Periciales informáticas: un enfoque de gestión y legal.

Para el desarrollo de este documento me inspiro básicamente en dos fuentes: una, la propia experiencia y experiencia compartida de amigos peritos y otra, los magníficos libros que en su día (hoy quizá desfasados en su aparato legal, lo que no les resta su enorme valor) de mí también amigo Rafael López Rivera, que recomiendo fervientemente, en particular su "Peritaje Informático y Tecnológico", editado en Barcelona en 2012.

El objetivo principal del Peritaje Forense Informático y Tecnológico es obtener información y evidencias, generalmente digitales, procedentes de distintos medios: documentos, mensajes, correos, trazas, ficheros multimedia, etc. con distinto origen: de algo tangible como un disco duro a algo más virtuales, como la nube o un comentario en una red sociales.

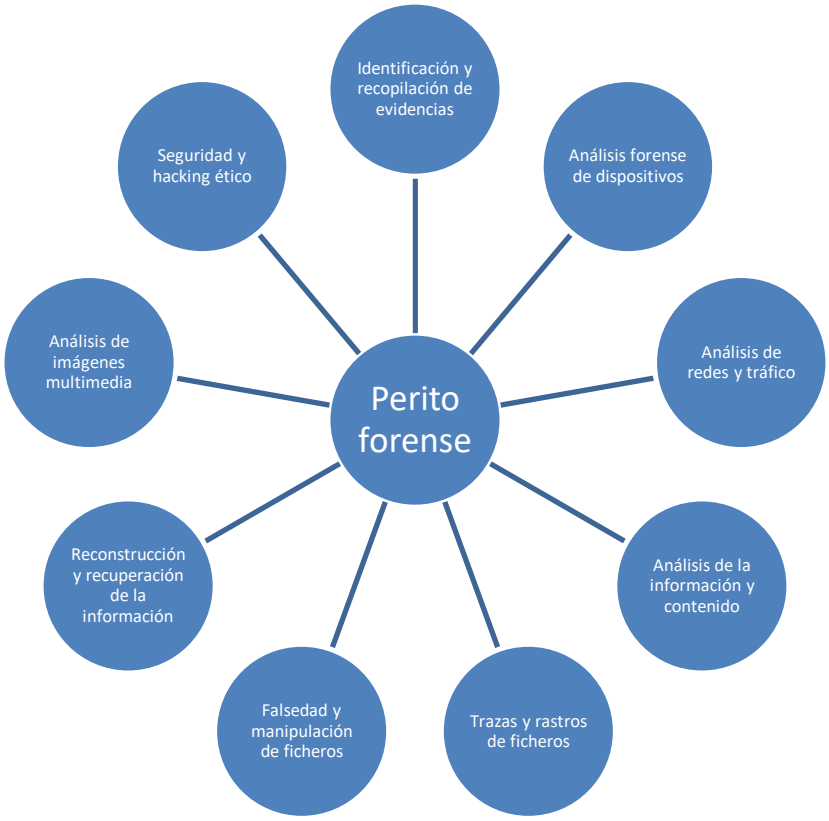
Nos vamos a mover en el interior de un triángulo formado por tres vértices: ley, personas, TIC.

Esto provocará que en la mayoría de las situaciones, el trabajo consista en tratar y generar medios de prueba con la materia prima de las e-evidencias (evidencia digitales, evidencias informáticas…). En muchas ocasiones, aunque no siempre, el trabajo finaliza en los Tribunales de Justicia.

No podemos hablar de un perfil único por la gran variedad de áreas y especialidades afectadas y la velocidad de cambio en nuestro campo (Android, GPS, nube, servidores, Linux… ¿hay un experto en absolutamente todo?). Pero es buena la especialización porque lo que es trabajo no faltará, gracias al uso extensivo de las TIC que cada vez convierte en más habituales (y numerosas) las actuaciones del perito forense informático.

Debemos tener en cuenta que de nuestro trabajo dependerá la validez de la prueba en un proceso legal.

Rafael López sugiere estas posibles actuaciones:



En el proceso de actuación de un peritaje forense se distinguen cinco fases que se encadenan de forma que hasta que no se cierra la anterior no se pasa a la siguiente: Identificación, Recopilación, Preservación, Análisis y Presentación o Emisión.

Antes de entrar en cada una de ellas tengamos claro que este proceso debe seguir una serie de pautas: debe ser científico/tecnológico (vamos, no basado en suposiciones, sino en comprobaciones, en datos), metódico (en todo momento emplearemos una metodología, bien descrita por alguna norma, bien porque forma parte de nuestro conocimiento profesional, al ser de uso extendido), sistemático (no dejamos nada por cubrir, es exhaustivo), reproducible (Esto es un poco redundante, pues si aplicamos el método científico, todo experimento debe poder reproducirse y comprenderse por otros expertos) y auditable (que no exista sospecha sobre nuestros resultados y métodos empleados[1]).

Lo mejor es seguir una metodología. INCIBE[2] recomienda varias. Yo invito a prestar atención a la RFC3227 - Directrices para la recolección de evidencias y su almacenamiento[3] que es, como dice bien el INCIBE, desde hace mucho, uno de los principales referentes y dos, por su comodidad para el perito, dentro de las normas UNE (una en realidad es una norma ISO ratificada). Como bien sabes, ambas puedes localizarlas en el buscador de AENOR (por eso no coloco enlace). Se trata de:

- **UNE-EN ISO/IEC 27037:2016 (Ratificada).** Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de

[1] Quizá es una percepción muy particular, pero esta última característica es la que más a menudo falla.
[2] https://www.incibe-cert.es/blog/rfc3227
[3] https://www.ietf.org/rfc/rfc3227.txt

evidencias electrónicas (ISO/IEC 27037:2012) (Ratificada por AENOR en diciembre de 2016.)

- **UNE 71506:2013.** Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.

Vamos con cada una de las partes.

Identificación

Es imprescindible conocer los antecedentes para entender la situación actual. Si no sabemos que ha habido amenazas de una persona a otra y se nos da un fichero con 10gb de correos estamos ciegos en la búsqueda. El conocimiento previo nos permite saber cómo organizar los trabajos, crear estrategias, etc., en nuestra búsqueda de unas evidencias necesarias.

Una vez claro el punto de partida debemos tener una serie de consideraciones:

1. Nuestro punto de partida: estudio claro del contexto legal, incluyendo autorizaciones legales, prerrequisitos, actores que pueden o no estar presentes… debemos en todo caso evitar que pueda quebrarse la validez de las evidencias.
2. Para todo aquello "físico", sean dispositivos o documentación, mantener una identificación que permita clasificarlo, incluso mediante etiquetado.
3. Muy ligado a lo anterior: descripción de los dispositivos implicados.
4. Estudiar si el objeto de estudio lo tenemos disponible de forma previa o debe ser capturada en el proceso de la investigación (tráfico de red, etc.)
5. Antes de empezar, comprobamos que disponemos de las herramientas precisas (hw y sw) para nuestro trabajo.
6. Inicio de la Cadena de Custodia: esto implica considerar los elementos precisos para garantizarla.

Recopilación

Esto será algo cambiante, según el tipo de dispositivo, entorno de uso e información con la que vamos a trabajar para extraer la e-videncia. Esto implica nuestra obligación de garantizar la integridad de la información que vamos configurando, dejando de forma auditable la comprobación de nuestra correcta manipulación y empleo metodológico. Un buen apoyo sería el empleo de "listas de chequeo" o "checklist" que de paso nos ayuden a no dejar nada por hacer. De forma añadida, si mantenemos un registro cronológico de nuestras actividades en el que anotemos cualquier hecho o dato encontrado curioso, significativo o que pueda ser de interés, es un complemento perfecto.

En esta parte de la actuación debemos priorizar aquellos objetos de estudio que sean más volátiles, considerando que en nuestro caso en muchas ocasiones solo tendremos una posibilidad de efectuar la capturar de la información, lo que nos lleva a extremar las precauciones que permitan preservar las garantías necesarias. Eso implica que, en todo contexto (captura de información de forma silente, p.e.) debemos confirmar que estamos respetando los requisitos de legalidad, p.e., no violando la privacidad de nadie sin la preceptiva autorización.

Preservación

Es más que posible que mientras hacemos nuestro trabaje manipulemos sometiendo al trabajo con herramientas a dispositivos y datos de forma que puede llegar a contaminar (alterar) el conjunto de evidencias.

Este y no otro es el motivo que recomienda no practicar trabajo alguno sobre las e-evidencias originales, sino a través de una copia idéntica (imagen) de la información.

Para evitar problemas debemos de identificar unívocamente las copias verificando que no solo no han sido manipuladas, sino que corresponden exactamente a las originales. Sobre esto volveremos más adelante, cuando hablemos de elementos como Hash o Blockchain. En cuanto a las e-evidencias originales, dado que pueden ser empleadas de nuevo (p.e. en una contrapericial) debemos poner especial mimo en evitar su alteración o borrado accidental. Es difícil que se pierda pues una copia se entregará al órgano de custodia, y nosotros nos quedaremos con otra por si tuviéramos que en otro momento realizar otras investigaciones alternativas. Siempre tendríamos que tener una copia aislada, de respaldo, para mantenerla a salvo de cualquier accidente.

Hay elementos que considerar y que anotar debidamente como, p.e.:

1. ¿Qué características tiene el dispositivo?
2. ¿estaba el dispositivo encendido?
3. ¿lo hemos apagado o encendido? ¿Por qué hemos actuado así?
4. ¿Está el dispositivo aislado de las redes/personas?
5. ¿Lo hemos aislado nosotros o no? ¿Por qué hemos actuado así?
6. ¿Dónde en el dispositivo podemos encontrar información de interés? (discos duros, tarjetas de memoria… ram, etc.)
7. ¿qué herramientas hw o sw vamos a emplear para realizar un duplicado?
8. ¿Qué garantías de no contaminación me dan esas herramientas?
9. ¿Qué proceso seguimos con cada herramienta?
10. ¿qué herramientas hw o sw vamos a emplear para interactuar con el dispositivo?
11. ¿Qué necesitamos para conservar la copia de las e-evidencias (medios, número, capacidad…)

Como en el paso anterior, mantendremos un registro de nuestros pasos, cronológico y todo lo prolijo posible, indicando la localización de cada una de las copias y las observaciones tomadas al efectuarlas.

Análisis

Ya tenemos nuestra copia de trabajo sobre la mesa. Ahora tenemos que enfrentarnos al “corazón del trabajo”. Cada caso es un mundo en sí mismo, dependiente de los antecedentes, la hipótesis de partida, los medios que empleemos para el estudio y recolección, las e-evidencias disponibles… todo esto hará diferir la ruta de cada análisis, dependientes de elementos como los sistemas operativos, redes empleadas, tipología de usuarios, dispositivos estudiados, etc. La perspectiva suele ser por parte del profesional un 99% tecnológica y un 1% legal… y esto es un error, porque por buena que sea la técnica, si nos salimos de los límites se

invalida la investigación. Por ello debemos considerar la necesidad de hacer un análisis, como antes indicábamos, basado en el método científico. Vamos a desarrollar esto un poco.

El método científico implica partir de una hipótesis y verificarla mediante e-evidencias, analizándolas para determinar la veracidad (o no) de nuestros presupuestos, todo sujeto al cumplimiento de buenas prácticas (hay muchos estándares definidos: ITIL, normas ISO, PMI, COBIT…). De esta manera nuestro estudio puede ser cotejado por terceros, sin mermar la credibilidad de nuestras acciones.

Pero en este punto hay un acontecimiento que se suele repetir ¿y si hemos de reconstruir la información? ¿Y si nos dan un disco borrado, un móvil reseteado, un pendrive manipulado? Obviamente, tendremos que emplear herramientas específicas, e incluso recurrir a terceros. Todo esto debe ser documentado con más mimo aun si cabe, en particular la intervención de terceros, para la que tendremos que disponer de las correspondientes autorizaciones.

Todo ello, acompañado de un completo registro donde figuren elementos tales como los metadatos de los ficheros y los actores del proceso (usuarios, programas, accesos, permisos, privilegios, etc), registro que debe incorporar una cronología precisa de los acontecimientos, que permita ver como se relacionan esos actores y así poder señalar los momentos críticos para nuestro estudio.

Presentación

Terminamos nuestro trabajo. Tenemos una conclusión que debemos plasmar en un informe.

Éste debe ser preciso y entendible por legos en la materia (debe ser entendido en un juzgado, en una corte de arbitraje, entre dos particulares…). Pensemos que en los casos extrajudiciales… nadie nos dice que nuestro informe no cabe finalmente sobre la mesa de un juez, sin olvidar que debe incorporar (en anexos generalmente) toda la información técnica suficiente para poder ser entendidas por un experto (que posiblemente haga una contrapericial).

El mejor consejo al respecto es dejarse llevar por la norma UNE 197001:2019. Criterios generales para la elaboración de informes periciales.

Tengamos en cuenta si es una pericial contratada por una de las partes de un juicio que no buscamos perjudicar a nuestros clientes, por lo que lo lógico es explicarles antes el informe, sus conclusiones y aclarar sus dudas. Puede que decidan no presentarlo si no les es favorable.

Una última cuestión: si finalmente deponemos ante el tribunal ¡seamos previsores! Preparemos no solo copia de todo, sino notas que nos ayuden (la justicia no siempre es todo lo rápida que sería deseable) a recordar todos los detalles y poder explicarlos ante un Tribunal.

Informe pericial de gestión

Vamos a darle una vuelta de tuerca. Con este apellido pasamos a hablar de esos informes periciales donde lo que buscamos es la obtención de evidencias del correcto cumplimiento con respecto a las responsabilidades contractuales implícitas y explícitas a distintos niveles tales como la calidad y la responsabilidad del trabajo.

Debemos considerar que cubre muchos campos, como, sin ánimo de completitud:

- gestión de proyectos
- prestación de servicios
- gestión de servicios
- gestión de clasificaciones profesionales o responsabilidades contractuales de los colaboradores
- casos sobre propiedad intelectual y propiedad industrial
- casos sobre protección de datos
- gestión de la seguridad informática
- revisión de estándares
- auditoría

En las recomendaciones de normas a consultar, hay un par de elementos que no se pueden olvidar: la UNE-EN ISO 9001:2015. Sistemas de gestión de la calidad. Requisitos (ISO 9001:2015)y la familia UNE-EN ISO/IEC 270000

Sobre la actuación de los peritos hay que hacer unas matizaciones con respecto a las páginas precedentes. Seguimos aplicando un ciclo de cinco fases, pero vamos a introducir unos cambios.

En este caso hablaremos de identificación, recopilación, análisis, informes, propuestas y recomendaciones. Vamos a verlas.

Identificación

De igual forma que en el caso anterior, precisamos conocer los antecedentes y todo lo que nos ilumine sobre el contexto: ¿por qué estamos estudiando esto? ¿Qué buscamos? En ese contexto que debemos tener claro entran las circunstancias comerciales, contractuales, técnicas, legales, organizativas, financieras, etc. del proyecto, así como los marcos de calidad y riesgos que se anticipaban (en cuanto a trabajos sobre protección de datos, si tenemos a mano las EIPD, mucho mejor). También conocer a los Stakeholders y los puntos calientes (hot points) de mayor prioridad identificados, que nos condicionarán la estrategia a seguir.

El punto de partida pasa por una llamada que nos hacen, precedida generalmente por un suceso anómalo. Esa llamada debe proceder de alguien con suficiente poder en la organización como para permitirnos acceso a lo que necesitemos y legitimar nuestro trabajo ante el resto de personas. De forma lo más rápida posible, debemos delimitar que se espera de nuestro trabajo, que, por otra parte, no debe ser coaccionado o intentado influenciar en sus resultados. A quien nos ha contratado (llamado) y solo a él debemos informar sobre nuestra investigación. Repito: informar, no pedir vientos favorables, no dejarnos influenciar por cantos de sirena. Obviamente, debemos conocer de forma previa las expectativas esperadas, qué objetivos se buscan, etc. Pero esto no es “influencia”, sino “ruta”.

Recopilación

Recogemos las e-evidencias que nos ayudarán a realizar el análisis, si es menester reconstruyendo los pasos de un proyecto. Es el momento de mayor contacto dentro de la organización, tanto con personas como con dispositivos. Para ello, en el paso anterior nos ha

tenido que quedar muy claro que es lo que estamos estudiando, que metodología se estaba aplicando, en que parte del ciclo de vida del proyecto estamos, si ha habido o no desviaciones frente a las previsiones originales, etc. Un trabajo, como se ve, arduo, pues cada entrevista, cada toma de datos, cada e-evidencia debe ser de forma minuciosa registrada con su origen, contenido, persona responsable, etc., autenticando estos documentos (hash) evitando posibles manipulaciones.

En el caso de entrevistas personales, en persona o a distancia, debemos no solo buscar eficacia sino perdurabilidad, de forma que lo que recojamos no pueda ser puesto en duda. Nos debe servir para ampliar la imagen del contexto que teníamos ya, con visiones sobre posibles conflictos o tensiones personales, cultura empresarial, etc.

Análisis.

De nuevo, estamos ante el eje de nuestro trabajo. Ya tenemos una perspectiva global y lo necesario para un estudio con detalle.

Con lo que tenemos podemos crear un **mapa cronológico de hitos** que nos permitirá (a nosotros y a futuros lectores) cómo porqué y de qué manera se ha llegado al punto actual.

Y casi podemos empezar. Pero antes **enumeraremos los puntos relevantes** para nuestro análisis. Esto es imprescindible, pues generalmente nos podemos ahogar en información irrelevante, que debemos saber focalizar destacando lo que realmente es importante.

Con el listado de las e-evidencias analizadas **resumimos los datos que obtenemos de cada una de ellas** para que luego podamos fácilmente reconocer la importancia y contenido de cada una. Podemos generar etiquetas o categorías.

Con esa información **crearemos un repositorio** que nos permita acceder rápida y efectivamente a la misma. Si hay relaciones entre ellas, deberemos tener una visión global de las mismas mediante cualquier técnica de organización de la información (una base de datos relacional, p.e.)

Una vez clara cuales son los documentos, e-evidencias claves, debemos comprobarlas. **Corroborar la exactitud del análisis**. No es lo mismo equivocarse en un fleco que en el eje de la investigación. Es el momento de verificar que nuestro trabajo está siendo correcto, no es perder el tiempo.

Y, ya con los elementos principales destacados, podemos ir verificando si esas hipótesis de partida se van cumpliendo, empezando por la **generación de conclusiones parciales**, lo que nos permitirá corregir la línea de argumentación de nuestro cliente si los hechos muestran que sus hipótesis eran erróneas. (p.e. pensábamos que Paquito filtraba datos a la competencia pero no, él no se ha comunicado nunca por ellos, pero si Jacinto)

Por último, nos queda obtener una **visión de conjunto**. Tenemos ya un lote de conclusiones parciales que juntas nos deben decir algo: ¿qué ha pasado en realidad?

Informes y Dictámenes

Lo ponemos todo negro sobre blanco. Las conclusiones de lo analizado, subrayadas por la información fundamental. Aquí hablaremos de distintos escenarios comparados: la situación actual (enfrentada a la que debería haber sido, la situación esperada), con la diferencia entre ambas, con una comparación que bien puede apoyarse en uno de los llamados "Gap Analysis".

Con respecto a la situación actual, se expone claramente, de forma conjunta a los antecedentes que han llevado hasta ella, junto a sus consecuencias. La visión es global, pero debe permitir profundizar en cada elemento que se desee.

La situación esperada es una visión realista de lo que debería haber pasado si no hubiera sucedido "eso" que ha provocado nuestra visita como peritos. Ojo, porque si los datos de partida están contaminados de optimismo, el resultado puede no ser muy realista. Y esto es peligroso, porque si la meta es establecer correcciones que nos lleven a esa situación, y esa situación es una utopía, estamos ante un imposible.

Nos quedan esas palabras raras, el Gap Analysis. Con el tratamos de proporcionar una visión de las diferencias entre los escenarios anteriores, subrayando lo que es posible de corregir todavía, los costes de esa corrección y los motivos si es imposible hacerlo. Si hacemos recomendaciones de cambio, deben partir de un tripe escenario: el peor, los mínimos imprescindibles, el medio, lo razonable y el mejor: la situación esperada.

Propuestas y recomendaciones

Casi lo tenemos con el Gap Analysis. Nos falta un estirón. Aquí se nos abren dos posibles caminos: corregimos o nos vamos a casa.

Continuidad.

Nos vamos. Pero nos vamos indicando que se debe hacer. Somos además de peritos consultores. Para ello podemos preparar una serie de herramientas de trabajo para nuestro cliente, que tomarán como base de partida nuestro trabajo previo. Vamos a orientar al cliente sobre como reconducir su problema.

Empezamos con un **mapa de objetivos**. Allí aparecerán, apoyados por un esquema gráfico, los distintos objetivos (de cualquier nivel) y nuestra propuesta para alcanzarlos minimizando lo que a la gerencia le interese más: tiempo o coste, indicando personas concretas, dispositivos afectados existentes o de compra nueva, suministros, etc., y con un análisis de costes y beneficios con relación de impacto en la organización. Se deben considerar así mismo riesgos, prerrequisitos, resistencias, barreras, previstas, como cuantificar y prevenir desviaciones y definir las contingencias para tomar las medidas

El siguiente paso es la creación de un plan de acción u **hoja de ruta**, que no es más que una relación de las acciones a realizar para para obtener los objetivos determinados. Esa relación será en extremo detallada con respecto a costes y recursos necesarios, relaciones y dependencias entre acciones, con su cronología y priorizaciones (pensemos en un PERT), impacto de cada una de ellas, responsables de cada una de ellas, etc.

Hemos de proponer unas medidas de seguimiento y control, generalmente verificables mediante **informes de seguimiento.** Estos informes los revisarán los comités de Dirección, Control y Seguimiento, que tendrán poder para decidir y resolver conflictos.

De forma optativa, dependiendo del volumen del trabajo, podemos aunar todo lo anterior de forma sintética en un **resumen ejecutivo** para la dirección, que de una visión concisa de nuestro trabajo como peritos.

Cierre.

Nuestro trabajo demuestra que seguir es un error. No es rentable, no es factible… esto a su vez puede enfocarse de tres maneras distintas:

Escenario de Cierre Ordenado:

Intentamos minimizar costes económicos, empleo de recursos, etc., generando un plan de trabajo para ello. Lo fundamental es ahorrar dinero y tiempo.

Escenario de Cierre Negociado:

Hay partes con intereses en conflicto y distintas pretensiones. Generalmente tras un consenso se llega a la situación anterior de cierre ordenado, pactando la estrategia a seguir y el plan de cierre. Lo fundamental es la calidad entre las relaciones de las partes.

Escenario de Cierre No Negociado:

Sálvese quien pueda. Vamos a juicio. Seguramente nuestro informe acabará en la mesa del juez.

Trabajo del perito como auditor

Dentro de los trabajos del perito de gestión puede que entre el ser llamado a efectuar tareas de auditor. Con respecto a temas relativos a la seguridad de datos personales, por ejemplo, que es una actividad al alza.

Verificar estándares y efectuar auditorías (o preauditorías) para que sean refrendadas por los organismos oficiales oportunos suele ser algo para lo que se recurre al perito, que debe revisar que no hay desajustes o ineficiencias, y emitir un informe con el detalle de su análisis con propuestas de cambio.

De normal los peritos hacemos uso de métodos de auditoría (volvemos a pensar en la protección de los datos personales o en el cumplimiento de normas UNE relativas a la seguridad informática)

En este tipo de métodos encaja también nuestro papel preparando los medios de prueba para un proceso judicial (derechos laborales, problemas con contratos, trabajos a entregar entregados: calidad, tiempos, cumplimiento de especificaciones…, violación de derechos de propiedad industrial o intelectual).