargo, algunos de las organizaciones o centros de capacitación en el exterior brindan programas de entrenamiento o cursos de especialización en este campo.

a) Organizaciones que proveen certificaciones de especialización en pericias informáticas:

- The International Association of Computer Investigative Specialists (IACIS)
- High-Tech Crime Network (HTCN)

b) Empresas que proveen entrenamiento para pericias informáticas con alguna herramienta informática específica:

- Key Computes Services Inc.
- New Technologies Inc.
- CyberEvidence Inc.
- Guidance Software Inc.
- AccessData Corp.

A partir de la capacitación específica, y de acuerdo a las características de las herramientas que se utilicen, se puede aplicar el estándar definido para los puntos de pericias informáticas y establecer otros más específicos.

#### 5. Conclusiones

El desarrollo de pericias informáticas que requiere contar con un marco normativo que permita a todos los operadores judiciales conocer las necesidades en materia de recursos humanos para poder brindar apoyo eficiente a la justicia, así como también el objetivo, alcance y limitaciones de las pericias informáticas. A través de un marco normativo se pueden formalizar los principales tópicos del desarrollo de pericias informáticas.

Dependiendo el área de especialización del Perito Informático, el juez podrá requerir pericias informáticas de diferentes grados de complejidad, desde análisis de datos hasta consultas específicas en materia de contratos informáticos.

#### 6. Referencias

- [Caf01] Caffaro, M.A., *“Argentina: Pericias Informáticas”*, R.E.D.I., Revista Electrónica de Derecho Informático N° 32, ISSN: 1576-7124, 2001.
- [Gom99a] Gómez, L.S.M., *“Actuaciones en Delitos Informáticos”*, Reporte Técnico, Tribunal Superior de Justicia, Poder Judicial del Neuquén, 1999.
- [Gom99b] Gómez, L.S.M., *“MD5 para la Certificación de Copias”*, Cuaderno de Reportes Técnicos Nro. 7 de la Escuela de Posgrado del Instituto Tecnológico de Buenos Aires, 1999.