Importancia del método de la prueba pericial en materias de tecnología y su impacto en la agilidad del proceso judicial

Antonio Luis Flores Galea

Revista Digital de ACTA

2019

Publicación patrocinada por

CEDRO

Importancia del método de la prueba pericial en materias de tecnología y su impacto en la agilidad del proceso judicial

INTRODUCCIÓN

La tecnología abarca cada día más ámbitos de la vida personal y empresarial. Inmersos en un mundo cada vez más digitalizado, los conflictos surgidos de las propias relaciones humanas no son una excepción. De esta manera, cada día se producen más reclamaciones y demandas judiciales donde la tecnología es el centro o, al menos, está presente.

En este artículo se analizará la prueba pericial como la clave principal para contribuir a dirimir disputas y reclamaciones entre dos partes. Se expondrán buenas prácticas para elaborar dictámenes periciales y cómo contar con el mejor profesional puede, en numerosas ocasiones, facilitar un acuerdo prejudicial o incluso encauzar correctamente una demanda o reclamación.

La prueba pericial es un documento esencial durante cualquier proceso judicial donde sea requerida, y la calidad de la misma, medida en los parámetros que se analizan en este artículo, puede impactar enormemente tanto en el resultado final como en el tiempo -y coste- invertido para resolver la disputa.

ORIGEN Y JUSTIFICACIÓN DE LA PRUEBA PERICIAL

La prueba pericial consiste en un dictamen emitido por un profesional con competencias técnicas en la materia del caso relacionado con una demanda judicial, cuyo fin es ayudar al juez a tomar una decisión. El Art. 335 de la Ley de Enjuiciamiento Civil (**LEC**, en adelante), indica que "*cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal*".

La prueba pericial es un medio de prueba especial, ya que se le exigen tres particularidades:

- no puede aportar hechos al proceso, sino utilizar exclusivamente los que ya existen;
- debe apoyarse en hechos de influencia notoria;
- los hechos deben precisar de conocimientos técnicos.

Si no se cumplen estas tres premisas, no procede solicitar una prueba pericial. Sin embargo, como resultado de lo anterior, pueden solicitarse pruebas periciales en todos los ámbitos jurisdiccionales:

- **Civil**: normalmente relacionadas con el incumplimiento de contratos y reclamaciones de responsabilidades extracontractuales.
- **Contencioso-administrativo**: recursos contra decisiones de las administraciones Central del Estado, autonómicas o locales (ayuntamientos y diputaciones provinciales).
- **Penal**: por ejemplo, en el ámbito tecnológico: estafas por Internet, delitos informáticos, escuchas ilegales, etc.
- **Laboral**: relacionadas con demandas entre trabajadores y empresa, donde caben reclamaciones por el uso indebido de correos electrónicos y bases de datos, en relación con la tecnología.
- **Mercantil**: principalmente relacionadas con problemas sobre la propiedad industrial y patentes.

La función pericial supone la asunción por parte del perito de una gran responsabilidad, pues suele ser un medio de prueba especialmente valorado por los jueces y magistrados a la hora de dictar sentencia en los procedimientos de gran complejidad técnica.

Es importante señalar que la prueba pericial debe contener la respuesta a las preguntas planteadas por quien la solicita (una de las partes demandantes o el propio juez, tras habérselo solicitado una o las dos partes) y que, en función de ellas, presentará un alcance distinto, distinguiéndose entre "informe pericial" y "dictamen pericial", según se muestra en la Fig. 1. Como se puede ver, el dictamen pericial incluye todo el contenido de un informe pericial y más contenido.

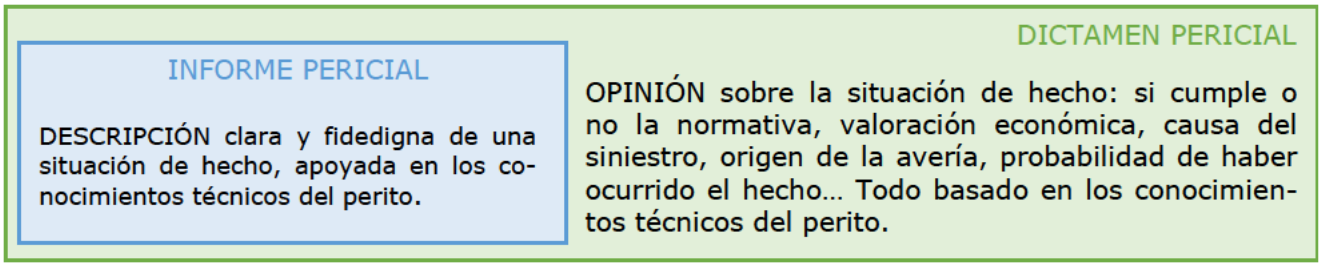

Fig. 1. Alcance del informe y el dictamen pericial

Cuando la prueba pericial es solicitada por el juez (por designación judicial), consiste en preguntas muy concretas que las partes formulan. El juez designa al perito, normalmente basándose en el listado facilitado por el colegio profesional competente. El perito será citado y comenzará el proceso reflejado en la Fig. 2.

Fig. 2. Proceso de elaboración de la prueba pericial solicitada por designación judicial

Cuando la prueba pericial es solicitada por una de las partes, el proceso se simplifica, tal como se muestra en la Fig. 3.

Fig. 3. Proceso de elaboración de la prueba pericial a instancia de parte

En todos los casos, "*las partes deben manifestar si desean que el perito …/… comparezca en el juicio …/… o, en su caso, en la vista oral, expresando si deberán exponer o explicar el dictamen o responder a preguntas, objeciones o propuestas de rectificación, o intervenir de cualquier otra forma útil para entender y valorar el dictamen en relación con lo que sea objeto del pleito*" (Art. 337 de la LEC). Si el informe se ha realizado sobre las alegaciones presentadas por el demandado

o por este, en respuesta a la demanda, estas exigencias también podría solicitarlas el propio juez al perito (Art. 338 de la LEC).

LA PRUEBA PERICIAL EN EL ÁMBITO EXTRA-JUDICIAL

Existen situaciones donde es posible solicitar una prueba pericial fuera de un proceso judicial. Esto suele ocurrir cuando se trata de cuestiones de alta complejidad técnica, donde se hace necesario un experto independiente, para tomar una decisión relevante para una empresa o negocio, aunque en numerosas ocasiones esta petición está relacionada con procesos de **arbitraje y mediación**.

En Derecho, el **arbitraje** es una forma de resolver un litigio sin acudir a la jurisdicción ordinaria. Las partes, de mutuo acuerdo, deciden nombrar a un tercero independiente, denominado árbitro, o a un tribunal arbitral, que será el encargado de resolver el conflicto. El árbitro, a su vez, se verá limitado por lo pactado entre las partes para dictar el laudo arbitral. Deberá hacerlo conforme a la legislación que hayan elegido las partes, o incluso basándose únicamente en el principio de equidad, si así se ha pactado. En cuestiones de índole tecnológica, es frecuente acudir a un perito para que actúe de árbitro y emita su dictamen desde el punto de vista experto.

El arbitraje exige que ambas partes lleguen al acuerdo de someterse a él voluntariamente, lo que se justifica con frecuencia por el interés de evitar los plazos y costes económicos de un procedimiento judicial ordinario.

La **mediación** es un proceso voluntario en el que dos o más partes involucradas en un conflicto trabajan con un profesional imparcial, el mediador, para generar sus propias soluciones para resolver sus diferencias. A diferencia de un proceso judicial o arbitral, donde la sentencia del juez o decisión del árbitro dan la razón a una de las partes y obligan a indemnizar a la otra, la mediación busca llegar a un acuerdo entre las partes y obtener una solución válida para ambas.

En ambas soluciones -arbitraje y mediación-, la prueba pericial consituye el arma más poderosa para el convencimiento de las partes, siempre que ésta se haya ejecutado de manera profesional y quede perfectamente explicada y detallada en el dictamen. Es, por tanto, esencial que el perito recabe toda la información disponible y aplique métodos generalmente aceptados e irrefutables, como ocurre en la prueba dentro de un proceso judicial, pero en este caso es sumamente importante conservar la imparcialidad y mantener cierta distancia con las partes, al no haber ninguna autoridad oficial que proteja su independencia.

Es altamente probable que una o ambas partes intentes influir para modificar el dictamen pericial, incluso después de haber sido este entregado. Por este motivo, es esencial determinar el procedimiento de elaboración, mecanismos de interacción e interlocución, plazos para la ejecución y presentación de los trabajos y el dictamen, respectivamente, al no existir una autoridad formal que los determine.

LA PRUEBA PECICIAL EN MATERIAS TECNOLÓGICAS

La tecnología está cobrando mayor relevancia cada día. Consecuentemente, cada día son más los procedimientos judiciales donde está involucrada alguna faceta tecnológica. Así, teniendo en cuenta que puede ser objeto de una prueba pericial toda actividad que pueda ser objeto de una demanda, en el ámbito tecnológico, podemos encontrar, por citar algunas:

- problemas relacionados con la calidad de servicios, equipos o instalaciones;
- averías y siniestros que hayan provocado daños o perjuicios;
- radiaciones electromagnéticas que puedan ser consideradas nocivas para la salud o para el correcto funcionamiento de maquinaria u otros sistemas;
- infracciones de uso o explotación de la propiedad intelectual o industrial (Ej. patentes);
- incumplimiento de las leyes de protección de datos o del derecho a la intimidad;
- identificar interlocutores en una grabación de audio o telefónica;
- recursos contra decisiones de las administraciones públicas;
- delitos en Internet;
- validación o invalidación de pruebas basadas en correos electrónicos, redes sociales o grupos cerrados de usuarios (Ej. Whatsapp);
- daños producidos por o a infraestructuras de telecomunicaciones, ya sea en viviendas, locales, oficinas, centros comerciales o en la vía pública;
- reclamaciones sobre el lucro cesante de proveedores de servicios de telecomunicaciones (Ej. operadores) o de Internet (Ej. ISPs);
- alcance y datos producidos por interferencias en servicios inalámbricos;
- ciber-ataques o ataques físicos contra equipos informáticos o de telecomunicaciones;
- incumplimiento de las leyes sobre comercio electrónico;
- siniestros en instalaciones eléctricas de baja y media tensión;
- accidentes producidos por maquinaria u otros elementos;
- defectos de calidad en la producción, duplicación o edición de materiales audiovisuales o páginas web;
- defectos en la calidad del software desarrollado para aplicaciones, servicios web o aplicaciones móviles (Apps);
- disputas sobre el derecho de explotación de productos audiovisuales;
- daños o perjuicios ocasionados en el ámbito de la electromedicina y telemedicina;
- Problemas en el ámbito de la seguridad y riesgos laborales derivados del uso de la tecnología;
- incumplimiento de la normativa y sus consecuencias en los sistemas contra incendios;
- daños relacionados con deficiencias o negligencia en la utilización de alarmas y sistemas de seguridad.

En este punto es importante señalar que las distintas ramas de la ingeniería establecen distintas naturalezas de perito, incluso dentro de una misma materia como son las TIC (Tecnologías de la Información y las Comunicaciones), a saber:

- **Peritos informáticos** → Dictámenes relacionados con software y hardware, incluyendo las redes de datos e Internet, aunque siempre desde un punto de vista lógico (software y aplicaciones).
- **Peritos de telecomunicación** → Dictámenes relacionados con sistemas audiovisuales y de telecomunicaciones (telefonía, radio, TV, Internet), cubriendo tanto las cuestiones relacionadas con el equipamiento como con el software asociado. En el caso de Internet, los peritos de telecomunicación están además cualificados para analizar el tráfico de redes al más bajo nivel, así como los equipos electrónicos de red (switches, routers, centrales de conmutación, instalaciones de fibra, etc.). El perito de telecomunicación también tiene competencias en cuestiones relacionadas con la acústica (emisiones, ruidos, etc.).
- **Peritos en electrónica** → Dictámenes relacionados con equipos electrónicos en general, ya sean de consumo o utilizados en infraestructuras empresariales o de operador. Estos equipos electrónicos pueden requerir -cada día más- de un software o firmware para funcionar, cuyo análisis también puede caer bajo las competencias del perito electrónico, aunque no caen bajo esta rama las aplicaciones de usuario.

Como se aprecia, existen campos en los que las distintas ramas de la ingeniería se solapan. Aunque la tendencia natural de alguien más o menos profano en estos campos suele ser asociar tecnología con informática, es importante señalar que, bajo mi punto de vista personal, el mayor abanico de competencias, en nuestro actual entorno hiper-conectado, la tienen los ingenieros de telecomunicación. No obstante, es importante determinar la principal naturaleza de la cuestión sobre la que se plantea la prueba pericial para acudir al profesional más cualificado sobre la misma, incluso con independencia de la titulación que posea.

Adicionalmente, la mayoría de demandas judiciales donde está involucrada la tecnología proceden de las jurisdicciones civil y contencioso-administrativa, por la propia naturaleza de las mismas.

Todos los informes periciales deben estar visados por el colegio profesional correspondiente. Un informe no visado puede dar lugar a problemas durante el procedimiento judicial o con posterioridad al mismo (por ejemplo, en el caso de desear impugnar los honorarios, el Juzgado solicita informe al Colegio, y éste solo lo emitirá sobre documentos visados por ese mismo Colegio). El visado de un informe pericial es un acto de control para comprobar y acreditar, en su caso, la adecuación de un trabajo a las disposiciones generales y corporativas que lo regulan, además de ser un requisito para cubrir la responsabilidad civil del ingeniero firmante, si fuera necesario, por la póliza colectiva de seguro del Colegio. Por lo tanto, es muy importante que los informes periciales vayan siempre visados por el Colegio Profesional competente en la materia, para garantizar que cualquier reclamación posterior no supondrá un problema añadido al procedimiento judicial para el que se ha solicitado.

El Colegio de Ingenieros de Telecomunicación (COIT, www.coit.es) establece un conjunto determinado de áreas de habilidades, tal como se muestra a continuación:

- Redes de telecomunicaciones
- Derechos digitales (patentes, propiedad industrial e intelectual)
- Sistemas audiovisuales – Medidas acústicas y verificación de voz e imagen
- Sistemas informáticos y telemáticos
- Procesos de diseño y fabricación de equipos de telecomunicaciones
- Estaciones de radiocomunicaciones (televisión, radio, telefonía móvil, WIFI)
- Medidas y comprobación de niveles de emisiones radioeléctricas
- Telecomunicaciones en la edificación

LA EVIDENCIA EN EL DICTAMEN PERICIAL

En materias tecnológicas, el perito tiene una especial relevancia en la recolección de evidencias o pruebas, para la elaboración del dictamen. Al ser la tecnología un campo con dos características que complican el proceso judicial, como son la intangibilidad de muchas pruebas (software, información) y la volatilidad de las mismas (pueden ser destruidas muy fácilmente de manera accidental), es muy importante que el perito cuente con los conocimientos y medios adecuados para garantizar todo el proceso de recopilación, tratamiento, almacenamiento y preservación de las pruebas o evidencias necesarias para la elaboración del dictamen.

Las evidencias se pueden clasificar en:

- **Físicas**: se corresponden con activos tangibles o materiales, como son los componentes informáticos (discos duros, pendrives, tabletas, smartphones), de red (routers, switches, torres, antenas) o de cualquier otra índole (satélites, instalaciones, cableado).
- **Digitales**: consisten en información o programas (software) almacenados en dispositivos electrónicos o que discurren a través de las redes (Internet, redes privadas) o los sistemas (buses de datos).

Las evidencias deben cumplir los siguientes criterios:

- **Autenticidad**: se debe poder demostrar que no han sufrido ninguna alteración. En el caso de evidencias digitales, habitualmente se utiliza la obtención de *hashes* para asegurar su integridad. Esta técnica consiste en aplicar un algoritmo sobre la información en cuestión unida con una firma digital con sello de tiempo de una autoridad reconocida (por ejemplo la Fábrica Nacional de Moneda y Timbre, FNMT), cuyo resultado es una clave o *hash*. Si se alterara un solo dígito de la información, el *hash* obtenido sería distinto. Igualmente, si se aplica el mismo algoritmo sobre la información original, siempre se obtiene el mismo *hash*.
- **Credibilidad**: deben ser comprensibles y asimilables para la razón.
- **Completitud**: desde el punto de vista objetivo y técnico, la evidencia debe representar una prueba en sí.
- **Confianza**: las técnicas para su obtención no pueden generar dudas sobre su autenticidad y veracidad.
- **Admisibilidad**: deben ser admitidas desde el punto de vista legal. Por ejemplo, las grabaciones sin consentimiento del grabado no son admisibles, en general.

EL PERITO JUDICIAL EN MATERIAS TECNOLÓGICAS

La capacidad para ejercer como perito judicial está recogida en el ordenamiento jurídico de manera muy clara y explícita. El Art. 341.1 de la Ley 1/2000 de Enjuiciamiento Civil estipula que "*en el mes de enero de cada año, se interesará de los distintos Colegios Profesionales …/… el envío de una lista de colegiados o asociados dispuestos a actuar como peritos*".

Adicionalmente, los colegios profesionales disponen de un servicio que ofrece a Juzgados y Tribunales, profesionales del Derecho, empresas y, en general, cualquier interesado, la posibilidad de solicitar el listado de peritos para un ámbito geográfico y área de especialidad determinados.

Los colegios profesionales asumen la responsabilidad de garantizar que los profesionales propuestos cumplen con los mínimos requisitos para desempeñar los trabajos. Sin embargo, estos mínimos son estimados de manera general para el colectivo (por ejemplo, exigiendo haber realizado una formación específica, además de la titulación oportuna).

En el caso del Colegio Oficial de Ingenieros de Telecomunicacion (www.coit.es), sus estatutos recogen como fines y funciones del COIT "cooperar con los Organismos Oficiales correspondientes en la forma que proceda en la designación de los Ingenieros de Telecomunicación para la emisión de informes, dictámenes, tasaciones, valoraciones, etc, en intervenciones profesionales de asuntos judiciales, tanto civiles como criminales (Art. 4 del R.D. 261/2002, de 8 de marzo).

El COIT solicita cada año a todos los colegiados que indiquen si desean estar incluidos en el listado de peritos judiciales, seleccionando las provincias de actuación y las áreas de conocimiento

dentro de la rama de Telecomunicaciones. Una vez concluido el plazo, el COIT elabora una lista para cada provincia, donde aparecerá en primer lugar los colegiados residentes en la provincia, por número de colegiado de menor a mayor (siendo los de menor número los que más tiempo llevan colegiados). Tras estos, se listan los que residan en otras provincias, ordenados por el mismo criterio de antigüedad. No obstante, el Art. 341 de la LEC establece que "*la primera designación de cada lista se efectuará por sorteo realizado en presencia del Letrado de la Administración de Justicia y, a partir de ella, se efectuarán las siguientes designaciones por orden correlativo*".

REQUISITOS Y LIMITACIONES DEL PERITO JUDICIAL

La ley contempla limitaciones al ejercicio de perito judicial, ya sea en forma de tachas, que se encuentran recogidas en la LEC, como en exigencias que deben cumplir quienes acepten el cargo de perito en un procedimiento judicial. Así, por ejemplo, "*al emitir un dictamen, todo perito deberá manifestar, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito*" (Art. 335 de la LEC).

La LEC establece además que, "*salvo acuerdo en contrario de las partes, no se podrá solicitar dictamen a un perito que hubiera intervenido en una mediación o arbitraje relacionados con el mismo asunto*".

EL PERFIL IDEAL DE PERITO JUDICIAL EN MATERIAS TECNOLÓGICAS

Fig. 4. Placa oficial de perito judicial reconocida en España

Aunque ya se han citado los requisitos legales para que un profesional pueda ejercer como perito judicial en cuestiones tecnológicas, si se persigue la excelencia en la elaboración y defensa de dictámenes periciales, se hace necesario considerar otros aspectos adicionales, exigibles al perito.

A continuación se enumeran los principales aspectos que debería cubrir un perito judicial, bajo el punto de vista del autor, con el objeto de conseguir un dictamen eficaz y una ulterior defensa durante la vista oral, siempre con el objetivo de reducir al máximo la duración del proceso y su coste económico:

- Aunque la Ley da la opción, en algunas circunstancias, a elegir entre ingenieros con o sin grado, en España la diferencia en los honorarios normalmente no justifica la elección de los primeros. Así, es preferible optar por un master en ingeniería o ingeniero superior, ya que contará con una formación más completa.
- En la inmensa mayoría de ocasiones, los peritos cuentan con muy buenos conocimientos técnicos, pero con poca visión de la dinámica de un proceso judicial, de las relaciones empresariales y de suficiente "altura de miras" para entender la esencia del conflicto, qué puede esperarse de cada parte y qué perfiles profesionales van a estar presentes durante el juicio. Así, es posible que se elabore un excelente trabajo de investigación y análisis,

pero cuyo resultado no sea comunicado de la manera más eficaz y convincente. Se recomienda que el perito disponga, además de sus conocimientos técnicos en la materia en cuestión, de alguna **experiencia en consultoría estratégica** (muchas empresas denominan "consultoría" simplemente a la ejecución de proyectos), en **actos públicos** (conferencias, defensas) y, mejor aún, disponer de **formación específica en dirección y gestión de empresas** (un Máster MBA o similar).

- Sobre los estándares de calidad, es de resaltar que el trabajo de perito se apoya, en una proporción muy alta, en la integridad, honestidad y profesionalidad. En este sentido, no solo es importante que el perito lo declare por escrito en su informe, sino también que cuente con un **historial profesional intachable**, que aplique **rigurosidad durante todo el proceso** (puntualidad, seriedad, calidad estética del trabajo) e, incluso, una **apariencia física** cuidada y adecuada a la ocasión. Al igual que un acusado suele asearse, vestirse formalmente y cuidad su lenguaje durante una vista oral, el perito debe cuidar aún más estas cuestiones, pues se le va a suponer la máxima autoridad en materias técnicas durante el juicio. La mejor forma de garantizar este aspecto es evaluar estos aspectos en el perito desde el primer momento y no simplemente confiar en que va a aparecer con traje y corbata el día de la vista oral.
- Por último, aunque parezca fuera de lugar, es muy importante no conformarse solamente con la habilitación técnica que realizan los colegios profesionales o equivalentes para valorar las capacidades técnicas del perito. Como en todos los aspectos de la vida, existen mejores y peores profesionales en todas las profesiones, y encontrar a los mejores profesionales en una materia no es tarea sencilla. Por eso, es muy recomendable contar con profesionales que **demuestren el conocimiento** en la materia y tengan la capacidad real de **avalarlo**. Es cierto que este aspecto es difícil de evaluar por una persona sin conocimientos técnicos en la materia, pero siempre se puede recurrir al tradicional *curriculum vitae* o a referencias de compañeros de profesión para tener una aproximación de la solvencia técnica del profesional en cuestión.

IMPORTANCIA DEL MÉTODO EN LA PRUEBA PERICIAL

ESTRUCTURA Y CONTENIDOS DEL DICTAMEN PERICIAL

La estructura general y los contenidos mínimos de un informe o dictamen pericial en materias tecnológicas se encuentran recogidos principalmente en dos normas UNE:

- **UNE 197001:2011** "Criterios generales para la elaboración de informes y dictámenes periciales" – orientada a los informes periciales en general.
- **UNE 197010:2015** "Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones" – específica para informes periciales en materias tecnológicas.

Para definir el cuerpo del informe o dictamen pericial se recomienda utilizar la norma UNE 50132, donde se enumeran los puntos que componen el cuerpo del informe. En los siguientes apartados se detallan las recomendaciones principales de cada una de estas normas.

Norma UNE 197001:2011 - Criterios generales para la elaboración de informes y dictámenes periciales

http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0046980

Esta norma, publicada en 2011, tiene por objeto el establecimiento de los requisitos formales que deben tener los informes y dictámenes periciales, con objeto de hacerlos lo más homogéneos posible, para facilitar su lectura y la comprensión de los análisis y estudios técnicos realizados por el perito.

La norma establece que debe hacerse constar la siguiente información de **identificación** del dictamen, en la primera página del mismo:

- Título del informe y su código o referencia de identificación.
- Nombre del organismo al que se dirige el informe pericial y, en su caso, número de expediente o procedimiento.
- Nombre y apellidos del perito, titulación o destreza específica y, en su caso, colegio o entidad a la que pertenece, DNI, domicilio profesional, teléfono, fax, correo electrónico y cualquier otro dato profesional que pudiera existir, salvo que no sea legalmente procedente.
- Nombre, apellidos y DNI del solicitante del informe pericial, si es en nombre propio o en representación de tercero, con sus datos, y cualquier otro identificador legalmente procedente.
- Si procede, dirección y población del emplazamiento geográfico concreto así como, en su caso, coordenadas UTM.
- Nombre y apellidos del letrado y del procurador del solicitante, si procede.
- Lugar y fecha de emisión del informe o dictamen pericial.

En cuanto a la **estructura**, la norma indica que esta debe estar compuesta, aparte de la identificación, por un índice, cuerpo del informe y, cuando corresponda, documentos anexos. Así mismo, en cada página del dictamen debe figurar su referencia identificativa, el número de la página y el total de estas. En lo que se refiere al **cuerpo** del dictamen, la norma detalla el título y contenido de los distintos apartados que debe recoger, tal como se muestran en la Fig. 5 y se detallan a continuación:

- Objeto
- Alcance
- Antecedentes
- Consideraciones preliminares
- Documentos de referencia
- Terminología y abreviaturas
- Análisis
- Conclusiones

Fig. 5. Apartados del cuerpo de un informe pericial (UNE 197001:2011)

- **Objeto**: indica la finalidad, que debe de ser especificada por el solicitante.
- **Alcance**: se deben indicar las cuestiones planteadas por el solicitante y el ámbito del estudio requerido.
- **Antecedentes**: descripción de los hechos, sucesos o asuntos que se hayan producido anteriormente y sobre los que se haya trabajado para elaborar el informe.
- **Consideraciones preliminares**: se deben enumerar todos los aspectos necesarios para comprender la investigación, así como la metodología empleada.
- **Documentos de referencia**: debe recoger las normas, la buena práctica profesional y la bibliografía citada en el informe.
- **Terminología y abreviaturas**: relación de definiciones técnicas, así como el significado de las siglas utilizadas en el informe.
- **Análisis**: en este apartado se deben describir los datos de partida y bases establecidas por el solicitante y los que se deriven de la legislación aplicable, de la investigación reali-

zada, de las referencias, documentos, procedimientos y pruebas que puedan dar fundamento a las conclusiones del informe.

- **Conclusiones**: describe, de manera inequívoca y resumida, la interpretación técnica de los hechos sobre los que se solicita el informe. Si el solicitante planteó preguntas concretas, se deberán incluir tanto las preguntas como las respuestas en este apartado.

Adicionalmente, debe incluirse una **declaración** del perito acerca de posibles tachas y juramento o promesa de imparcialidad. Un ejemplo puede ser el siguiente:

"De conformidad con lo dispuesto en el Art. 335.2 de la Ley de Enjuiciamiento Civil 1/2000, de 7 de enero, el perito promete que todo lo declarado en este dictamen respeta el principio de veracidad y que ha actuado con la mayor diligencia posible tanto en las cuestiones técnicas como en la consideración de fuentes de información confiables, con completa independencia de lo que pueda afectar a cualquiera de las partes, y que conoce las sanciones en las que podría incurrir si incumpliera las premisas establecidas por Ley para la elaboración de este dictamen pericial."

Por último, la norma recomienda que los **anexos** deben ser identificados de manera correlativa y paginados de forma inequívoca.

Norma UNE 197010:2015 - Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones

http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0055393&PDF=Si#.VtSiwPnhBMw

En su introducción, la norma enumera los principios que deben respetarse durante la selección, obtención, presentación y almacenado de evidenciasm, físicas o digitales:

- **Relevancia**: es la propiedad que resalta unas evidencias sobre otras en función de su transcendencia y el valor que aportan en el informe pericial.
- **Fiabilidad**: capacidad de que se puedan reproducir los resultados del proceso de forma consistente por investigadores independientes, a partir de las mismas evidencias.
- **Suficiencia**: que la evidencia presentada sea representativa, acorde y proporcionada al objeto de lo que se quiere demostrar.
- **Oportunidad**: que sea representativa de las circunstancias y momento temporal en que se presenta como prueba, y pueda ser transcendente en el juicio.

En su apartado 4, la norma describe los requisitos generales del informe pericial en materias tecnológicas, apoyándose en la norma UNE 197001:2011. Resalta en este aspecto la inclusión del sello de visado del colegio profesional correspondiente, cuando proceda.

Se hace también mención a que la firma del dictamen por el perito, si se proporciona el mismo en soporte digital, debe ir incorporada digitalmente.

Por último, la norma enumera las evidencias digitales mínimas que deben contener los informes o dictámenes periciales TIC, según su tipología:

- Sistemas de Información
  - Descripción del sistema de información analizado.
  - Gestión de la cadena de custodia.
  - Fecha y hora de intervención.
  - Condiciones de funcionamiento del sistema.

  - Medidas que se han tomado para salvaguardar el sistema de información.
  - Procedimiento y documentación.
  - Política de seguridad de la instalación donde está operando el equipo, incluyendo copias de seguridad.
  - Identificación del personal con acceso al equipo, como mínimo el administrador el sistema.
  - Topología de red, cortafuegos, NAT (Network Address Translation), VPN (Virtual Private Network), enlaces a internet, entre otros.
  - Normativa aplicada en la instalación afectada.
- Autenticación del correo electrónico
  - Valorar la seguridad del mecanismo de firma electrónica del correo.
  - Si no va firmado, hacer análisis de la cabecera o ver si existe un tercero con copia del mensaje.
  - Cotejo de las cabeceras del correo electrónico con los históricos de los servidores utilizados.
  - Informe del proveedor de internet, si procediera.
- Delitos contra la propiedad intelectual e industrial en formato digital. Identificación, manipulación o utilización de:
  - componentes hardware,
  - elementos software,
  - documentos digitales, películas, vídeos, música y juegos,
  - patentes y propiedad intelectual relacionadas con las TIC.
- Utilización e identificación de metadatos encontrados en:
  - correos electrónicos,
  - fotografías y documentos gráficos,
  - documentos electrónicos de texto.
- Contenido web
  - captura de la pantalla en modo gráfico,
  - acta testimonial del contenido,
  - acceso a la página web en cuestión.
- Soporte de almacenamiento digital (discos duros, pendrives, memorias SD, etc.)
  - inventario del contenido,
  - si se ha iniciado o continuado la cadena de custodia,
  - si se ha realizado copia forense del componente original,
  - si se ha aplicado las claves HASH11 al elemento original y a la copia.
  -

IMPORTANCIA DE LOS MÉTODOS UTILIZADOS EN LA PRUEBA PERICIAL

Para resaltar la importancia de seguir el mejor método en la preparación de la prueba pericial y la redacción del correspondiente informe o dictamen, según corresponda, debemos considerar que tanto los plazos como el número de pruebas periciales están limitados durante un proceso judicial. En la Fig. 6 se ilustra el esquema de un proceso de demanda en la jurisdicción civil, donde se puede comprobar que el máximo número de pruebas periciales presentables por las partes es tres.

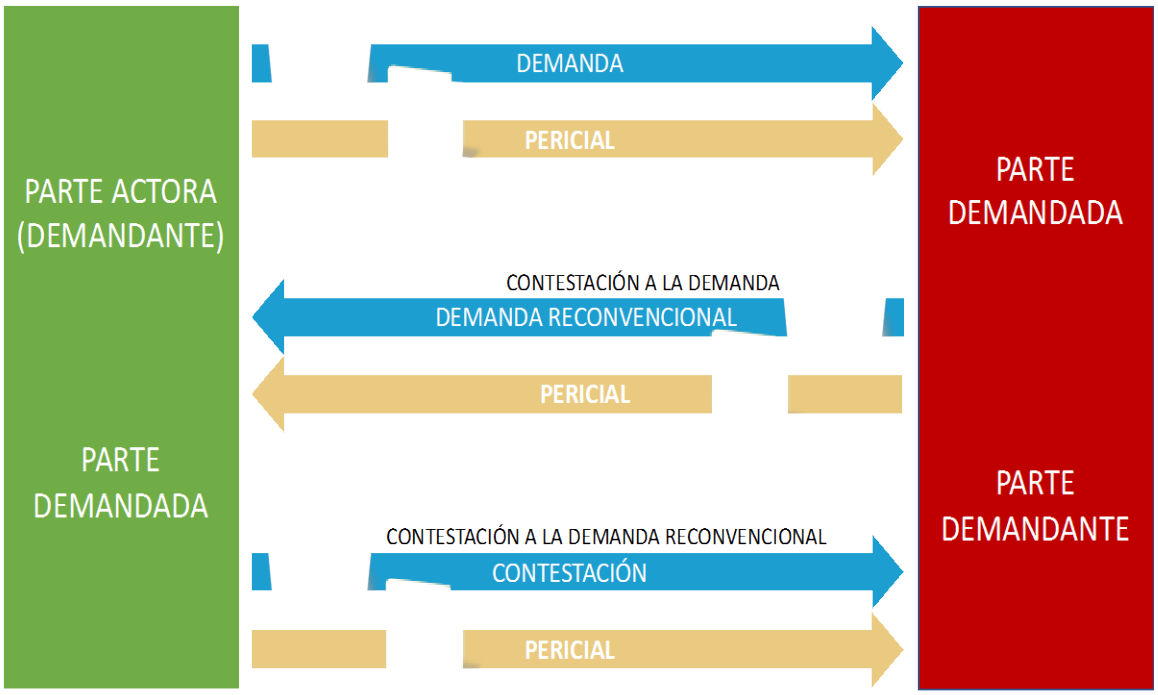

Fig. 6. Esquema del proceso judicial en la jurisdicción civil con demanda reconvencional

Además, resulta especialmente interesante que el informe o dictamen pericial sea lo suficientemente completo, claro y contundente como para evitar la asistencia del perito al juicio, e incluso llegar a un acuerdo antes de su celebración. Se ha de recordar que, tal como recoge el Art. 347 de la LEC, las partes podrán solicitar que el perito acuda al juicio para algunas de las siguientes cuestiones:

1. Exposición completa del dictamen, cuando esa exposición requiera la realización de otras operaciones, complementarias del escrito aportado, mediante el empleo de los documentos, materiales y otros elementos …/…
2. Explicación del dictamen o de alguno o algunos de sus puntos, cuyo significado no se considerase suficientemente expresivo a los efectos de la prueba.
3. Respuestas a preguntas y objeciones sobre método, premisas, conclusiones y otros aspectos del dictamen.
4. Respuestas a solicitudes de ampliación del dictamen a otros puntos conexos, por si pudiera llevarse a cabo en el mismo acto y a efectos, en cualquier caso, de conocer la opinión del perito sobre la posibilidad y utilidad de la ampliación, así como del plazo necesario para llevarla a cabo.
5. Crítica del dictamen de que se trate por el perito de la parte contraria.
6. Formulación de las tachas que pudieren afectar al perito.

Como se aprecia, si un dictamen es lo suficientemente completo y da respuestas inequívocas, sólidas y con la profundidad técnica necesaria, se aumenta la probabilidad de que la presencia del perito no resulte necesaria y, lo que es más, la probabilidad de llegar a un acuerdo entre las partes o de acortar la duración del proceso aumenta.

Para ello, es sumamente importante que en el dictamen pericial se responda solo a lo que se pregunta en el documento redactado por las partes (conocido como la “pericial”), con rigor científico, utilizando las figuras, esquemas, tablas y dibujos que sean necesarios, y evitando indefini-

ciones, como el uso de la palabra "etcétera". Es conveniente resaltar lo más relevante, mediante subrayado, negrita u otro método, teniendo en cuenta que la utilización de colores puede no ser eficaz, ya que en muchas ocasiones los juzgados imprimen o fotocopian los documentos en blanco y negro, en la actualidad. Debe también prestarse especial atención a redactar las conclusiones de manera sencilla y entendible por personas que no sean tecnólogas, así como sustentarlas siempre en los datos y resultados mencionados.

En relación con la información consultada o de base para responder a las preguntas solicitadas, es recomendable seguir los siguientes criterios, para una mejor comprensión y claridad en la lectura:

i) Enumerar las preguntas realizadas en la pericial y resaltar cada una de ellas como un apartado o epígrafe independiente en el documento.
ii) Cuando se adopte un dato de un documento externo (informe, reglamento, bibliografía), añadir una nota al pie con los datos del documento y, si es posible, un enlace URL al mismo.
iii) En todos los casos, añadir un apartado, antes de los que corresponden a las respuestas a las preguntas formuladas, facilitando la lista de todos los documentos consultados para la elaboración del informe, incluyendo sus datos y, en la medida de lo posible, un enlace URL al mismo.
iv) Si se desea transcribir todo o parte de alguno de los documentos, por ser de difícil acceso, no estar disponible para su consulta u otro criterio, todo este contenido deberá ir en un anexo al dictamen pericial, con el fin de no entorpecer su lectura y facilitar la distribución de copias múltiples del documento principal, de manera ágil.

Aunque resulte bastante evidente, no se deben olvidar determinadas cuestiones de forma en la elaboración del informe o dictamen pericial, como:

i) Identificar claramente en la página de portada el procedimiento judicial al que hace referencia, el nombre completo, número de colegiado y datos de contacto del perito.
ii) Firmar el documento, ya sea con firma tradicional o certificado digital, si se envía por métodos telemáticos.
iii) Visarlo por el colegio profesional competente, cuyo sello aparecerá a lo largo del documento en todas las páginas o algunas, según los criterios de cada colegio.

Es bastante probable que el perito necesite examinar determinadas cosas o lugares de la otra parte, para lo cual es necesario que el procurador de la parte solicitante de la prueba pericial pida al juzgado o tribunal tal necesidad (según se recoge en el Art. 336 de la LEC), por lo que el perito deberá dirigirse a él en los términos más concretos y con la mayor precisión posible, a fin de obtener tal autorización.

Adicionalmente, "*cuando la emisión del dictamen requiera algún reconocimiento de lugares, objetos o personas o la realización de operaciones análogas, las partes y sus defensores podrán presenciar uno y otras, si con ello no se impide o estorba la labor del perito y se puede garantizar el acierto e imparcialidad del dictamen. Si alguna de las partes solicita estar presente …/…, el tribunal decidirá lo que proceda y, en caso de admitir esa presencia, ordenará al perito que dé aviso directamente a las partes, con antelación de al menos* ***cuarenta y ocho horas****, del día, hora y lugar en que aquellas operaciones se llevarán a cabo*" (Art. 345 de la LEC).

RECOMENDACIONES METODOLÓGICAS PARA LA ELABORACIÓN DEL DICTAMEN PERICIAL

Apoyándonos en lo que recogen Babitsky, S. y Mangraviti, J.[1] y ampliándolo según experiencia propia, un informe pericial debe respetar las siguientes recomendaciones:

- **No especular o tratar de adivinar cosas**: debe hacerse mención a los hechos y pruebas fehacientes en todo momento, sin hacer afirmaciones que queden sin estar soportadas por los datos facilitados. No se debe escatimar en cuanto a la cantidad de información y datos a aportar, siempre que estos vayan orientados directamente a soportar las afirmaciones del perito.
- **Evitar el uso de universales o absolutos como "siempre", "nunca", "para todos los casos"**: la credibilidad de un informe radica en la concreción de sus afirmaciones. Por este motivo, conviene siempre acotar las afirmaciones y juicios de valor que emita el perito, explicando con la máxima claridad las circunstancias y condiciones que implican que la conclusión única posible es la enunciada.
- **Evitar expresiones que sugieran vaguedad, aspectos equívocos o incertidumbre**: una sola frase que infunda confusión, incertidumbre o sensación de poco dominio de la materia puede ser suficiente para desacreditar un informe completo. Es muy conveniente releer el informe una vez terminado y no dudar en eliminar directamente cualquier frase que pueda infundir dudas sobre el dominio de la materia por parte del perito.
- **Evitar el uso de lenguaje empático, signos de exclamación, uso de formatos, como negrita, cursiva y mayúsculas para enfatizar los hallazgos o conclusiones**: un dictamen pericial es un documento totalmente formal, que quedará registrado dentro del sumario del proceso judicial. El uso de lenguaje y formatos informales contribuirá a generar dudas sobre la rigurosidad del informe en la mete de los lectores, aunque sea de manera subconsciente, impactando negativamente en el resultado que se persigue: resolver todas las dudas y cuestiones planteadas por una persona realmente experta.
- **Utilizar un lenguaje preciso, sin jerga**: aunque al perito tecnológico le va a resultar bastante complicado expresar determinadas ideas sin acudir a jerga del sector, el informe debe conseguir un equilibrio entre la utilización de tecnicismos y conceptos altamente técnicos, que contribuyan a demostrar el dominio de la materia, y una redacción sencilla y directa, que ayude al lector no técnico a entender mejor el análisis y los resultados reflejados en el informe.
- **Hacer uso de un lenguaje seguro, sin adornos literarios y evite las palabras como "se ve como", "podría", "aparentemente", "yo creo", "es probable que", entre otras**: como ya se ha mencionado, cualquier atisbo de incertidumbre o muestra de falta de dominio en la materia técnica en cuestión puede desacreditar todo el informe. Por este motivo, es sumamente importante redactarlo con frases que demuestren contundencia, directas, breves y concisas. En este sentido, hay que recordar que no se está dando una lección, por lo que es preferible una redacción contundente y menos autoexplicativa a una expresión que intente "enseñar" al lector a llegar a las conclusiones, partiendo de conceptos demasiado básicos para un profesional del sector, ya que es posible que esto genere dudas sobre la competencia del perito si el informe es leído por otro profesional del mismo

[1] Babitsky, S. y Mangraviti, J. "Writing and Defending Your Expert Report: The Step-by-Step Guide with Models", 2002. Seak Inc.

sector (un ejemplo de lo que no hacer sería explicar el concepto de "ancho de banda" en un informe sobre radiofrecuencia).

- **Definir todos los términos técnicos que aparezcan en el informe**: se pueden añadir notas al pie para explicar conceptos complejos, incluyendo acrónimos y cualquier otro término técnico, con independencia de que todos los acrónimos deberían aparecer al final, en su sección específica.
- **Utilizar un lenguaje concreto sobre los hechos y evite caracterizaciones subjetivas para describir la investigación, los hallazgos y las conclusiones**: es sumamente importante que la descripción de los hechos se encuentre totalmente separada de análisis y juicios de valor del perito. Se deben redactar en párrafos aislados y utilizando un lenguaje descriptivo. Evitar siempre entremeter en estos párrafos condicionantes o afirmaciones no probadas, incluso aunque se encuentren así redactadas en documentos del sumario (por ejemplo, "tal como afirma la parte demandante" o "en contra de lo que se argumenta en el documento X"). Los hechos deben ser claros, directos y concisos, para ser fácilmente tomados como "ingredientes" para elaborar el análisis, a posteriori.
- **Explicar cualquier abreviatura utilizada**: aunque la recomendación general es no utilizar nunca abreviaturas, si un término se repite en numerosas ocasiones a lo largo del informe y existe una abreviatura aceptada para él, debe reflejarse la abreviatura y el término completo la primera vez que sea mencionado en el informe, entre paréntesis, salvo que se trate de una abreviatura comúnmente conocida (por ejemplo, "Sr.").
- **Evitar lenguaje argumentativo, que pueda sugerir un interés particular**: el perito debe demostrar neutralidad en todo momento. Expresiones del tipo "Se concluye X. De otro modo, implicaría que Y" sonará a que existe una inclinación del perito a concluir X a toda costa. La segunda frase debería ser eliminada del informe. En todo caso, si se considera que la afirmación Y es esencial para concluir X, entonces debería mencionarse antes de la conclusión, como parte del análisis.
- **No hacer comentarios sobre la credibilidad de los testigos y las pruebas**: hay que ser conscientes de que las pruebas han sido aceptadas por el juez y no son cuestionables, y que las declaraciones de los testigos se han hecho bajo juramento o promesa de decir la verdad. Un informe que cuestione lo que se toma como verdadero carecerá de ninguna validez. No obstante, si el perito tiene sospechas fundadas de que una prueba o declaración no puede ser cierta desde sus conocimientos estrictamente técnicos en la materia, puede reflejarlo en el informe de una manera elegante, por ejemplo, reflejando que "*se asume que la prueba X ha sido validada por el método Y, única manera de demostrar su veracidad desde el punto de vista técnico, dado que es esencial para obtener las conclusiones de este informe*".
- **Validar la consistencia del informe**: es muy conveniente, sobre todo en informes de cierta longitud, realizar esquemas o añadir párrafos recopilatorios que ayuden a conservar el hilo argumental en la mente del lector, del tipo: "*Como se ha detallado en el apartado X, la evidencia o prueba X conduce a Y y, mediante el cálculo Z se deduce que W*".
- **Evitar cualquier sesgo en el informe**: la mejor forma de realizar esta verificación es ponerse en la postura de la parte contraria a la que ha solicitado el informe y releerlo. Aunque es muy difícil que no exista un sesgo por parte del perito, una vez realizado el análisis completo y extraídas las conclusiones, es muy importante que el informe se muestre totalmente imparcial hasta llegar a las conclusiones puesto que, si desde el principio se vislumbra la conclusión a la que "se quiere llegar", perderá credibilidad y peso.
- **Numerar las líneas del informe**: aunque esto puede resultar extraño, es una buena práctica en el caso de que existan apartados muy extensos para quem, en el caso de requerirse alguna revisión de los resultados, cualquiera pueda remitirse de manera rápida al lugar concreto en el mismo. No es necesario indicar todos los números de línea. Se pue-

den indicar, por ejemplo, múltiplos de 5 o 10 líneas, para evitar sobrecargar el documento.

Como se ha podido comprobar, la redacción del informe o dictamen pericial no implica solamente disponer de los conocimientos técnicos adecuados para realizar el análisis sobre los hechos y extraer las conclusiones y respuestas a las preguntas planteadas, sino también estructurarlo y redactarlo de una manera eficaz para el fin que persigue. Tan importante es conseguir el resultado como saberlo comunicar de manera correcta y eficaz, para conseguir el fin que se persigue: dirimir el conflicto con la mayor rapidez y el menor coste posible.

METODOLOGÍAS EN ANÁLISIS FORENSE DIGITAL. NORMAS Y GUÍAS ACTUALES

Las evidencias digitales están adquiriendo formas cada vez más inesperadas, debido a la proliferación de nuevos dispositivos y componentes tecnológicos, que desafían los procedimientos y metodologías actuales. Para ello, los comités e instituciones normalizadores están haciendo grandes esfuerzos en actualizar o publicar nuevas normas y guías que contemplen estos avances.

En la actualidad existen diferentes guías, metodologías y normas para ayudar al perito tecnológico. Adicionalmente a aquellas que se centran más en el formato y contenido del dictamen pericial en sí, como la ya analizada UNE 197010:2015 “Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones”, en este apartado se recogen las siguientes normas internacionales ISO, españolas UNE y las referencias documentales RFC, orientadas al tratamiento de evidencias, metodologías para el análisis forense digital y elaboración de informes o dictámenes periciales:

- RFC 3227 - “Directrices para la recopilación de evidencias y su almacenamiento”
- ISO/IEC 27037:2012 - “Guía para la identificación, recolección, adquisición y preservación de evidencias digitales”
- UNE 71505-2:2013 - “Buenas prácticas en la gestión de evidencias electrónicas”
- UNE 71506:2013 - “Metodología para el análisis forense de evidencias electrónicas”
- ISO/IEC 27041:2015 - “Guidance on assuring suitability and adequacy of incident investigative method”
- ISO/IEC 27042:2015 - “Guidelines for the analysis and interpretation of digital evidence”
- ISO/IEC 27043:2015 - “Incident investigation principles and processes”
- ISO/IEC WD 27044 - “Security Information and Event Management (SIEM)”

RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento

http://www.ietf.org/rfc/rfc3227.txt

Este documento de febrero de 2002 forma parte del conjunto de recomendaciones técnicas y organizativas, editadas por el Internet Engineering Task Force (IETF), que conforman los protocolos para el funcionamiento de Internet y tiene como objeto proporcionar a los administradores de sistemas las directrices a tener en cuenta en las fases de recopilación y de almacenamiento de las evidencias digitales que resulten relevantes en un incidente de seguridad producido en un sistema informático.

Para ello, describe en primer lugar unos principios directores a tener en cuenta durante la recopilación de evidencias, que divide en cuatro apartados:

- **Orden de volatilidad de las evidencias digitales**, debiendo recopilarse en orden de mayor a menor volatilidad. En un sistema típico, se empezaría por los registros o la memoria caché del sistema y se finalizaría por los dispositivos de almacenamiento (CDs, DVDs, etc.)
- **Cosas que se deben evitar para impedir la fácil destrucción de evidencias**, como no apagar el equipo hasta terminar la recopilación de evidencias, utilizar programas residentes en dispositivos conocidos y que no modifiquen la fecha de los ficheros o recopilar la información de red previamente a su desconexión.
- **Consideraciones sobre privacidad**, respetando las normas legales y de empresa. En especial, no recoger información de áreas privadas sin respaldo jurídico suficiente.
- **Consideraciones legales respecto de las evidencias**, que deben ser admisibles en juicio, auténticas, completas, fiables y creíbles para el juez.

En segundo lugar, describe las recomendaciones para el procedimiento de recopilación, que debe de ser lo más detallado posible, sin ambigüedades y minimizando la toma de decisiones durante la recogida de evidencias. En especial:

- Los métodos de recopilación deben ser transparentes y reproducibles.
- Se deben seguir estos pasos para la recopilación:
    - Listar los sistemas desde los que se recopilarán las evidencias.
    - Determinar lo que va a ser relevante y admisible en juicio, procurando errar más bien por exceso que por defecto.
    - Determinar en cada sistema el orden de volatilidad de las evidencias.
    - Desconectar las interfaces de red.
    - Recopilar las evidencias según el orden de volatilidad y con las herramientas que se describen posteriormente.
    - Preguntarse qué más puede resultar una evidencia útil.
    - Documentar cada paso.
    - Tomar notas acerca de las personas involucradas durante la recopilación y de sus reacciones.
- Siempre que sea posible, generar la huella digital de cada evidencia y firmarla criptográficamente.

En tercer lugar y en relación al procedimiento de archivo, cada evidencia debe asegurarse estrictamente y documentar su cadena de custodia, detallando:

- Cómo se encontró y fue tratada la evidencia
- Dónde, cuándo y quién la descubrió y recogió
- Dónde, cuándo y quién la trató o examinó
- Quién, durante qué periodo y cómo la ha custodiado y, en caso de cambio de custodia, cuándo y cómo se ha llevado a cabo

Para el archivo de evidencias deben usarse elementos estándar en lugar de propietarios, restringiendo los accesos, que deben quedar registrados, así como los intentos no autorizados.

Por último, en relación con las herramientas informáticas a utilizar en la recopilación, y ya en términos más técnicos, se recomienda disponer previamente de un conjunto de herramientas para cada sistema operativo en soportes de solo lectura, incluyendo:

- Un programa para el examen de los procesos del sistema, como “ps”.
- Programas para examinar el estado del sistema, como “showrev”, “ifconfig”, “netstat” o “arp”.

- Un programa para hacer copias a nivel de bit, como “dd” o “SafeBack”.
- Programas para generar huellas digitales y firmas, como “SafeBack”, “sha1sum” o “pgp”.
- Programas para generar y examinar imágenes del núcleo del sistema (*core*), como “gcore” o “gdb”.
- Ficheros de órdenes (*scripts*) para automatizar la recopilación, como “The Coroner's Toolkit”.

Finaliza recomendando utilizar enlaces estáticos a dichos programas y advirtiendo de que existen herramientas en módulos cargables del núcleo del sistema que pueden proporcionar una imagen parcial del mismo. En cualquier caso, se debe estar preparado para garantizar la autenticidad y fiabilidad de las herramientas utilizadas.

ISO/IEC 27037 - Guía para la identificación, recolección, adquisición y preservación de evidencias digitales

www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

Publicada el 15 de Octubre de 2012, es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

Esta norma proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digital, como discos duros, discos ópticos, cintas, etc, que se suelen emplear en ordenadores y sistemas informáticos.
- Teléfonos móviles, PDAs, dispositivos personales electrónicos, tarjetas de memoria.
- Sistemas de navegación geográfica (GPS).
- Cámaras digitales y de vídeo.
- Equipos con conexión de red.
- Redes funcionando sobre el protocolo TCP/IP u otros.
- Todos aquellos dispositivos con funciones similares a los anteriores.

A diferencia de la RFC 3227, la norma ISO/IEC 27037 hace referencia a componentes tecnológicos más avanzados y tiene esta característica en cuenta en el desarrollo de la misma. Por ejemplo, es más adecuada y actual para el análisis de teléfonos móviles.

UNE 71505-2 - Buenas prácticas en la gestión de evidencias electrónicas

http://www.aenor.es/aenor/normas/buscadornormas/resultadobuscnormas.asp#.Vt3DfvnhBMw

Norma española publicada en julio de 2013, que establece los controles y procesos para la gestión de seguridad de las evidencias electrónicas. Se aplica a entornos propios de las organizaciones con independencia de su actividad o tamaño. Puede ser también aplicada por empresas que desempeñen servicios cuyos ciclo de vida y controles son descritos en la norma.

Establece la información que debe acompañar a la evidencia electrónica, además de su propio contenido, con el fin de documentar una determinada operación:

- **Estructura**: formato y relaciones entre elementos que la integran, que deberían permanecer intactos.
- **Fecha** que fue creada, recibida y manipulada, así como, los **participantes** a lo largo del proceso.
- En caso de existir, **vínculo entre evidencias**.

La norma UNE 71505 consta de tres partes. La primera está dedicada a vocabulario y principios generales, la segunda contiene buenas prácticas para lo que denomina Sistema de Gestión de Evidencias Electrónicas (SGEE), consistentes en la definición de controles relativos a la gestión de la identidad, trazabilidad, almacenamiento y custodia segura de las evidencias digitales, y la tercera trata de los formatos de intercambio de evidencias electrónicas que permiten asegurar su contenido, así como de los mecanismos técnicos aplicables al mantenimiento de su confiabilidad.

En su apartado 4.2, trata sobre la confiabilidad de los sistemas, procesos y procedimientos, para minimizar la posibilidad de que se cuestione la veracidad y exactitud de las pruebas:

- Disponibilidad y completitud
- Autenticación e integridad
- Cumplimiento y gestión

En su apartado 4.3, se describen los beneficios de la gestión de las evidencias y la importancia, como recurso valioso en una organización, de las evidencias electrónicas.

El **Sistema de Gestión de Evidencias (SGEE)** se trata en el apartado 5, donde se describe la gestión del ciclo de vida de la evidencia electrónica, incluso antes de su adquisición: generación, almacenamiento, transmisión, recuperación, comunicación y preservación.

Esta norma adopta un enfoque por procesos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGEE. También describe como la política de la organización debe reflejar la implicación del marco normativo y regulatorio en sus procesos de negocio. En su anexo A, se detalla un código de buenas prácticas, específicas para el SGEE.

En su anexo B, se aporta la matriz utilizada para asignar nuevas funciones a los responsables de la implantación de la norma (funciones x responsable).

UNE 71506 -Metodología para el análisis forense de las evidencias electrónicas

http://www.aenor.es/aenor/normas/buscadornormas/resultadobuscnormas.asp#.Vt3DvPnhBMw

La norma UNE 71506 complementa la norma anterior, al abordar la metodología para el análisis forense, incluyendo en ella la preservación, adquisición, documentación, análisis y presentación de evidencias electrónicas. Fue publicada en julio de 2013 y es de aplicación a cualquier organización, así como profesional competente en este ámbito, como por ejemplo el perito informático forense. Va dirigida especialmente a los equipos de respuesta a incidentes y seguridad, así como al personal técnico de laboratorios o entornos de análisis forense de evidencias digitales.

Define el proceso de análisis forense para complementar el SGEE de la norma UNE 71505 descrita en el punto anterior.

El capítulo 5 está dedicado a la preservación de las evidencias originales, garantizando su inalterabilidad y validez legal, lo que permite la reproducibilidad de estudios sobre ellas. Almacenamiento en lugares y soportes estancos y aislados de interferencias o posibles agentes externos.

El siguiente capítulo trata la adquisición de las evidencias, distinguiendo el trato a seguir si el sistema está apagado o encendido. También se valora que el análisis forense puede ser sobre datos de origen estático, datos en tránsito de sistemas en funcionamiento, datos volátiles, sistemas embebidos, datos de móviles y redes, así como grandes sistemas almacenamiento con información repartida en varios repositorios.

El capítulo 7 se refiere a la documentación, garantizar la cadena de custodia y la trazabilidad de las evidencias, a través de la implantación de un sistema de gestión documental que registre las actuaciones sobre dichas evidencias, bien sean originales o clonadas.

Su capítulo 8 está dedicado al análisis de las evidencias digitales objeto de investigación y el capítulo 9 trata la presentación de los resultados obtenidos a la autoridad judicial o entidad que solicita el informe pericial.

En sus anexos se encuentran el modelo de informe pericial, las competencias para el análisis forense de las evidencias electrónicas y el equipamiento recomendado para el análisis forense de evidencias electrónicas.

Esta norma junto con la UNE 71505 conforman una metodología muy utilizada por profesionales y organismos nacionales en la actualidad, así como las fuerzas y cuerpos de seguridad del estado.

ISO / IEC 27041 – Guidance on assuring suitability and adequacy of incident investigative method

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44405

Esta norma internacional fue publicada, en inglés, en junio de 2015 y ofrece orientación sobre los mecanismos para garantizar que los métodos y procesos utilizados en la investigación de incidentes de seguridad informática son los adecuados. Incluye la consideración de cómo los proveedores y pruebas de terceros se pueden utilizar para ayudar a este proceso de garantía.

Sus objetivos son:

- Proporcionar pautas sobre la captura y el posterior análisis de los requisitos tanto funcionales como no funcionales relacionados con la seguridad en la investigación de incidentes.
- Utilizar la validación como medio de garantías de la idoneidad de los procesos involucrados en la investigación.
- A partir de un ejercicio de validación, determinar nuevos niveles de validación que se requieran y las pruebas requeridas.
- Determinar pruebas externas y la documentación a incorporar en el proceso de validación.

Esta norma puede resultar útil para garantizar la validez de las evidencias digitales durante un proceso judicial.

ISO/IEC 27042 - Guidelines for the analysis and interpretation of digital evidence

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44406

Esta norma proporciona una guía para el análisis e interpretación de la evidencia digital. Fue publicada en junio de 2015 (en inglés). Provee información sobre como adelantar un análisis e interpretación de la evidencia digital potencial en un incidente con el objeto de identificar y evaluar aquella que se puede utilizar para ayudar a su comprensión. Ofrece un marco común para el análisis e interpretación de la gestión de incidentes de seguridad, que pueda utilizarse para implementar nuevos métodos. También introduce una serie de definiciones relevantes para la práctica del análisis forense digital.

Adicionalmente, la norma trata los modelos analíticos que pueden ser usados por los peritos informáticos forenses en sistemas estáticos o activos y las consideraciones, a tener en cuenta en cada caso, en especial atención a incidentes en sistemas vivos o activos como: dispositivos móviles, sistemas cifrados, redes, etc.

Se definen dos formas de adelantar el análisis en vivo:

- **Sistemas que no pueden ser copiados o que no permiten crear una imagen**: existe el riesgo de perder la evidencia digital cuando se está copiando. Es importante ser cuidadoso para minimizar el riego de daño de la evidencia y asegurar que se tiene un registro completo de los procesos.
- **Sistemas que permiten copiar o realizar una imagen**: examinar el sistema interactuando u observándolo en su operación. Ser cuidadoso para emular el hardware o software del entorno original, usando máquinas virtuales verificadas, copias del hardware original con el fin de permitir un análisis lo más cercano posible al real.

Por otro lado, se detalla el contenido de los resultados del análisis en el informe pericial y sus consideraciones legales. Finalmente, recoge las competencias de los peritos forenses: formación, aprendizaje, habilidades, objetividad y ética profesional.

ISO/IEC 27043 – Incident investigation principles and processes

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44407

Norma internacional, publicada en inglés en marzo de 2015. Proporciona una guía de principios para los procesos de investigación de incidentes que involucran evidencias digitales. Incluye los procesos de preparación previa al incidente a través del cierre de la investigación, así como advertencias al respecto.

Las directrices describen los procesos y principios aplicables a los distintos tipos de investigaciones delictivas, como por ejemplo, violaciones de seguridad, fallos del sistema, accesos no autorizados, entre muchos otros. No ofrece detalles particulares para cada tipo de investigación pero si una visión general de los principios y procesos de investigación aplicables.

ISO/IEC WD 27044 - Security Information and Event Management (SIEM)

http://www.iso.org/iso/catalogue_detail.htm?csnumber=62287

Norma internacional todavía en desarrollo, que trata de describir un sistema para la gestión de eventos y de la seguridad de la información (SIEM). Con esta norma se pretende dar solución a los actuales problemas que existe a la hora de recoger evidencias en sistemas activos, complejos o con falta de recursos.

Estas herramientas permiten monitorizar en tiempo real los eventos, proporciona la visibilidad de toda la estructura de información, captura y análisis de redes y dispositivos móviles, control de aplicaciones y eventos que generan. Análisis de sistemas objeto de ataque, antes, durante y después del mismo. Administrador de riegos de la organización o entorno. Gestión de logs de los elementos y dispositivos del sistema global. Capacidad de resiliencia en las organizaciones objeto de ataque.

En resumen, proporciona a las organizaciones una plataforma de inteligencia de la seguridad.

CONCLUSIONES

La prueba pericial puede convertirse en un arma esencial para agilizar y reducir el coste de un proceso judicial. En el ámbito de las materias tecnológicas, el desconocimiento generalizado y la complejidad de las materias de estudio pueden llegar a producir el efecto contrario, si el dictamen o informe pericial no está bien ejecutado.

A lo largo de este artículo se ha detallado los requisitos mínimos y deseados exigibles a un perito judicial en materias tecnológicas, así como metodologías que contribuyen a un dictamen de gran calidad, difícilmente refutable y con la suficiente claridad para contribuir a acelerar la sentencia durante un proceso judicial, o incluso favorecer un acuerdo y hasta llegar a evitar acudir a los tribunales.

Adicionalmente, se ha realizado un análisis general de todas las normas y recomendaciones existentes sobre informes periciales en materias tecnológicas, destacando las claves principales de cada una de ellas.

En conclusión, queda reflejada la importancia tanto de la forma como del contenido y de los medios utilizados -incluyendo las capacidades y conocimientos del propio perito- para producir un dictamen que cumpla el fin perseguido: aclarar todas las cuestiones técnicas de manera contundente, sin lugar a dudas, contribuyendo a acelerar el proceso judicial y, por ende, reducir los costes para ambas partes.

Para más información y profundidad en la materia, el lector puede dirigirse al Instituto de Asesores:

www.institutodeasesores.com

INSTITUTO DE ASESORES

NORMATIVA SOBRE EL PERITAJE JUDICIAL TECNOLÓGICO

A continuación se enumeran algunas leyes relacionadas directa o indirectamente con la realización de pruebas periciales en materias tecnológicas y las competencias del perito tecnológico:

1. Decisión 2002/630/JAI del Consejo, de fecha 22 de julio de 2002 relativa a la cooperación policial y judicial en materia penal (AGIS)
2. Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (LEC)
   https://www.boe.es/buscar/pdf/2000/BOE-A-2000-323-consolidado.pdf
3. Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa (LJCA)
   http://www.boe.es/buscar/pdf/1998/BOE-A-1998-16718-consolidado.pdf
4. Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social (LRJS)
   http://www.boe.es/buscar/pdf/2011/BOE-A-2011-15936-consolidado.pdf
5. Ley de Enjuiciamiento Criminal (LECrim), de 14 de septiembre de 1882
   http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf
6. Ley 59/2003, de 19 de diciembre, de Firma Electrónica
   http://www.boe.es/buscar/pdf/2003/BOE-A-2003-23399-consolidado.pdf
7. Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)
   http://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf
8. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
   http://www.boe.es/buscar/pdf/1992/BOE-A-1992-26318-consolidado.pdf
9. Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
   http://www.boe.es/buscar/pdf/1995/BOE-A-1995-7730-consolidado.pdf
10. Ley 25/2007, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones
    http://www.boe.es/buscar/pdf/2007/BOE-A-2007-18243-consolidado.pdf
11. Boletín Oficial Cortes Generales. Proyecto de Ley 121/000139
    http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-139-1.PDF