Universidad Carlos III de Madrid

Máster Universitario en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información

2014-2015

Trabajo Fin de Máster

"Informe sobre el Peritaje Informático"

José Luis García Gómez

Tutores

Manuel Huerta (Lazarus)

Mª Nieves de la Serna

Madrid, Julio de 2015

Palabras clave: peritaje dictamen pericial informático prueba electrónica cadena custodia evidencia digital análisis forense incidente seguridad

Resumen: Este trabajo presenta una perspectiva jurídica de los elementos característicos que intervienen actualmente en la realización de los peritajes informáticos, tanto en los distintos órdenes jurisdiccionales como en el ámbito extrajudicial, desde la identificación del motivo concreto que da origen al peritaje hasta la presentación y defensa del dictamen pericial en el acto del juicio ante el tribunal o ante la persona que lo ha solicitado. Se incide en las especialidades normativas de las fuentes de prueba utilizadas en las pericias informáticas y los pronunciamientos jurisprudenciales al respecto. El planteamiento jurídico del informe no pierde, sin embargo, de vista la perspectiva técnica que es necesaria para facilitar su mejor comprensión.

Contenido

Abreviaturas

ATS Auto del Tribunal Supremo

AAP Auto de la Audiencia Provincial

DEFR *Digital Evidence First Responder*

DES *Digital Evidence Specialist*

GPS *Global Positioning System*

IEC *International Electrotechnical Commission*

IETF *Internet Engineering Task Force*

ISO *International Organization for Standardization*

LEC Ley de Enjuiciamiento Civil

LECrim Ley de Enjuiciamiento Criminal

LJCA Ley Reguladora de la Jurisdicción Contencioso Administrativa

LRJS Ley Reguladora de la Jurisdicción Social

LSSI Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

PDA *Personal Digital Assistant*

PED *Personal Electronic Device*

RFC *Request For Comments*

RFID *Radio Frequency IDentification*

SAP Sentencia de la Audiencia Provincial

SGEE Sistema de Gestión de Evidencias Electrónicas

SGSI Sistema de Gestión de Seguridad de la Información

SMS *Short Message Service*

STC Sentencia del Tribunal Constitucional

STSJ Sentencia del Tribunal Superior de Justicia

STS Sentencia del Tribunal Supremo

UNE Una Norma Española

UTM *Universal Transverse Mercator*

1. Introducción

Desde hace tiempo, el Consejo General del Poder Judicial ha detectado la necesidad de que los Magistrados estén formados en un tema que cada día adquiere una mayor relevancia en el mundo judicial. Se trata del peritaje informático, en el que, como consecuencia de los importantes avances que las tecnologías están teniendo en las relaciones jurídicas, cada día son más los supuestos en los que se presentan dudas y cuestiones al respecto. Por esta razón, el Consejo General ha decidido solicitar a la empresa "TECNOLOG", especializada en este tema, que emita un informe sobre qué se entiende por peritaje informático y cuál es en este momento la situación del mismo. Con la difusión de dicho informe entre los distintos magistrados prtende crear un foro de discusión y dar a conocer la situación actual del peritaje informático, su significado, la normativa que lo regula, los aspectos prácticos a considerar, así como los pronunciamientos existentes respecto del mismo.

Actualmente, como destaca Gimeno Sendra, el dictamen de peritos, informe pericial o peritaje, como también se suele denominar, es considerado, en la práctica judicial del proceso civil, el medio de prueba de mayor relevancia junto con la prueba documental[1]. Pero su importancia adquiere una dimensión aún mayor cuando en la controversia intervienen aspectos técnicos de tipo informático, debido a la necesidad, ineludible en la mayor parte de las ocasiones, de aportar de manera inteligible los conocimientos técnicos específicos al caso que faciliten al juez la formación de su convicción. Algo similar ocurre en la jurisdicción social, en donde el uso cada vez mayor de equipos informáticos y comunicaciones telemáticas en las relaciones laborales provoca una mayor conflictividad, e, igualmente, aunque quizás en menor medida, en la jurisdicción contencioso-administrativa, si bien existe una perspectiva de su mayor relevancia en esta jurisdicción, como consecuencia de la aprobación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que ha provocado un incremento paulatino pero continuo de las relaciones por medios electrónicos de los ciudadanos con las Administraciones Públicas. Tampoco es posible dejar de mencionar la importancia que el informe pericial informático tiene en el proceso penal dado que

[1] Gimeno Sendra, Vicente. *Derecho Procesal Civil. El proceso de declaración. Parte General*. Colex 2010. 3ª edición, pág. 473

constituye un acto de investigación imprescindible en la instrucción de los cada vez más complejos y variados casos de delitos informáticos.

Finalmente, resulta también relevante destacar que los peritajes informáticos no sólo sirven como un medio de prueba en los distintos procesos judiciales. También este tipo de informes periciales tienen una relevancia en los procedimientos de arbitrajes o en las discusiones extrajudiciales, en donde su uso es solicitado por los intervinientes en ellas para alcanzar una solución acerca de los elementos controvertidos o también como paso preliminar para iniciar un posterior proceso judicial.

Establecida así la importancia creciente del peritaje informático tanto en el ámbito judicial como en el extrajudicial, en el presente informe que se solicita se procederá a exponer los elementos característicos de los peritajes informáticos desde el punto de vista de la práctica jurídica, pero sin perder la perspectiva técnica que subyace en ellos y que resulta necesaria para su mejor comprensión.

2. Concepto y tipos de peritaje informático

2.1. Concepto de peritaje informático

Siguiendo al profesor Gimeno Sendra, tomando como base el artículo 335.1 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), se define el dictamen pericial como "una actividad procesal mediante la que una persona o institución especialmente cualificada suministra al juez argumentos o razones para la formación de su convencimiento acerca de ciertos datos controvertidos, cuya percepción o comprensión escapa a las aptitudes comunes judiciales"[2].

En este sentido, si el peritaje es informático, se caracterizará por proporcionar al juez esos argumentos o razones acerca de los aspectos que resulten controvertidos en una determinada situación de un sistema informático y que tengan relevancia jurídica.

Para obtener tales razones y argumentos, el perito informático usa una rama de la Informática denominada Informática Forense, definida en la literatura anglosajona (*Computer Forensics*) como "la colección de técnicas y herramientas para encontrar evidencias en un ordenador" [3], y también, de una manera algo más exhaustiva, como "la ciencia de adquirir, preservar, recuperar y presentar datos que han sido procesados electrónicamente y almacenados en un sistema informático"[4]. En dicha literatura se distingue la Informática Forense (*Computer Forensics*) como una rama diferenciada de lo que podríamos traducir por Electrónica Digital Forense (*Digital Forensics*), que define como "el uso de métodos científicamente derivados y comprobados para la preservación, adquisición, validación, identificación, análisis, interpretación, documentación y presentación de evidencias digitales derivadas también de fuentes digitales con el propósito de facilitar o promover la reconstrucción de eventos de carácter criminal o de ayudar a anticiparse a acciones no autorizadas que puedan perturbar operaciones planificadas"[5]. Esta última rama comprende una gama más amplia de dispositivos, abarcando en ella no sólo los ordenadores en sentido estricto, sino cualquier variedad de dispositivo digital, como *smartphones* o *wearables*, incluidos

[2] Ibidem, Gimeno Sendra 2010, pág. 473
[3] Caloyannides, Michael A. *Computer Forensics and Privacy*. Artech House Inc. 2001
[4] Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley. *Recovering and examining computer forensic evidence* October 2000. Volume 2, Nr 4
[5] M Reith, C Carr, G Gunsch. *An examination of digital forensic models*. International Journal of Digital Evidence. 2002, pág. 2

también los equipos de redes telemáticas, como *routers* o *firewalls*. Por otra parte, es fundamental que los métodos utilizados sean aceptados y permitan la repetibilidad de los procesos que llevan al resultado para que éste sea considerado medio de prueba válido.

Al margen de la nomenclatura anglosajona anterior y dado que en nuestra literatura se suelen emplear los términos "Informática Forense" de manera generalizada y en sentido amplio, se va a utilizar dicha expresión para referirse al análisis forense de todo tipo de dispositivo digital, incluido el equipamiento de redes de comunicaciones telemáticas.

Dicha disciplina tiene evidentes puntos en común con la Seguridad Informática, ya que su aplicación consiste en ocasiones en el análisis forense posterior a la manifestación de un incidente de seguridad, de tipo delictivo o no, en un sistema informático o en prevención de un posible ataque. Así, cuando una empresa contrata un servicio de Informática Forense puede perseguir bien un objetivo preventivo, para tratar de anticiparse a un posible problema de seguridad o para auditar que los mecanismos de seguridad instalados en los sistemas de información son idóneos, o bien un objetivo correctivo, para recopilar las evidencias y encontrar la solución más adecuada tras ocurrir el incidente de seguridad.

No obstante, hay que resaltar que la Informática Forense no siempre guarda relación con problemas de seguridad, ya que en muchas ocasiones la búsqueda de evidencias digitales puede tener fines probatorios de índole civil, como certificar veracidad, reconstrucción de hechos, existencia e inexistencia de datos, por ejemplo, en la prueba de la existencia de un contrato electrónico o de una actuación mercantil de competencia desleal. Todo ello, dejando además al margen otros usos que no derivan de incidentes de seguridad ni de controversias y que tienen como finalidad obtener diversos conocimientos técnicos acerca de situaciones concretas en un determinado sistema informático, si bien en estos casos, tal peritaje no constituiría obviamente un medio de prueba judicial o extrajudicial, sino una mera investigación privada.

A pesar de los esfuerzos y de los resultados alcanzados en la estandarización de la metodología a emplear en la Informática Forense, la realidad es que actualmente no existe un único estándar metodológico de amplia aceptación. Los estándares existentes

se han definido habitualmente de forma abstracta para elaborar métodos de trabajo que no resulten dependientes de la utilización de una tecnología informática en particular o de un determinado delito informático o cibercrimen. Tampoco existe un estándar homologado a nivel nacional para la certificación y acreditación de un especialista en la materia como perito informático.

No obstante, a pesar de las dificultades mencionadas, la realidad es que la Informática Forense es una disciplina pujante en la que existe una importante comunidad de desarrolladores, tanto dentro de empresas como organizados autónomamente, que incorporan de forma continuada nuevas herramientas de análisis y nuevos procedimientos.

2.2. Tipos de peritaje informático

Recordemos que, como se ha mencionado en el capítulo de Introducción, una primera clasificación tipológica del peritaje informático consiste en diferenciar:

- peritaje judicial, es decir, aquel que se lleva a cabo como medio de prueba dentro de un proceso judicial.
- peritaje extrajudicial, que a su vez puede ser:
    - aportado a un arbitraje
    - un instrumento para alcanzar en un litigio extraprocesal una solución por autocomposición entre los intervinientes
    - una fase preliminar para el estudio de una posible demanda judicial posterior

Por otra parte, dentro del peritaje informático judicial existen dos casos diferenciados:

- De parte, en el que el perito es designado por una de las partes intervinientes en el proceso, como es el caso habitual en el proceso civil o laboral.
- De oficio, en el que el perito es designado por el juez, caso habitual en el proceso penal.

Dentro del peritaje de parte, aunque no sólo en él, es frecuente encontrar una tipología de peritaje informático caracterizada por su contenido crítico respecto a otros peritajes, tales como:

- Contraperitaje informático: consistente en el análisis crítico de las conclusiones de otro informe pericial informático, normalmente presentado por la contraparte en el litigio, de forma que se reflejan sus errores de hecho o deductivos para, finalmente, rebatir dichas conclusiones.
- Metaperitaje informático: consistente en analizar otro peritaje informático desde un punto de vista pericial o, lo que es lo mismo, realizar un peritaje sobre otro peritaje informático. Su objetivo suele ser demostrar la falta de rigor técnico o metodológico del peritaje analizado para poner en tela de juicio su validez como prueba.

Asimismo, es posible distinguir distintos tipos de peritaje informático en base a la función llevada a cabo en ellos[6]:

- Peritaje forense informático, cuya función es obtener evidencias de la información digital encontrada en los dispositivos informáticos y confeccionar los medios de prueba correspondientes, tanto si se presentan ante el juez o no. Este es el tipo de peritaje informático que es el objeto principal de este trabajo.
- Peritaje tecnológico de gestión, cuya función es la obtención de evidencias relacionadas con el cumplimiento de las responsabilidades contractuales asumidas por las partes en cuanto a niveles de calidad o niveles de servicio. Su ámbito de actuación es por ello, la gestión y explotación de proyectos, de servicios o de colaboraciones empresariales, la consultoría y la auditoría informática, etc.
- Peritaje tecnológico de mediación, cuya función es la resolución de modo amistoso entre dos o más partes, de controversias relacionadas con las Tecnologías de la Información y de las Comunicaciones u otras tecnologías.
- Tasación tecnológica, cuya función es la valoración de bienes tangibles o intangibles de tipo informático en base a normativas y procedimientos establecidos.

[6] López Rivera, Rafael. *Peritaje Informático y Tecnológico. Un enfoque teórico-práctico*. 2012, pág. 45 y ss.

3. Realización de un peritaje informático

3.1. Análisis forense y obtención de evidencias

La obtención de evidencias digitales mediante la realización de un análisis forense supone una actividad compleja que se ha tratado de estandarizar sin excesivo éxito a lo largo de los últimos 20 años. Han sido muchos las propuestas realizadas a nivel internacional, intentando hacer frente al continuo crecimiento y diversidad de los delitos digitales, para desarrollar una metodología que permita definir un marco de actuación estándar y que tenga la consistencia necesaria para llevar a cabo una investigación forense en un dispositivo digital. No existe un consenso para elegir ninguno de estos marcos en concreto, debido a que cada metodología propuesta tiene sus ventajas e inconvenientes. No obstante, como por otra parte es lógico, las diferencias entre ellas no son absolutas, consistiendo en ocasiones simplemente en diferencias de denominación de los diversos pasos o actividades que integran el modelo de realización del análisis forense o en aglutinar algunos de ellos.

Teniendo en cuenta lo anterior, se van a detallar a continuación los pasos a seguir para la realización de un análisis forense, de forma independiente de cualquier tecnología y de cualquier delito informático en concreto, tomando para ello como referencia básica, por su detalle descriptivo sin pérdida de generalidad, el modelo de actuación definido por Reith y otros[7].

3.1.1. Identificación del incidente

Consiste en la detección por cualquier medio de la existencia de un incidente acaecido en un dispositivo digital y en la determinación, a través de los indicios existentes, del tipo de incidente de que se trata. Este paso inicial no forma parte en sí mismo del campo forense, pero es relevante por su influencia en los pasos siguientes.

3.1.2. Preparación del análisis

Consiste en disponer las herramientas y técnicas con las que se va a llevar a cabo el análisis forense, así como en la obtención de las autorizaciones necesarias para llevar a cabo las monitorizaciones y búsquedas que sean precisas.

[7] M Reith, C Carr, G Gunsch. *An examination of digital forensic models*. International Journal of Digital Evidence. 2002. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.9683

3.1.3. Estrategia de aproximación

Se trata de definir de forma dinámica la manera de acometer el análisis mediante una buena comprensión de la situación que permita definir la mejor estrategia de definición de fuentes, evidencias y procedimientos, teniendo en cuenta la tecnología concreta de que se trata y la reducción en la medida de lo posible del impacto sobre los usuarios del sistema digital sobre el que se va actuar. La estrategia debe tener como objetivo maximizar la recogida de evidencias digitales que no hayan sufrido alteraciones después del incidente digital, al tiempo que se minimice el impacto sobre las victimas de dicho incidente.

Este paso es normalmente realizado de forma simultánea e interactiva con la actividad de preparación anterior.

3.1.4. Preservación de las evidencias

Tiene por objeto aislar, asegurar y preservar el estado de las evidencias existentes tanto desde el punto de vista físico como de su contenido digital. La actividad a llevar a cabo incluye impedir el uso de cualquier dispositivo digital que contenga evidencias, idealmente desde el mismo momento en que se haya producido el incidente digital, evitando igualmente su apagado, así como el uso de otros dispositivos electromagnéticos, como es el caso de equipos con interfaz WiFi, dentro del radio de influencia en el que puedan acceder o afectar a aquéllos.

3.1.5. Recopilación de evidencias

Consiste en llevar a cabo la grabación de la escena física y el duplicado de las evidencias digitales, utilizando para ello procedimientos que hayan sido aceptados y estandarizados, de forma que los jueces puedan confiar en que son fiables y satisfacen los requisitos exigidos.

El objetivo es preservar las evidencias originales inalteradas, mediante el bloqueo electrónico de la escritura en el dispositivo origen, y manipular únicamente los duplicados durante su posterior examen y análisis.

3.1.6. Examen

Se trata de realizar una búsqueda sistemática y en profundidad de evidencias que estén relacionadas con el incidente digital que se ha identificado previamente durante el reconocimiento llevado a cabo en el primer paso.

Evidencias típicas son, por ejemplo, contraseñas, archivos borrados, tráfico de red, registros del sistema, etc. Suele ser fundamental el establecimiento del *timeline* de estas evidencias para permitir la reconstrucción histórica de los hechos.

3.1.7. Análisis

Se debe determinar la importancia de cada una de las evidencias, reconstruir los diversos fragmentos de información extraída y establecer las conclusiones basadas en las evidencias encontradas. La determinación de una concreta teoría que explique el incidente digital ocurrido puede requerir varias iteraciones sucesivas de actividades de examen y análisis.

Para llevar a cabo la actividad de análisis puede que no se requieran grandes habilidades técnicas, por lo que puede haber más personas participando en ella. También puede ocurrir que el caso sea multidisciplinar y requiera distintos tipos de especialidades para abordar el análisis.

3.1.8. Presentación

Se trata de detallar con la exhaustividad necesaria el proceso de análisis con los resultados obtenidos desde el punto de vista técnico, de forma que se dote al informe de rigor y consistencia frente a una posible futura impugnación.

Además, se debe de aportar un resumen, habitualmente en el apartado de conclusiones, con la explicación, en términos no técnicos, de los resultados extraídos del análisis de las evidencias y de la reconstrucción del incidente digital, usando una terminología abstracta que haga referencia a los detalles específicos y que pueda ser empleada ante un tribunal.

3.1.9. Devolución de las evidencias

Tiene como objeto la devolución, en su caso, a sus propietarios de los dispositivos físicos así como de sus contenidos digitales, determinando qué evidencias generadas por el incidente deben ser eliminadas y cómo realizar dicha eliminación. Esta devolución también puede ocurrir en el propio acto de adquisición de evidencias, ya que, en ocasiones, no se puede retirar la evidencia por afectar a sistemas de producción.

Como en el caso de la actividad de identificación llevada a cabo en el primer paso, no tiene en sí misma carácter forense.

3.2. Almacenamiento seguro e inalterable

Para lograr la convicción del juez frente a la prueba pericial presentada, tan importante como elaborar un buen informe pericial, es garantizar que las evidencias digitales encontradas han sido almacenadas de forma segura y sin posibilidad de alteración, o, como también se suele expresar en términos forenses, que se ha mantenido la cadena de custodia.

Se puede definir la cadena de custodia como el proceso utilizado para documentar la historia cronológica de una prueba, con el objetivo de convencer al tribunal de que es razonablemente probable que la exposición sea auténtica así como de que nadie ha alterado la prueba[8].

La garantía básica de inalterabilidad se documenta y consigue mediante la huella digital o función hash obtenida de cada evidencia digital, de manera que siempre se pueda comprobar a posteriori el hash original.

Para probar adicionalmente la historia cronológica de la cadena de custodia de una evidencia digital, es necesario conocer cómo se ha manejado dicha evidencia a lo largo del tiempo, dejando constancia de forma documentada en cada paso de "quién, qué, cuándo, dónde, por qué y cómo"[9] la ha manejado, pudiendo resultar para ello necesaria en algunos casos la presencia de un notario o de un secretario judicial.

Un modelo conceptual de referencia, propuesto[10] para reflejar dicha constancia, consiste en la realización y registro de datos obtenidos de las siguientes cuatro actividades, que a su vez son las que se corresponden punto por punto con las respuestas a cuatro de las seis preguntas anteriores: qué, quién, cuándo y dónde.

3.2.1. Qué contenido tiene la evidencia digital

La forma propuesta de certificar el contenido, es decir, el "qué" de la evidencia digital bajo custodia, diferenciándola así de otros contenidos digitales, consiste en obtener su huella digital mediante la aplicación de una función hash, en concreto la función estándar SHA-2, que permite obtener una cadena de longitud fija, habitualmente de 256

[8] Marqués-Arpa, Tomás. *Cadena de Custodia en el Análisis Forense*. RECSI 2014, pág. 167

[9] Las cinco Ws y una H en idioma inglés correspondientes a la vieja fórmula empleada en las investigaciones policiales

[10] Cosic, Jasmin. *A Framework to (Im)Prove Chain of Custody in Digital Investigation Process*. Proceedings of the 21st Central European Conference on Information and Intelligent Systems, 2010

bits, como huella digital independientemente del tamaño de la evidencia. Alternativamente, puede utilizarse la función MD5, de 128 bits, más sencilla y rápida.

De esta forma, es posible representar la evidencia digital por su función hash en cualquiera de las actuaciones de la cadena de custodia, en lugar de tener que utilizar para ello el contenido completo de la evidencia digital original.

3.2.2. Quién es responsable de la evidencia digital

Para dejar constancia cierta acerca de quién ha manejado la evidencia digital en un momento determinado de su historia cronológica, es preciso realizar su autenticación e identificación al acceder ella.

Para ello, se ha propuesto la utilización de técnicas biométricas como la mejor manera de llevar a cabo dicha autenticación, ya sea mediante reconocimiento de iris, de huella digital o del rostro, aunque quizás resulte exigente en exceso y sólo aplicable en casos de seguridad nacional. Esta técnica de autenticación requiere además la existencia previa en una base de datos de las características biométricas de todas las posibles personas con posibilidad de manejar evidencias.

Una manera de mejorar incluso, en caso necesario, la garantía de dicha autenticación, utilizada en ocasiones en sistemas de análisis complejos en los que intervienen varios analistas o peritos, consistiría en añadir un certificado electrónico de la persona y, adicionalmente, una contraseña personal de acceso. De esta forma, para facilitar el acceso a la evidencia digital, se requeriría comprobar tres puntos: algo que la persona es, su característica biométrica, algo que tiene, su certificado electrónico, y algo que conoce, su contraseña de acceso.

3.2.3. Cuándo se ha realizado la actuación

La actividad a llevar a cabo consiste en dejar constancia, siguiendo el procedimiento establecido en la recomendación RFC 3161, del momento temporal en que se produce tanto el descubrimiento de la evidencia como cada una de las posteriores actuaciones de acceso a ella, mediante una estampación digital de la fecha y hora corrientes emitida por una Autoridad de Certificación, actuando como Autoridad de Sellado de Tiempo, y que interviene como tercero de confianza. De esta manera, la Autoridad de Certificación

cumple con el requisito, necesario en este sistema de marcado de tiempos, de que existan auditores externos actuando como testigos.

Como es sabido, en España se emplea como Autoridad de Sellado de Tiempo, según establece el Real Decreto 1308/1992, de 23 de octubre, el Real Instituto y Observatorio de la Armada de San Fernando (Cádiz).

3.2.4. Dónde se ha realizado la actuación

Para determinar el lugar exacto en el que se realiza una determinada actuación sobre una evidencia digital, se ha propuesto la utilización de sistemas de geolocalización, como GPS, de los que actualmente disponen ya la mayoría de dispositivos electrónicos. De esta forma, se pueden leer, directamente del dispositivo, las coordenadas de geolocalización y registrarlas en los datos que acompañan al hash de la evidencia digital correspondientes a la actuación realizada sobre ella.

Otra forma alternativa de hacer un seguimiento y poder localizar una evidencia digital consiste en utilizar una etiqueta RFID, aunque dicho sistema no permite la obtención de coordenadas absolutas de localización, por lo que es preferible el uso del sistema anterior basado en GPS.

3.2.5. Cifrado asimétrico por el responsable de la cadena de custodia

Conforme al proceso expuesto anteriormente, para cada actuación realizada sobre la evidencia digital existirá un valor hash correspondiente a la evidencia, junto con unos datos de autenticación biométricos, un sello de tiempo y unas coordenadas de geolocalización, además de otros posibles datos acerca del cómo y del porqué de la actuación.

Para fortalecer la seguridad de los datos anteriores, se ha propuesto su cifrado asimétrico con la clave privada correspondiente al certificado electrónico emitido por una Autoridad de Certificación para el responsable de la cadena de custodia.

El resultado de dicho cifrado deberá almacenarse para su uso posterior tendente a demostrar ante el tribunal, o ante la persona física o jurídica que requiera dicha demostración, el mantenimiento de la cadena de custodia sobre la evidencia digital obtenida.

4. Normativa relacionada con el peritaje informático. Derecho Probatorio

El peritaje informático está regulado por la normativa procesal correspondiente a la prueba pericial en general establecida dentro de los diversos órdenes jurisdiccionales. No existe, por tanto, ninguna especialidad en el tratamiento normativo dado a la pericia informática respecto al del resto de pericias. De esta manera, es posible decir que el peritaje informático es, desde el punto de vista de su tratamiento procesal, un peritaje más: el momento y la forma de aportación del dictamen pericial al proceso, su valoración por el juez, las obligaciones y las condiciones del perito, su posible tacha o recusación o su posible actuación en el juicio, se rigen por las mismas reglas que cualquier otro tipo de peritaje.

Así, las distintas normas procesales aplicables en cada caso son:

a) En el orden civil, la LEC establece el tratamiento general a dar a los dictámenes de peritos en la Sección 5ª del Capítulo VI, dentro del Título I correspondiente al Libro II, artículos 335 a 352.
b) En el ámbito de la jurisdicción contenciosa administrativa, la LEC es en este tema de plena aplicación, dado que la Ley Reguladora de la Jurisdicción Contencioso-Administrativa (LJCA) remite, en su artículo 60.4, el desarrollo de las pruebas en el proceso contencioso administrativo a las normas generales establecidas para el proceso civil.
c) En el ámbito laboral, la regulación de la prueba pericial se encuentra en el artº 93 de la Ley 36/2011 Reguladora de la Jurisdicción Social (LRJS), si bien su disposición final 4ª establece que, para lo no previsto en la propia Ley, regirá como norma supletoria la LEC.
d) Por último, en el orden penal la Ley de Enjuiciamiento Criminal (LECrim) regula lo relativo al informe pericial en el Capítulo VII del Título V, dentro del Libro II correspondiente al Sumario, artículos 456 a 485, y en la Sección 3ª del Capítulo III, dentro del Título 3º del Libro III correspondiente al Juicio Oral, artículos 723 a 725.

En todo caso, corresponde advertir que debido a la ausencia de especialidades en dichos tratamientos para la pericia informática, no se considera pertinente incidir en el detalle de dicha normativa.

Por el contrario, es necesario señalar que donde sí que aparecen especialidades normativas es en lo referente a las fuentes probatorias que son utilizadas como base material en las pericias informáticas, es decir, las evidencias digitales obtenidas del incidente de seguridad. El motivo de dichas especialidades lo constituyen las características particulares de las fuentes de prueba digitales, especialmente su volatilidad y su facilidad de replicación y alteración, que las distingue del resto de fuentes de prueba utilizadas en otro tipo de pericias y, en particular, de las fuentes de prueba documentales.

Por este motivo, se va a exponer a continuación el Derecho Probatorio relacionado con el peritaje informático, es decir, el tratamiento procesal aplicable a las fuentes de prueba digitales una vez que ya son aportadas al proceso, pasando por lo tanto a convertirse en medios de prueba.

En los siguientes apartados, se va a sustituir en muchas ocasiones el adjetivo "digital" por "electrónico" para tratar de adaptarse a la nomenclatura[11] utilizada habitualmente tanto por el legislador como por la doctrina para referirse a conceptos tales como "prueba electrónica" o "documento electrónico", entre otros.

4.1. La prueba electrónica: trámite procesal

El concepto de prueba electrónica no aparece definido en la legislación española. No obstante, sí que existe una definición sobre este concepto procedente de la normativa europea. En concreto, de la Decisión 2002/630/JAI del Consejo, de fecha 22 de julio de 2002, relativa a la creación del programa marco para la cooperación policial y judicial en materia penal (AGIS), en el que se define la prueba electrónica como "la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho". También define los medios de prueba electrónicos como "los soportes técnicos que recogen la prueba electrónica".

[11] Sería deseable un mayor rigor para distinguir los conceptos de electrónico, digital e informático, términos técnicos que no son equivalentes y cuyo uso indistinto puede inducir a errores de interpretación

En relación con el derecho fundamental a la prueba electrónica, es posible encontrar el fundamento en el artículo 24 de la Constitución Española que, como es sabido, reconoce a todos el derecho "a utilizar los medios de prueba pertinentes para su defensa", lo que ha permitido al legislador de los diversos órdenes jurisdiccionales introducir nuevas categorías de medios de prueba, al margen de los tradicionales, entre los que lógicamente se encuentra la prueba electrónica.

4.1.1. Ámbito civil

Dentro del orden civil, la LEC ha ampliado la lista de medios tradicionales de prueba con nuevos medios de prueba propiciados por los avances científicos o tecnológicos[12]. Así el artº 299.2 establece dos de estos nuevos medios con una sustantividad propia: los medios de prueba audiovisuales, a los que se refiere como "medios de reproducción de la palabra, el sonido y la imagen", y los medios de prueba en soportes informáticos, reflejados como "instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas".

Tanto a uno como a otro, la LEC les diferencia de los medios de prueba documentales, atribuyéndoles una valoración por el juez según las reglas de la sana crítica en lugar de su sometimiento a las reglas de la prueba documental. Esta diferenciación ha sido fuertemente contestada por parte de la doctrina, que considera la equivalencia funcional entre una declaración de voluntad plasmada en documento electrónico y la misma reflejada en un documento en papel, estimando que "las previsiones legales de la norma procesal común hayan devenido escasamente operativas en la materia que nos ocupa, arrolladas por una aplastante realidad social … La actividad cotidiana de nuestros tribunales, bien de oficio, bien a través de las alegaciones y/o iniciativa de las parte, está supliendo en muchos casos las aparentes carencias de la ley por vía de asimilación a la prueba documental"[13], si bien, como puntualiza Illán Fernández[14], al menos el artº 318 de la LEC sí que otorga la fuerza probatoria de documento público, es decir valor tasado legal, fuera por ello de la valoración según la sana crítica, a los documentos públicos electrónicos.

[12] Illán Fernández. *La Prueba Electrónica, Eficacia y Valoración en el Proceso Civil*. 2009.pág. 229
[13] Pérez Gil, Julio. *Prueba electrónica y prueba documental en el proceso civil: los límites de su equivalencia funcional*. Suplemento de Derecho Procesal de ElDial.com. 2006
[14] Illán Fernández, pag. 259

Sin embargo, existen dos normas legales sustantivas que atribuyen a estos medios de prueba, en determinados casos, naturaleza de prueba documental: La Ley 59/2003 de Firma Electrónica, para los soportes en que se hallen datos firmados electrónicamente, y la Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI), para "el soporte electrónico en que conste un contrato celebrado por vía electrónica".

Un aspecto importante en cuanto a su incidencia en el peritaje informático, es que la LEC permite (artº 382.2 y 384.2) a la parte que proponga estos medios de prueba, "aportar los dictámenes y medios de prueba instrumentales que considere convenientes", pudiendo las demás partes del proceso, "con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga". En el caso de los medios de prueba en soportes informáticos, la documentación de autos se hará del modo más apropiado al medio de prueba y bajo la fe del Secretario Judicial que adoptará las medidas de custodia necesarias. Con esta previsión legal, el peritaje informático adquiere una nueva dimensión, no ya como medio de prueba en sí mismo, sino como apoyo a los medios de prueba en soportes informáticos propuestos por las partes.

4.1.2. Ámbito penal

Es en el orden penal donde la prueba electrónica se erige de forma paradigmática como el elemento esencial que sirve de base para la formación de la convicción del juez cuando se sigue una causa por algún delito informático. Pero también, al margen de los delitos informáticos, la prueba electrónica puede ser utilizada para acreditar hechos en cualquier proceso abierto para la investigación de todo tipo de infracciones penales.

El legislador del Código Penal de 1995, a diferencia del legislador procesal civil, sí dio una carácter documental al documento electrónico al recoger en su artº 26 que "se considera documento todo soporte material que exprese o incorpore datos, hechos, o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica". Por tanto, cualquier soporte material, y los soportes electrónicos de cualquier tipo lo son, será un documento a efectos probatorios penales cuando contenga datos, hechos o narraciones con eficacia probatoria o relevancia jurídica, haciendo posible su examen por el tribunal como prueba documental según dispone el artº 726 de la LECrim[15].

[15] Gimeno Sendra, Vicente. *Manual de Derecho Procesal Penal*. Colex. 2010. 2ª edición, pág. 424

Pero esta Ley no recoge ninguna regulación específica acerca de la prueba electrónica ni de sus garantías, lo que ha sido denunciado por parte de la doctrina que reclama que una "nueva Ley de Enjuiciamiento Criminal proceda a regular expresamente el acceso a la información contenida en dispositivos electrónicos y su incorporación al proceso penal, eliminando incertidumbres con pleno respeto a las garantías del proceso, especialmente cuando puedan verse afectados derechos fundamentales de las personas"[16], solicitando al tiempo que esa regulación legal se complemente con una normativa reglamentaria "que regule aspectos tales como las formas de acceso a las pruebas electrónicas, las singularidades de la cadena de custodia con la finalidad de garantizar su autenticidad e integridad y diferentes cuestiones sobre la realización de la prueba pericial informática, entre otras." En esta misma línea de necesidad de una clarificación legislativa, se ha denunciado la imposibilidad de diferenciar entre original y copia de un documento electrónico y la repercusión que esto tiene sobre su valor probatorio, al tener fuerza probatoria plena solamente el original, así como sobre la ausencia de delito de falsedad documental en caso de alteración de una copia electrónica, lo que simplemente constituiría un engaño[17].

Con relación a esta reclamación doctrinal de novedades legislativas, cabe mencionar el Proyecto de Ley Orgánica de modificación de la LECrim, recientemente aprobado por el Congreso de Diputados[18] y cuya tramitación está pendiente en el Senado, que recoge novedades en las siguientes medidas de investigación tecnológica, requiriendo de forma preceptiva para todas ellas la autorización judicial que las valorará según los principios de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad:

- Se amplía la interceptación de comunicaciones, que afectará a servicios de la Sociedad de la Información, como WhatsApp, a SMSs y a escuchas ambientales.
- Registro de dispositivos de almacenamiento masivo de información bajo los términos y alcance fijados por el juez, que podrá autorizar la realización de copias informáticas con las condiciones necesarias para asegurar la integridad de los

[16] Delgado Martín, Joaquín. *La prueba electrónica en el proceso penal*. Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, pág. 2
[17] Bacigalupo, Enrique. *El delito de Falsedad Documental*. Ed. Dykinson, Madrid, 1999. pág. 13
[18] 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

datos y las garantías de su preservación que hagan posible, en su caso, la práctica de un dictamen pericial y su repetibilidad.

- Registros remotos sobre equipos informáticos únicamente para determinados delitos bajo las condiciones fijadas por el juez en cuanto a delimitación de equipos objetos del registro, forma de acceso, autorización de copias y medidas de preservación de los datos, así como, en su caso, de su inaccesibilidad o supresión.

4.1.3. Ámbito contencioso-administrativo

Como hemos adelantado, según lo dispuesto en el artº 60.4 de la LJCA, la prueba se regirá por las reglas generales establecidas para el proceso civil, por lo que cabe aplicar a este orden todo lo anteriormente expuesto en relación a la prueba electrónica en el orden civil, no siendo mencionable ninguna especialidad al respecto.

Al margen del proceso judicial y en relación con el procedimiento administrativo, cabe decir que la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, ya estableció en su día de forma pionera la validez del documento electrónico al establecer que "los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes", anticipándose así a su recepción por parte de otras normas legales.

4.1.4. Ámbito laboral

Por su parte, la LRJS admite en su artº 90 que las partes puedan valerse de cuantos medios de prueba se encuentren regulados en la ley incluidos los de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos. En esta lista abierta de medios de prueba, en la que se incluyen los medios de archivo y reproducción de datos, puede incluirse a priori sin ninguna dificultad cualquier tipo de prueba electrónica.

No obstante, el artículo citado de la LRJS incluye explícitamente un límite para la obtención de la prueba: que no suponga violación de derechos fundamentales o libertades públicas. Se trata de un límite sin duda evidente y aplicable en cualquier otro orden jurisdiccional, pero que probablemente el legislador ha incluido explícitamente para resaltar su importancia en el ámbito laboral por la facilidad con que puede ser vulnerado, en especial en cuanto a la necesidad de salvaguardar el derecho a la intimidad y protección de datos de carácter personal del trabajador. En relación con ello, cuando se requiere investigar en el ordenador utilizado por un trabajador, es habitual emplear el método denominado de "búsquedas ciegas" consistente en filtrar la búsqueda de ficheros mediante unas palabras clave proporcionadas por el contexto de la investigación, con objeto de que sean analizados solamente aquellos ficheros que contengan dichas palabras clave, descartándose así cualquier contenido que no guarde relación con el caso investigado.

Otro derecho cuya salvaguarda debe atenderse especialmente en este ámbito es el de la tutela judicial efectiva en relación con la igualdad de armas entre empresario y trabajador, debido a la diferencia existente entre ellos por regla general en cuanto a la facilidad de uno y otro para acceder a las fuentes de prueba electrónicas que le puedan favorecer en el litigio.

Asimismo, para evitar la posible declaración posterior de una prueba electrónica como ilícita, el apartado 4 del citado artículo prevé la solicitud de autorización al juez para el acceso a archivos electrónicos, que éste podrá conceder tras ponderar los intereses afectados. En el auto de autorización determinará las condiciones de acceso, las garantías de conservación y aportación al proceso, la obtención y entrega de copias, así como la intervención de las partes o de sus representantes y expertos, en su caso.

Puede decirse, en conclusión, que la atención especial a la garantía de los derechos fundamentales del trabajador es quizás la especialidad más relevante que presenta la prueba electrónica en lo referente al orden social.

4.2. Conservación y custodia

Como ya se ha indicado en el apartado del capítulo anterior relativo al modelo metodológico propuesto para dejar constancia de la cadena de custodia, la conservación

y custodia adecuadas de los soportes digitales que van a servir de base fáctica para la prueba electrónica son de especial importancia para poder acreditar ante el juez su autenticidad, dada la fragilidad de la información digital. Deberá garantizarse por ello, tanto la perdurabilidad como la fidelidad de los soportes digitales custodiados, de forma que estén disponibles de forma permanente y que su contenido responda fielmente al obtenido sin que haya podido resultar posteriormente alterado.

Desde el punto de vista normativo, no existen apenas prescripciones concretas que arrojen luz sobre la forma y requisitos que deben de cumplir dicha conservación y custodia.

Con carácter general, la LEC en su artº 148 otorga a los secretarios judiciales la responsabilidad de la conservación y custodia de los autos en general y, en relación concreta con los "instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas", es decir, las evidencias digitales, el artº 384.2 prescribe que la documentación de autos se hará de la forma más apropiada a la naturaleza del instrumento, bajo la fe del secretario judicial, que adoptará, en su caso, las medidas de custodia necesarias.

El nuevo Proyecto de Ley de modificación de la LECrim dispone que, en caso de registro de dispositivos de almacenamiento masivo de información, el juez "fijará las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial" y, en caso de un registro remoto sobre equipos informáticos, la resolución judicial que lo autorice "deberá especificar las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso". Asimismo, realiza unas previsiones acerca de la conservación de los registros electrónicos tras la sentencia firme del proceso, disponiendo que se borrarán y eliminarán los registros originales, conservándose una copia bajo custodia del secretario judicial hasta que se cumplan "cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito".

En el mismo sentido, la LRJS, en su artº 90.4, establece que el juez determinará las garantías de conservación y aportación al proceso de los archivos electrónicos para los que haya autorizado el acceso.

En conclusión, las previsiones legales utilizan expresiones genéricas tales como "medidas precisas" o "condiciones necesarias" para garantizar la conservación e integridad de la información digital obtenida, pero no establecen ninguna concreción adicional sobre el contenido de dichas medidas de custodia, por lo que la aceptación en el juicio de la fuente de prueba custodiada quedará a la valoración del juez según las reglas de la sana crítica.

Ante esta ausencia de concreción legislativa y en tanto no sea corregida con nuevas aportaciones normativas, es necesario acudir al análisis jurisprudencial para tratar de determinar con una mayor precisión los criterios generales de aceptación en juicio de la prueba electrónica.

5. Jurisprudencia

Las carencias regulatorias sobre el peritaje informático expuestas en el capítulo anterior y, en particular, sobre las fuentes probatorias con las que opera habitualmente, hacen que la jurisprudencia deba de ocupar en este caso un lugar aún más importante del que normalmente le corresponde a la hora de completar dichas carencias en las leyes procesales.

5.1. Jurisprudencia Constitucional

Lo primero que es preciso destacar es que los pronunciamientos respecto de este tema por parte del Tribunal Constitucional, son muy escasos. En la mayoría de los casos en que el tema de la pericia informática ha llegado al Alto Tribunal, su tratamiento sobre el fondo del asunto es marginal, por lo que no es posible extraer de dichas sentencias criterios importantes. No obstante, a continuación se analizarán aquellas sentencias de las que es posible deducir algunos aspectos de interés sobre el tema de estudio.

5.1.1. Excepción de autorización judicial para las pericias informáticas policiales

Ha sido muy comentada por la doctrina la STC 173/2011, de 7 de noviembre de 2011, debido a que reconoce, por primera vez en la jurisprudencia constitucional, que los archivos contenidos en un ordenador personal se encuentran también amparados por el artº 18 de la Constitución Española, en concreto, en lo relativo al derecho a la intimidad y a la protección de datos de carácter personal.

En lo que se refiere a la prueba pericial informática llevada a cabo por la policía judicial sobre los archivos contenidos en un ordenador, que había sido aportado por el empleado de una tienda de reparación de informática tras su denuncia del encuentro casual de contenido pornográfico de menores en el interior de dicho ordenador durante la reparación de su grabadora óptica, la sentencia valida la realización de dicha prueba pericial sin autorización judicial previa. Considera su realización legítima al resultar necesaria y razonable en términos de proporcionalidad, al establecer que “la policía perseguía un fin legítimo, por cuanto se enmarcaba dentro de las investigaciones que ésta realizaba dirigidas al esclarecimiento de un delito de pornografía infantil. Al propio tiempo existe la habilitación legal necesaria para la realización, por parte de los agentes intervinientes, de este tipo de pesquisas, pues, como hemos visto, se encuentran entre sus funciones las de practicar las diligencias necesarias para comprobar los delitos,

descubrir sus autores y recoger los efectos, instrumentos o pruebas, pudiendo efectuar 'un primer análisis' de los efectos intervenidos". Finaliza su conclusión diciendo que "si bien la intervención policial desplegada no contó con la previa autorización judicial, … podemos afirmar que nos encontramos ante uno de los supuestos excepcionados de la regla general, que permite nuestra jurisprudencia[19], pues existen y pueden constatarse razones para entender que la actuación de la policía era necesaria, resultando, además, la medida de investigación adoptada razonable en términos de proporcionalidad", no sin mencionar a continuación la necesidad de que el legislador regule esta materia con más precisión.

La sentencia cuenta con un voto particular discrepante, en lo relativo a la actuación policial que considera que vulneró el derecho a la intimidad del recurrente al realizar una intromisión en el contenido del ordenador más allá de una primera toma de contacto y al no existir urgente necesidad (el ordenador se encontraba apagado y en dependencias policiales). Previamente, considera la «calidad de la ley» deficiente en cuanto a la protección de la intimidad contenida en medios informáticos, lo que debería haber llevado al Tribunal a extremar su celo garante de los derechos fundamentales, determinando con precisión los supuestos y las condiciones, como quizás en este caso la prevalencia de los derechos del menor, en que puede producirse una intervención policial en el ordenador personal de un ciudadano.

Al margen de lo anterior, la sentencia incurre en mi modesta opinión en dos errores de hecho de tipo tecnológico. El primero, al determinar que el acceso que hizo el encargado de la reparación a los archivos de la carpeta Mis documentos constituía un mínimo necesario para verificar que la grabadora funcionaba correctamente, ya que para realizar dicha verificación hubiera bastado, y sería técnicamente más correcto, utilizar cualquier archivo en posesión y bien conocido por él, residente bien en un soporte óptico (DVD, CD, etc.) legible por la grabadora reparada, o bien en cualquier otro soporte externo (pendrive USB o similar). El segundo, al considerar que la contraseña de la que carecía el ordenador servía para permitir el acceso al disco duro interno de éste, en lugar

[19] El objeto recogido como hallazgo casual valida por completo la revelación de este delito, además del deber de denunciarlo por su conocimiento

de permitir el acceso al sistema operativo, lo que no tiene por qué implicar el acceso a la carpeta del disco duro donde se encontraban los archivos con contenido delictivo.

5.1.2. Admisión de petición de prueba pericial informática

La STC 153/2004, de 20 de septiembre de 2004, analiza la petición de amparo para la tutela efectiva en relación con la verificación del cumplimiento de una sentencia mediante la práctica de un peritaje informático que lo certifique. Concede la petición de amparo en base a que aunque el juzgado "no venía obligado a acordar necesariamente la prueba pericial informática propuesta por el demandante", sí le era exigible al órgano judicial una actuación que no se limitase a aceptar sin más la manifestación de la entidad crediticia de que había procedido a cumplir la sentencia. Por ello, retrotrae las actuaciones a fin de que el Juzgado resuelva respetando el derecho fundamental reconocido a la tutela judicial efectiva sin indefensión, garantizando el cumplimiento efectivo de la sentencia.

Una petición similar de amparo es sobre la que decide la STC 53/2006, de 27 de febrero de 2006. En esta ocasión, el objeto de la pericia informática era demostrar la autenticidad de unos disquetes de contabilidad de una empresa a fin de corroborar una información periodística. La pericia se intentó realizar en el juzgado de instancia, pero el perito no pudo llevarla a cabo por no disponer del programa informático de contabilidad cuya petición de obtención se había denegado por el juez. La sentencia constitucional deniega la petición de amparo por carecer dicha prueba de relevancia para determinar el sentido del fallo, por lo que no se había traducido en una indefensión efectiva del recurrente.

5.2. Jurisprudencia relevante sobre la materia

A lo largo de estos años, los distintos tribunales se han ido pronunciando acerca de distintas cuestiones relacionadas de una u otra manera con el peritaje informático. Para lograr una mayor homogeneidad en su análisis, se van a agrupar de forma sistematizada las distintas sentencias, organizándolas por epígrafes según temas de interés.

5.2.1. Necesidad de informe pericial sobre un medio de prueba informático

El Tribunal Supremo, en su reciente sentencia STS 2047/2015 de 19 de mayo de 2015, ha establecido la necesidad de llevar a cabo un informe pericial informático que acredite la identidad de los interlocutores, así como la integridad de la conversación mantenida

a través de una red social, para que dicha conversación sea aceptada como prueba válida en un procedimiento judicial.

Tal como recuerda esta sentencia, "la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas" y basa esta preocupación en la facilidad de manipulación de los archivos digitales mediante los que se materializa ese "intercambio de ideas", amparándose en el anonimato y en la facilidad de creación de cuentas con identidades fingidas que habitualmente permiten las plataformas de redes sociales, haciendo posible de esta manera "aparentar una comunicación en la que un único usuario se relaciona consigo mismo". Por ello, en caso de impugnación, se desplaza la carga de la prueba hacia quien pretende aprovechar la idoneidad probatoria de dichas conversaciones cuando éstas son aportadas al proceso mediante archivos de impresión. La sentencia concluye estableciendo de forma terminante que "será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido."

Esta prescripción jurisdiccional complementa la disposición del artº 384.2 de la LEC en cuanto a la posibilidad de aportar dictámenes y medios de prueba instrumentales al presentar medios de prueba consistentes en archivos informáticos, haciendo su aportación obligada cuando los archivos son fácilmente manipulables de manera unilateral, como es el caso de las conversaciones mantenidas en redes sociales.

Anteriormente a esta sentencia, el TS ya había dado validez en Auto ATS 1800/2013 de 14 de febrero de 2013 a conversaciones procedentes de SMS, MMS, o WhatsApp que habían sido obtenidas por la policía judicial mediante intervención telefónica autorizada por el juez.

Adicionalmente, la jurisprudencia menor, como las Sentencias de la Audiencia Provincial de Cádiz, SAP CA 122/2014 de 28 enero o de la Audiencia Provincial de Pontevedra, SAP PO 18/2014 de 10 enero ya habían denegado la validez como medio de prueba de conversaciones de WhatsApp por falta de garantías en cuanto a su posible manipulación.

5.2.2. Interrupción de la cadena de custodia

El auto del Tribunal Supremo ATS 2197/2012 describe muy gráficamente la importancia del mantenimiento de la cadena de custodia cuando dice que “es a través de la corrección de la cadena de custodia como se satisface la garantía de la "mismidad" de la prueba”, garantizando que aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes en el acto del juicio es lo mismo que los vestigios que se recogieron relacionados con el delito.

En este mismo sentido se manifiesta el auto de la Audiencia Provincial de Madrid AAP M 18559/2011 al desestimar la validez de una prueba pericial informática sobre un disco duro por haberse interrumpido la cadena de custodia al haber permanecido durante un año en poder del denunciante, previamente a la realización del informe pericial. Es de resaltar que este tipo de eventualidades se pueden solventar con un proceso de contextualización de la evidencia digital, evitando así que se invaliden todas las circunstancias probatorias obtenibles de un hecho que se descubra tiempo después de haber ocurrido.

Es de especial minuciosidad, el detalle con el que la sentencia de la Audiencia Provincial de Barcelona SAP B 1301/2008 de 29 de enero[20], describe el proceso de custodia del material informático intervenido durante un registro policial, llevado a cabo por los dos peritos judiciales, concluyendo de ello que “hubo una correcta identificación de elementos incautados y una adecuada custodia judicial”, aunque afirmando a continuación de forma sorprendente: "pero es que además considera la Sala acreditado que en este caso no hubo ninguna manipulación”, algo que va de suyo si, como se ha dicho, ha existido una adecuada custodia judicial.

La jurisprudencia anterior resalta, por tanto, la necesidad de congelar la evidencia digital inmediatamente después de ocurrido el delito o el incidente de seguridad y de garantizar a partir de ese momento la cadena de custodia, de forma que no puedan existir dudas sobre la "mismidad" de la que habla el auto del TS anteriormente mencionado.

[20] Esta sentencia incluye otras cuestiones de interés sobre las que se incidirá en el siguiente capítulo

En relación al procedimiento de obtención de la evidencia digital, es interesante la sentencia del Tribunal Supremo STS 7208/1999 de 15 de noviembre, que exonera al Secretario Judicial de permanecer durante un proceso de clonado de un disco duro realizado por la policía judicial con estas palabras: "Lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano, que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia."

5.2.3. Requisitos subjetivos de validez de la prueba pericial informática

En cuanto a la validez de la prueba pericial en base a las circunstancias subjetivas de los peritos que la llevan a cabo, la sentencia del Tribunal Supremo STS 4315/2008 establece la plena validez de la prueba pericial informática en un proceso penal con un informe de un perito, cuando el artº 459 de la LECrim establece la necesidad de que sean dos, al establecer que "el número de peritos no condiciona la validez del informe pericial, máxime cuando ha sido emitido por un organismo oficial que realiza la labor en equipo. Un perito efectúa materialmente el informe de un aspecto de la pericia que es certificado y confirmado por el otro perito firmante y viceversa".

Asimismo, la sentencia de la Audiencia Provincial de Madrid SAP M 12497/2013 de 24 de julio, determina la validez de un informe pericial informático sin que para ello suponga un obstáculo la titulación académica del perito "Doctor en Ciencias Físicas con una amplia formación adicional en informática, siendo Director de una empresa de seguridad informática, por lo que no encuentra la Sala obstáculo para el desarrollo de la pericia".

5.2.4. Acotamiento de las funciones del perito informático

El Tribunal Supremo en la sentencia STS 6007/2008 de 29 de octubre, delimita claramente la función que corresponde al perito informático al establecer que "es evidente que la equiparación que efectúa el perito entre: ausencia de advertencia del programa Emule del sistema de archivos transparentes con la conclusión de que el usuario del programa desconocía y estaba ignorante de este dato no es admisible. Tal

conclusión solo podría ser efectuada por el juzgador a quien le corresponde la tarea de valorar la actividad probatoria".

En sentido similar se pronuncia en la sentencia STS 2743/2013 de 17 de mayo, al determinar que "el perito informático, por definición, sólo podrá extender sus opiniones a aquellos aspectos técnicos relacionados con el grado de manipulación apreciable en las fotografías o en los correos electrónicos aportados, pero absteniéndose, claro es, de cualquier valoración sobre el desenlace probatorio que haya de asociarse a su dictamen. La fijación de su alcance ha de ser siempre de la exclusiva incumbencia del Tribunal".

5.2.5. Informe pericial informático en el ámbito laboral

Las sentencias del Tribunal Supremo STS 6128/2007 de 26 de septiembre y STS 1323/2011 de 8 de marzo establecen el criterio acerca de la no aplicación directa ni analógica del artº 18 del Estatuto de los Trabajadores, sino del artº 20.3, a la hora de la realización de una prueba pericial encargada por el empresario sobre el ordenador de un trabajador.

Considera por ello que el ordenador es un instrumento de producción del que es titular el empresario y no un efecto particular del trabajador, lo que no obsta para que se guarde en la aplicación de la prueba pericial la consideración debida a la dignidad e intimidad del trabajador, que también se extiende a sus archivos personales existentes en el ordenador, por lo que un acceso a dichos archivos, sin previa advertencia sobre el uso y el control del ordenador, supondría una lesión a su derecho a la intimidad. Por ello "lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos".

Adicionalmente, la sentencia STS 8876/2011 de 6 de octubre, añade a lo anterior que "si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones", en contra de la previa prohibición del empresario o con una advertencia expresa o implícita de control.

En el mismo sentido y con los mismos argumentos se expresa la jurisprudencia menor en sentencias como la del TSJ del País Vasco STSJ PV 1118/2012 o la del TSJ de Andalucía STSJ AND 2248/2014, esta última considerando cumplidos por la empresa los requisitos mencionados para la validez de la prueba pericial que sirvió de base para el despido del trabajador.

5.2.6. Identificación del autor mediante dirección IP

El Tribunal Supremo ha establecido en su sentencia STS 8316/2012 de 3 de diciembre, la insuficiencia de determinar la autoría de un delito informático mediante la simple constatación de que la dirección IP, desde la que existe certeza de que se cometió el delito, haya sido asignada a una línea telefónica y a un ordenador conectado a ella que pertenece al supuesto autor. La inferencia que vincula ser usuario de un ordenador y de una línea telefónica no lleva necesariamente a la conclusión de que ese usuario sea el autor de toda utilización telemática de esa infraestructura informática.

La sentencia explica, a través del contenido del informe pericial de parte que había sido desestimado en la instancia, que el ordenador al que hace referencia estaba conectado en modo *modem*, no *router*, por lo que sus puertos disponibles eran cognoscibles por otros usuarios de Internet, suponiendo un factor de vulnerabilidad que podía ser aprovechado por un atacante malicioso y utilizar el equipo ajeno quedando su uso registrado como si fuera el auténtico titular, sin que éste pueda siquiera percatarse de ese uso malicioso y ajeno de su equipo.

Finalmente, la sentencia achaca a la indolencia investigadora de la actuación policial, la falta de obtención, de forma inmediata a los hechos, de otras evidencias digitales en el disco duro que hubieran podido ratificar la inferencia de la autoría.

En otro orden de cosas, la sentencia de la Audiencia Provincial de Granada SAP GR 391/2013, de 26 de abril, invalida el informe pericial que permitió la determinación de la dirección IP desde la que se cometió el delito, debido a que el auto del juez que las autorizó no resistía las exigencias de legalidad recogidas en la Ley 25/2007, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, que, en prevención de la protección constitucional del derecho a la privacidad e intimidad de las comunicaciones, permite sólo la autorización judicial en el caso de delitos graves.

6. Consecuencias derivadas y aspectos prácticos

En los capítulos anteriores se han expuesto los aspectos más relevantes relativos a la normativa y a la jurisprudencia del peritaje informático, así como a la metodología para su realización técnica. Estos aspectos relevantes forman así, lo que podría denominarse el cuerpo de doctrina para llevar a cabo un peritaje informático.

En el presente capítulo, se van a tratar de abordar aquellos aspectos de índole práctica que surgen como consecuencia de aplicar dicho cuerpo de doctrina así como también de las carencias que aparecen al intentar llevarlo a cabo.

6.1. Contextualización de la prueba electrónica

Para lograr que la prueba electrónica tenga una mayor fuerza de convicción sobre el tribunal, un aspecto básico es presentar la evidencia digital, que se va a utilizar como medio de prueba, dentro del contexto en el que se ha generado.

Resulta evidente que no basta con aportar escuetamente como medios de prueba los equipos y dispositivos (ordenadores, *smartphones*, discos duros, discos ópticos, memorias USB, etc.), es decir, el hardware, en los que reside la fuente de prueba, pero tampoco es suficiente aportar sin más los programas de software y archivos de datos que dichos equipos o dispositivos puedan contener, por mucho que pueda parecer evidente a primera vista la información que de ellos se pueda derivar.

El artº 384.2 de la LEC, ya prevé la conveniencia de que la parte que quiera proponer este tipo de medios de prueba, aporte un dictamen pericial, así como cualquier medio de prueba instrumental que considere conveniente, para incrementar el poder de convicción de dicha prueba sobre el tribunal.

En este dictamen pericial informático será necesario explicar de forma clara y descriptiva, aunque concisa para no alargarla inútilmente, el **contexto** de la evidencia digital, resaltando los siguientes aspectos:

- El entorno físico y humano en el que se ha encontrado la evidencia digital.
- Los procedimientos que se han empleado para obtenerla, detallando, en su caso, las autorizaciones que se hayan obtenido para ello.
- Las herramientas empleadas en la obtención y análisis de la evidencia.

- Los resultados conseguidos de cada uno de los procesos de análisis a los que se ha sometido a la evidencia digital, haciendo referencia a los detalles técnicos de estos resultados de forma que en los datos aportados se salvaguarde en cualquier caso la privacidad y cualquier otro derecho fundamental de las partes o de terceros.

Es importante realizar un análisis respecto a la posible manipulación o falsificación de las evidencias y del entorno, de manera que la acción se atribuya al usuario efectivo.

6.2. Incertidumbres alrededor de la cadena de custodia

La sentencia de la Audiencia Provincial de Barcelona SAP B 1301/2008, ya comentada en el capítulo relativo a Jurisprudencia, realiza de forma muy detallada un gran número apreciaciones al respecto de la cadena de custodia para finalmente concluir que se ha realizado de forma adecuada. Sin embargo, tal cantidad de detalles sirven para poner en evidencia la falta de una metodología idónea a la naturaleza de las fuentes digitales de prueba custodiadas, que permita garantizar adecuadamente la conclusión pretendida. Así:

- Se da por buena la falta de concordancia en una cantidad de 6 CDs entre el material aprehendido y el entregado a los peritos, con la justificación de que "en modo alguno fundamentan la condena" y concluyendo que hubo una correcta identificación de elementos incautados.
- Reconoce que, a pesar de la recomendación técnica de trabajar siempre con copias clónicas, no se hicieron las copias de seguridad[21] de todos los archivos encontrados, pero que los peritos habían puesto de manifiesto "que no habían realizado modificación alguna en los archivos y que tan solo habían introducido una utilidad a fin de poder imprimir".
- Pero el episodio más llamativo en cuanto a "metodología atípica" es el que relata a continuación la sentencia en el que la propia policía, en el momento de detener al apelante, le manifiesta la conveniencia de que él mismo realice un volcado del correo que tuviera almacenado en el ordenador de la empresa, lo que lleva a cabo grabándolo en un CD, protegiéndolo con una contraseña que sólo él

[21] Es de señalar que esta omisión supone una descontextualización de la evidencia, ya que no se determina bajo qué criterio se aporta o no.

conocía y firmando todos los actuantes sobre el CD que es archivado a continuación fuera del control de los peritos.

También la sentencia de la Audiencia Provincial de Málaga SAP MA 1/2011 es una buena fuente de detalles acerca de procedimientos de custodia de las evidencias digitales. Así, la sentencia recoge declaraciones de los agentes policiales, tales como "se extrajeron los discos de 4 ordenadores, se sellaron y se precintaron - por ello no se hizo huella digital" o "los CDs empleados eran de una sola escritura y como las copias de los discos se sellaron, no hizo falta hacer el "Hash" o huella digital"[22]

La conclusión que se puede extraer de todo lo anterior es la **carencia de una metodología** con suficiente rigor y que permita garantizar que las evidencias digitales no se han alterado en absoluto desde su recogida hasta su contrastación en el juicio oral. Sería conveniente que por vía normativa o, al menos, jurisprudencial se recogiera un modelo de referencia similar al presentado en el capítulo 3 con capacidad para responder a las cuatro preguntas, qué, quién, cuándo y dónde, acerca de cada cambio de la evidencia digital a lo largo de la cadena de custodia, desde su recogida hasta su presentación ante el tribunal. El riesgo de mantener una metodología de cadena de custodia con lagunas graves como las mencionadas anteriormente, es la facilidad con que un contraperitaje informático bien estructurado puede destruir la certidumbre de la prueba pericial que deba servir de soporte probatorio a la demostración de un delito informático o de un ilícito de cualquier tipo.

6.3. La prueba electrónica como documento

Existe una profunda discusión doctrinal sobre el carácter documental o no de la prueba electrónica. La consecuencia derivada de que pudiera ser considerada prueba documental es su distinto tratamiento procesal, más favorable en general del aplicable si careciera de esa consideración. Así, la LEC en su artº 326.1 confiere al documento privado el valor de prueba plena en el proceso si no es impugnado por la parte a quien perjudica y, aún en este caso, la parte que presenta la prueba podrá proponer un medio de prueba útil para probar su autenticidad.

[22] Es de señalar que esa forma de actuar no tiene en cuenta la posibilidad de multisesión en la grabación del CD, lo que invalidaría la certeza sobre lo grabado en él.

Frente a este valor de prueba plena como documento, la consideración de la prueba electrónica como simple instrumento de archivo informático, conforme al artº 384, le daría solamente un valor probatorio conforme a las reglas de la sana crítica del juez, dependientes por tanto de su conocimiento sobre la materia.

Tradicionalmente, la doctrina ha mantenido al respecto dos teorías contrapuestas: la teoría autónoma[23], según la cual la prueba electrónica tendría una naturaleza propia, singular y diversa[24], y la teoría analógica, según la cual tendría una naturaleza equiparable a los medios de prueba tradicionales, sin más que sustituir el papel por un soporte electrónico. Al margen de ambas teorías, ha surgido una tercera: la teoría de la equivalencia funcional que propugna que un documento electrónico surte los mismos efectos jurisdiccionales que el documento en papel.

Ciertamente, esta última teoría está respaldada por el tratamiento que el artº 3.8 de la Ley 59/2003 de Firma Electrónica da a los soportes de los documentos electrónicos firmados electrónicamente, ya que esta Ley les dota del carácter de prueba documental en juicio. Si además dicha firma es reconocida, la impugnación del documento se resolverá comprobando que dicha firma cumple todos los requisitos prescritos en esta Ley. Si no es firma reconocida, sino avanzada, la impugnación tendrá el mismo tratamiento que el establecido en el artº 326.2 de la LEC para resolver la impugnación de cualquier documento privado.

El mismo carácter de documento, y, con ello, de prueba admisible en juicio como documental, otorga el artº 24.2 de la LSSI al soporte electrónico en que conste un contrato celebrado por vía electrónica.

Pero al margen de los dos casos anteriores, documentos electrónicos firmados electrónicamente y contratos por vía electrónica, no existe base legal para considerar al resto de las evidencias digitales como fuentes de prueba documentales. En esa misma línea se manifiesta la sentencia del Tribunal Supremo STS 6216/2011 de 16 de junio, al considerar que una grabación de audio y vídeo no tiene naturaleza documental. Parece

[23] Montón Redondo. *Medios de reproducción de la imagen y el sonido. La prueba*. CGPJ, Madrid. 2000, págs. 50 y ss.
[24] Álvarez-Cienfuegos Suarez, J.Mª. *Las obligaciones concertadas por medios informáticos y la documentación*. La Ley, 1992 nº 4, pág. 1013

referirse al conjunto de medios de prueba audiovisuales, que recoge el artº 382 de la LEC, “Instrumentos de filmación, grabación y semejantes” los denomina. Nada dice, sin embargo, dicha sentencia de los soportes informáticos, tal como los recoge el artº 384 de la LEC, “Instrumentos que permitan archivar, conocer o reproducir datos”.

Dicho lo anterior, no se puede dejar de considerar que la misma Ley de Firma Electrónica hace, en el apartado 5 del mismo artículo 3, una definición de documento electrónico como “la información de cualquier naturaleza en forma electrónica, archivada en soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado”. Son destacables en esta definición los siguientes aspectos:

1. No diferencia entre naturalezas de la información. Al contrario de lo que hace la LEC, da igual que se trate de información audiovisual o de datos informáticos cualesquiera.
2. Debe estar archivada en soporte electrónico. Cabe entender por ello cualquier soporte implementado con dispositivos electrónicos y no únicamente soportes informáticos. Así, una antigua cinta de video o de audio, o dispositivos electrónicos no programables, como sensores o *wearables*, serían soportes electrónicos no informáticos.
3. Debe de tener un formato determinado, es decir, definido según una especificación concreta establecida de antemano.
4. Debe de poderse identificar y tratar como un conjunto individualizado y separado del resto de información existente en el soporte electrónico.

Ciertamente se trata de una definición de amplio espectro, en la que cabría incluir prácticamente cualquier tipo de registro electrónico de datos. Sin embargo, hay que recordar que la Ley de Firma Electrónica no da al documento electrónico per se carácter de prueba documental en juicio, sino únicamente al documento electrónico firmado electrónicamente, lo que demuestra las reticencias del legislador para considerar prueba documental aquello que previamente ha denominado sin ambages documento. Por el contrario, como ya se comentó en el apartado correspondiente a la normativa en el ámbito penal, el Código Penal da carácter de documento, examinable de oficio por el tribunal ex artº 726 LECrim, a todo soporte material con datos de relevancia jurídica.

En conclusión, se puede afirmar que no existe una homogeneidad legislativa en el tratamiento de la prueba electrónica como documento, lo que da lugar a un tratamiento habitualmente restrictivo por los tribunales que no se compadece con la realidad digital del mundo actual y con el impulso al desarrollo de la Sociedad de la Información por parte de los poderes públicos. Todo ello hace necesario modernizar la legislación procesal para que defina, de forma homogénea y coherente, el tratamiento a dar a dicha prueba y así se han manifestado una mayoría de expertos jurídicos también a nivel europeo e internacional, con objeto de mejorar la cooperación transnacional en la persecución de los delitos informáticos[25].

6.4. Uso de estándares para el tratamiento de la evidencia digital

Para la realización del análisis forense, según se ha descrito en el capítulo 3, existen una serie de estándares nacionales e internacionales que recogen unas guías de buenas prácticas que tratan de garantizar mediante su seguimiento y correcta aplicación, la validez como medios de prueba de las evidencias recogidas en un posterior proceso judicial. No obstante, es preciso constatar a renglón seguido, que, tal como ya se mencionó entonces, no existe un consenso para que los profesionales del sector puedan llevar a cabo su actividad pericial según una metodología única[26].

Se van a resumir a continuación las normas técnicas o estándares más significativos que, a diferencia del modelo general descrito en dicho capítulo, centran sus recomendaciones en el seguimiento de unos procedimientos concretos de actuación y en la utilización de unas herramientas técnicas por parte del perito informático, con objeto de evitar contaminar las evidencias recogidas con cualquier eventualidad que pueda provocar su invalidez probatoria.

6.4.1. RFC 3227

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 sistema las directrices a tener en cuenta en las

[25] Illán Fernández. *La Prueba Electrónica, Eficacia y Valoración en el Proceso Civil*. 2009.pág. 256

[26] Gervilla Rivas, Carles. *Metodología para una Análisis Forense*. TFM Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC). UOC – INCIBE. Diciembre 2014. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

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 que existen herramientas en módulos cargables del núcleo del sistema que pueden proporcionar una imagen parcial del mismo. En cualquier caso, se debe de estar preparado para garantizar la autenticidad y fiabilidad de las herramientas utilizadas.

6.4.2. ISO 27037 e ISO 27042

La norma ISO 27037, más reciente que la recomendación anterior, ya que está publicada en 2012, proporciona orientaciones relativas al procedimiento de actuación pericial en el escenario de la identificación, recopilación y archivo de la evidencia digital, sin entrar en su análisis, mediante la aplicación de métodos que permitan que dicho procedimiento sea auditable, reproducible y defendible.

La norma pertenece al grupo de normas ISO/IEC 27000 concernientes a las técnicas de seguridad de la información y a las especificaciones de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Sin entrar en una descripción de la norma similar a la realizada para la RFC 3227, debido a su extensión, existen en ella dos aspectos singulares que merecen destacarse.

Por una parte, la norma define dos roles especialistas diferenciados en la obtención y gestión de las evidencias digitales:

- *Digital Evidence First Responders* (DEFR) Experto en primera intervención de evidencias electrónicas: Persona que está autorizada, formada y habilitada para actuar en la escena de un incidente, y así recoger y adquirir las evidencias digitales con las debidas garantías.

  Su formación dependerá del contexto, aunque entre las actuaciones que normalmente debería realizar se encuentran:

  - Asegurar el área dónde ocurre el evento informático y los elementos materiales probatorios que se encuentren allí: notas, documentos, dispositivos electrónicos, entre otros.
  - Evitar que personal extraño al área, tenga acceso a la misma y a los equipos que allí se encuentren.
  - Tomar fotos o video de cómo encontró el área y documentar fecha, hora y condiciones en las cuales llega al sitio donde ocurren los hechos.

- *Digital Evidence Specialists* (DES) Experto en gestión de evidencias electrónicas: Persona que puede hacer lo que hace el DEFR con la evidencia digital y además cuenta con conocimientos, destrezas y entrenamiento especializado en un amplio rango de aspectos tecnológicos, lo que podríamos llamar un perito informático o en inglés un *computer expert witness*.

Por otra parte, la norma distingue y particulariza los procedimientos a llevar cabo en una serie de tipologías de dispositivos y entornos como:

- Equipos y medios de almacenamiento digital y dispositivos periféricos (discos duros, discos flexibles, discos ópticos y magneto-ópticos y dispositivos de datos con funciones similares).
- Dispositivos móviles, como teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria.
- Sistemas de navegación móvil como GPS.
- Cámaras digitales de video y fotográficas (incluyendo sistemas de circuito cerrado de TV).
- Ordenadores de uso generalizado conectados a redes.
- Equipos de redes basadas en protocolos TCP / IP y otros.
- Dispositivos con funciones similares a las anteriores.

De manera complementaria a la norma anterior, que no entraba en los aspectos de análisis de las evidencias, acaba de publicarse en junio del presente año, la norma ISO 27042, que proporciona recomendaciones relativas al análisis e interpretación de las evidencias digitales, focalizándose en su continuidad, validez, reproducibilidad y repetibilidad. Sintetiza una guía de buenas prácticas para seleccionar, diseñar e implementar los procesos de análisis de la evidencia que resultan idóneos en cada caso y para registrar la información suficiente que permita someter dichos procesos a un escrutinio independiente en caso de necesidad, así como para demostrar la capacidad y competencia del equipo de investigación que los ha llevado a cabo.

Esta norma pretende proporcionar un marco común que contenga elementos de análisis e interpretación de incidentes de seguridad, de forma que puedan utilizarse en la

implementación de nuevos métodos analíticos y como un estándar común en el tratamiento de las evidencias digitales.

6.4.3. UNE 71505 y UNE 71506

Estas normas, publicadas en 2013 por la Asociación Española de Normalización y Certificación, tienen como finalidad proporcionar un apoyo metodológico para la gestión de evidencias electrónicas de cara a su obtención, conservación y, en su caso, aportación en juicio. [27]

En concreto, 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.

Por su parte, 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.

Ambas normas son de aplicación a cualquier organización o profesional competente en la investigación de incidentes de seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas, aunque no es su objeto la acreditación o validación de laboratorios forenses ni la homologación de software o equipos relacionados.

Su objeto último es formar un corpus normativo que sirva de referencia en este ámbito tanto ante los Tribunales de Justicia como, en su caso, ante la cúpula directiva de las distintas empresas.

[27] García, Paloma. *Normas para las evidencias electrónicas*. Revista de la Normalización y la Certificación. Nº 287. Noviembre 2013

6.4.4. UNE 197001

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 facilitar y homogeneizar la lectura y comprensión de los análisis y conclusiones desarrollados por el perito. Sin embargo, no determina los métodos y procesos específicos para la elaboración del informe.

La norma incluye unas sencillas recomendaciones acerca de que todo informe o dictamen pericial debe disponer de un título que identifique claramente su objeto y debe constar de una estructura básica compuesta por identificación, índice, cuerpo del informe y, cuando corresponda, documentos anexos, así como que, en cada página del dictamen, debe figurar su referencia identificativa, el número de la página y el total de éstas.

La información de identificación del dictamen debe incluir:

- 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.

Si procede, debe incluirse una declaración del perito acerca de posibles tachas y juramento o promesa de imparcialidad.

En cuanto al cuerpo del dictamen, la norma detalla el título y contenido de los diversos apartados que debe recoger: objeto, alcance, antecedentes, consideraciones preliminares, documentos de referencia, terminología y abreviaturas, análisis y conclusiones.

En resumen, nos encontramos ante una norma española para definir de forma general los requisitos formales que debe cumplir un dictamen pericial, si bien en la medida en que su cumplimiento no es obligatorio, sólo se trata de una buena práctica recomendada[28].

[28] López Rivera, Rafael. *Peritaje Informático y Tecnológico. Un enfoque teórico-práctico*. 2012, pág.222

7. Conclusiones

El peritaje informático, si bien no ha sido recogido de forma específica en nuestra legislación, sí que tiene cabida en ella a través de las especialidades que las distintas normas procesales y, en menor medida, también sustantivas, han establecido acerca de las fuentes de prueba que son utilizadas como base material del peritaje informático, es decir, las denominadas evidencias digitales. Pero estas especialidades muestran algunas connotaciones que es conveniente resaltar a modo de conclusión de este informe.

En primer lugar, de la exposición llevada a cabo en este informe, se deduce con bastante claridad la carencia normativa en la adopción de una metodología que someta la recopilación y custodia de las fuentes de prueba informáticas a un procedimiento definido y que resulte confiable por parte de los jueces. Sería conveniente, en ese sentido, que la norma definiera un marco de referencia o que, en su defecto, dicho marco fuera establecido de forma jurisprudencial, de forma que permitiera mejorar la seguridad jurídica alrededor de la prueba electrónica.

Supone un paso significativo en esa dirección la reciente sentencia del Tribunal Supremo 2047/2015 que ha establecido la necesidad de llevar a cabo un informe pericial informático que acredite la identidad de los interlocutores y la integridad de la conversación mantenida a través de una red social, para que dicha conversación sea aceptada como prueba válida en un procedimiento judicial. De esta manera, se dota al juez de forma imperativa de un dictamen pericial informático que le ayuda en la formación de su convicción acerca de una evidencia digital que es, a priori, fácilmente susceptible de manipulación.

En segundo lugar, no existe una homogeneidad ni una claridad legislativa en el tratamiento procesal de la prueba electrónica en cuanto a su carácter documental, lo que da lugar a un tratamiento desigual y, por lo general, restrictivo por parte de los tribunales. Este tratamiento es poco acorde con el impulso pretendido a la Sociedad de la Información por parte de las Administraciones Públicas y, en particular, en el ámbito de la Justicia.

Debido a ello, desde diversas instancias, se ha propuesto modernizar y homogenizar las normas que regulan el tratamiento procesal de la prueba electrónica, no sólo

internamente, sino también a nivel europeo e internacional, a fin de mejorar la cooperación global en la persecución del ciberdelito.

En tercer lugar, las recientes previsiones legislativas en el ámbito penal acerca del tratamiento de la prueba electrónica, utilizan frecuentemente expresiones genéricas que dan lugar a conceptos jurídicos indeterminados, lo que puede resultar necesario a la hora de abordar los aspectos de fondo que establece la norma, pero no tanto en cuanto a determinar los aspectos relativos a la forma.

Así, resultaría aconsejable una concreción de los aspectos formales del tratamiento de la prueba electrónica en base a la adopción de estándares o normas técnicas emitidas por Autoridades de Normalización como las mencionadas en el capítulo anterior, de manera similar a la regulación que se ha realizado a nivel europeo y nacional de la firma electrónica, en la que se ha hecho referencia a normas técnicas criptográficas y a Autoridades de Certificación Electrónica o, en terminología legislativa, “dispositivos y datos de creación y de verificación de firma” y “prestadores de servicios de certificación”, respectivamente.

Anexo. Elaboración de un caso práctico

En el presente anexo, se expone un ejemplo de informe pericial informático extraído de un caso real y convenientemente seudonimizado en cuanto a los datos que contiene de carácter personal. Dada su extensión superior a treinta páginas, su contenido va a ser resumido eliminando los elementos más repetitivos o que no aporten una información de relevancia para comprender la estructura del informe.

- La página inicial del informe muestra el título, así como otros datos identificativos y las firmas de los peritos y personas encargadas de la revisión y aprobación en la entidad encargada de realizar el peritaje:

DEPARTAMENTO INFORMATICA FORENSE

Departamento:	**Forense**

Revisión	**Fecha**	**Fecha Aprobación**
2	**23/06/2011**	
Realizado por	**Revisado por**	**Aprobado por**

Firma: **Firma:** **Firma:**

INFORME TECNOLOGICO FORENSE

DEL ORDENADOR PERSONAL DE:

- D. JOSE EJEMPLO

- DEPARTAMENTO DE SISTEMAS DEL BANCO DE EJEMPLO

- En el apartado 1 se realiza, tal como se muestra a continuación, un resumen del objeto y del contenido del informe, así como su finalidad y los datos del solicitante:

1.- INTRODUCCION Y OBJETO DEL INFORME PERICIAL

De acuerdo con nuestra propuesta de servicios profesionales de 15 de abril de 2011, hemos realizado una investigación tecnológica, a petición de los representantes legales de D. Ramón Ejemplo (en adelante, el Sr. Ejemplo o REE), con el objeto de identificar y presentar las pruebas digitales existentes en el buzón de correo del ordenador personal del Sr. Ejemplo y en los sistemas informáticos del Banco de EJEMPLO (en adelante, el Banco). Nuestro trabajo tiene como finalidad presentar las evidencias digitales de las comunicaciones mantenidas por el Sr. Ejemplo, con el Banco de EJEMPLO a través del correo electrónico. Y verificar la autenticidad e integridad de los correos electrónicos y los archivos adjuntos intercambiados.

El presente informe pericial ha sido preparado con la finalidad de reflejar los resultados de nuestro trabajo, para ser utilizado en los eventuales procedimientos judiciales y/o las denuncias a las autoridades competentes.

Los firmantes de este informe pericial, sin perjuicio del proceso de ratificación del mismo, ofrecemos nuestra máxima colaboración a los Tribunales que resulten competentes en el caso, para prestarles asesoramiento técnico o facilitarles cualquier aclaración que consideren oportuna, así como para complementar la investigación en aquellos aspectos que pudieran considerar relevantes.

Los procedimientos de trabajo que hemos realizado, son aquellos que hemos considerado necesarios en base a nuestra experiencia, con el fin de obtener y presentar en este informe las evidencias digitales de la información contenida en el ordenador, y buzón de correo asignados al empleado por la compañía.

Una descripción de los procedimientos de trabajo realizados se incluye en el apartado 4 de este informe pericial.

Las conclusiones de nuestro trabajo se detallan en la sección 9 de este informe.

- En el apartado 2, se muestra una breve presentación del o de los peritos firmantes del informe, así como de la identidad y experiencia de la entidad encargada del peritaje.
- En el apartado 3, se detallan, según se muestra a continuación, los antecedentes del caso previos al informe pericial, que son conocidos por el perito:

3.- ANTECEDENTES

La descripción de los hechos que se realiza a continuación, supone nuestro entendimiento de la situación, que se ofrece con el objeto de que permita al lector de nuestro informe circunscribir nuestro trabajo dentro de un contexto determinado. Por lo tanto, la misma no forma parte de nuestras conclusiones, ni debe entenderse como una interpretación legal de los hechos acaecidos:

- D. Ramón Ejemplo es cliente del área de banca privada del banco EJEMPLO junto con los siguientes miembros de su familia: ANA María Ejemplo, MARIA Ejemplo y ANA María Ejemplo
- El Banco EJEMPLO presento al Sr. Ejemplo y su familia una oportunidad de inversión en mayo del año 2010
- El Sr. Ejemplo considera que el Banco no les informó adecuadamente sobre el nivel de riesgo de la inversión y fruto de esta desinformación han sufrido cuantiosas pérdidas económicas

En este contexto, D. Ramón Ejemplo , a través de sus representantes legales, Ejemplo Abogados (en adelante Ejemplo o la Sociedad) han solicitado nuestros servicios profesionales para presentar las evidencias digitales existentes en los equipos informáticos de REE y del Banco que contienen las comunicaciones electrónicas entre el Banco y REE y su familia, realizar un análisis forense del contenido de las mismas, y en su caso presentar la información relevante que puedan contener, verificando la autenticidad e integridad de las mismas.

Nuestro informe pericial podrá ser aportado a los procedimientos judiciales que el Sr. Ejemplo pudiere iniciar.

- El apartado 4, “Alcance”, presenta los distintos procedimientos que se han llevado a cabo en el desarrollo del informe pericial:

4.- ALCANCE

Los procedimientos a realizar en el desarrollo de nuestro trabajo han sido los que se describen a continuación:

- Conversaciones con representantes legales de REE y el Banco Ejemplo.
- Obtención de una imagen forense de los ordenadores y buzones de correo de los equipos informáticos de REE que contienen las comunicaciones entre el Banco y REE y sus familiares.
- Reconstrucción de los correos electrónicos que hayan podido ser borrados de los buzones de correo y que sean susceptibles de ser recuperados.
- Identificación de la información relevante para el caso y verificación de la autenticidad e integridad de la misma.
- Elaboración de un informe pericial detallando el análisis forense realizado sobre las evidencias digitales y su contenido.

4.1 Procedimientos de Evidencia Digital Aplicados

La obtención de las imágenes forenses fue realizada siguiendo los procedimientos aplicables de la metodología de trabajo de Lazarus, basada en los estándares y mejores prácticas profesionales en tecnología forense y utilizando procedimientos y herramientas específicamente diseñados para llevar a cabo este tipo de trabajos.

Los procedimientos particulares aplicados se detallan en el apartado 8 de este informe y se refieren exclusivamente a los procesos que hemos considerado necesarios para obtener los resultados de nuestro trabajo de acuerdo al alcance

- El apartado 5, muestra las fuentes de información de todo tipo que han sido utilizadas para la elaboración del informe pericial y, en el caso de las fuentes digitales, se indica asimismo su huella digital o hash:

5.- FUENTES DE INFORMACION

La información empleada para realizar los procedimientos de trabajo arriba mencionados es la siguiente:

- Conversaciones con los representantes legales de REE y del Banco.
- Ordenadores y buzones de correo electrónico propiedad de REE y sus familiares
- Cualquier otra documentación que consideremos relevante en el curso de la realización del trabajo de campo.
- La obtención de pruebas digitales por parte de los técnicos forenses de Lazarus se realizó de forma que las evidencias adquiridas no fueran susceptibles de manipulación ya que cualquier modificación de los datos originales, alteraría la firma digital obtenida e identificada por el código denominado Hash de adquisición y verificación (número de 32 dígitos hexadecimal que identifica unívocamente la imagen realizada).

A continuación se detallan cada una de las evidencias digitales obtenidas y que más adelante a lo largo del informe se han utilizado como fuente de información:

Cuadro 1: Evidencias digitales y códigos Hash de adquisición y verificación

Número de evidencia	Descripción y tipo de evidencia	Asignado	Ubicación y Nº Serie del equipo	Código "hash" de adquisición y verificación
EJEMPLO-A001	Ordenador Personal	Ramón Ejemplo	Domicilio de REE HP DC510 SFF Número de Serie: CZC6050RTX	F9F3318D 85CA54DD 28B583DA BA791226
EJEMPLO-A004	Información disponible en los sistemas informáticos del Banco Ejemplo		Varios Sistemas	1066365BEE216440F1 34E0639E90FC38

Fuente: Actas de copiado (Documento 1).

Adjuntamos como **Documento 1** copia de las actas y documentos de obtención de las evidencias digitales

- El apartado 6 muestra, según dispone la LEC, las manifestaciones de los peritos en cuanto a su juramento o promesa de decir verdad y de imparcialidad:

6.- MANIFESTACIONES

- De conformidad con lo dispuesto en el artículo 335.2 de la Ley de Enjuiciamiento Civil 1/2000, de 7 de enero, juramos o prometemos que cuanto acontece es verdad y que hemos actuado, y en su caso actuaremos, 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 conocemos las sanciones penales en las que podríamos incurrir si incumpliéramos nuestro deber como peritos.

- Hemos expresado en nuestro informe nuestro entendimiento de las cuestiones sobre las cuales se nos ha requerido nuestra opinión como expertos. Todos los asuntos sobre los cuales nos hemos pronunciado entran dentro de nuestro ámbito de conocimiento.

- En aquellos casos donde no teníamos un conocimiento directo hemos indicado la fuente de la información.

- En el momento de firmar este informe, consideramos que es completo y adecuado a las circunstancias. Notificaremos a los destinatarios de este informe si, por cualquier razón, con posterioridad tuviéramos conocimiento de algún hecho o dato relevante adicional a la información que se contiene en el mismo, y consideráramos que el informe debería incluir alguna salvedad o corrección significativa.

- Entendemos que este informe será la evidencia que nosotros proporcionaremos, sujeto a cualquier corrección o salvedad que se pueda hacer.

- En el apartado 7, se describen los diferentes fundamentos en que están basadas las afirmaciones que se realizan en el informe pericial, así como las acotaciones en cuanto a su contenido y alcance:

7.- FUNDAMENTOS DE ESTE INFORME PERICIAL

- Nuestro análisis cubre exclusivamente los aspectos tecnológicos y en ningún momento, se refiere a las implicaciones legales de los mismos.

- Las afirmaciones vertidas en este informe pericial están basadas, exclusivamente, en el análisis de la información proporcionada por nuestro cliente o en los procedimientos de trabajo que hemos realizado de acuerdo con lo descrito en el apartado de alcance del trabajo de este informe, y en la interpretación de dicha información. Las conclusiones de este dictamen pericial están únicamente basadas en la información obtenida y documentación revisada que se describen en el apartado de fuentes de información de este informe.

- En la documentación en papel, utilizada, hemos trabajado con documentación original siempre que ha sido posible, aunque no hemos realizado ninguna verificación sobre la autenticidad de la misma, al no ser ésta nuestra área de especialización y, en algunos casos en los que los documentos que hemos obtenido eran copias, no hemos verificado su concordancia con el original. Todo ello sin perjuicio de habernos conducido con el máximo rigor y fiabilidad en los procedimientos de obtención de evidencias digitales e imágenes forenses que se describen en el apartado ocho de este informe.

- Las actualizaciones a este informe se producirán únicamente a solicitud expresa de la Sociedad o de los Tribunales que resulten competentes en la materia.

- El apartado 8 es el que presenta pormenorizadamente los resultados obtenidos de los procedimientos llevados a cabo en el informe pericial.
    - En primer lugar se describen de forma detallada las evidencias digitales obtenidas, así como el procedimiento llevado a cabo, en cada caso, para su adquisición:

8.- RESULTADOS DE LOS PROCEDIMIENTOS REALIZADOS

En esta sección presentamos los resultados del trabajo realizado de acuerdo con los procedimientos descritos en la sección 4 de este informe.

8.1 Obtención de evidencias digitales

Las imágenes forenses son una copia exacta y no manipulable de los datos contenidos en los equipos informáticos originales.

Las principales características técnicas de una imagen forense son las siguientes:

- Es una copia íntegra de todos los sectores que componen un volumen físico o soporte digital. Es decir, es una copia completa (copia byte a byte) de toda la información contenida en un soporte digital. De esta forma obteniendo una imagen forense podemos garantizar que tenemos una copia con el 100% de la información original.
- Están firmadas digitalmente mediante una función HASH que permite identificar unívocamente el contenido de la imagen forense. Es decir, es posible verificar en todo momento que la información contenida en la copia es idéntica a la original. De esta forma obteniendo una imagen forense podemos garantizar la integridad de la información que se presenta.

Las imágenes forenses constituyen la forma más eficaz y fiable de preservar y presentar la información digital.

Hemos obtenido imágenes forenses de los siguientes equipos:

– Ordenador personal propiedad del Sr. Ejemplo

La obtención de imágenes se realizó siguiendo los procedimientos que a continuación se detallan:

– La toma de evidencias se produjo en el laboratorio de tecnología forense de Lazarus en San Sebastian de los Reyes, Madrid y fueron realizadas por personal especialista en prueba digital de Lazarus LFS, en presencia de testigos de la propia empresa tal y como figuran en las actas de copiado que se aportan como **Documento 1** de este informe.

– Para la adquisición de las evidencias digitales procedimos a realizar una imagen forense, de los equipos detallados en el cuadro 1 de este informe pericial.

– La obtención de las imágenes forenses fue realizada siguiendo la metodología de trabajo del departamento de Forensic Services de Lazarus LFS, basada en los estándares y mejores prácticas profesionales en tecnología forense y utilizando procedimientos y herramientas específicamente diseñados para llevar a cabo este tipo de trabajos.

– En este caso concreto, la adquisición se realizó mediante el empleo de un equipo especializado de análisis forense denominado Image Masster Solo III Forensic y el análisis forense se realizó con el software Encase Forensic versión 6.4.

– Las imágenes forenses se obtuvieron de acuerdo al siguiente proceso:

- Se realiza una doble copia de la evidencia original y se etiquetan como imagen principal e imagen secundaria. Las imágenes obtenidas contienen una copia exacta, byte a byte, del contenido completo de la evidencia.
- La relación y numeración de las imágenes originales y secundarias puede verse a continuación:

Cuadro 2: Relación de evidencias obtenidas

Número de evidencia	Descripción y tipo de evidencia	Descripción y tipo del soporte digital	Ubicación
EJEMPLO-A001	ORIGINAL	ORDENADOR personal REE HDD Samsung S/N: S08EJ1MA115070	Laboratorio Forense de Lazarus
EJEMPLO-A002	IMAGEN PRIMARIA TARGET	HDD: Western Digital S/N: WD-WXB1AA023402	Archivo LFS
EJEMPLO-A003	IMAGEN SECUNDARIA BACKUP	HDD: Western Digital S/N: WD-WXB1AA037923	Archivo LFS

Fuente: Actas de copiado (Documento 1).

- Las imágenes obtenidas son firmadas digitalmente con un algoritmo que aplica una función hash sobre el volumen completo de las imágenes, de forma que estas no puedan ser manipuladas sin modificar la firma digital original.

- El resultado de la firma digital es un código hexadecimal de 32 caracteres que denominaremos HASH de adquisición y que identifica unívocamente cada evidencia digital.

- La relación de "Códigos Hash de Adquisición" obtenidos puede verse en el *Cuadro 1: Evidencias digitales y códigos Hash de adquisición y verificación* en el apartado 5 de este informe.

- La imagen forense primera ha sido puesta en custodia en el archivo de Lazarus, en sus oficinas de Madrid. Y la imagen secundaria se lleva al laboratorio de tecnología forense de Lazarus Technology para su análisis por técnicos especializados.

- Las actas y documentación de la obtención de las imágenes forenses puede verse en el **Documento 1**.

- A continuación, se mencionan los detalles con respecto a la cadena de custodia y las autorizaciones solicitadas para llevar a cabo el informe pericial:

8.2 Documentación de la cadena de custodia.

Con el fin de garantizar la integridad de las evidencias digitales, se ha establecido una cadena de custodia sobre las imágenes forenses obtenidas.

La cadena de custodia, documenta la ubicación y la persona encargada de su custodia durante todo el ciclo de vida de las evidencias.

En la sección 5 de las actas de copiado, que se adjuntan en el **Documento 1,** pueden verse las actas y documentación de la cadena de custodia de cada una de las imágenes forenses obtenidas.

8.3 Autorizaciones

Siguiendo nuestros procedimientos internos se solicitó la autorización expresa de la Sociedad para la obtención de las evidencias digitales objeto de este informe.

Adjuntamos en el **Documento 2** las autorizaciones solicitadas para la obtención de evidencias digitales.

- Se indican a continuación los resultados detallados del análisis forense realizado en el ordenador personal del Sr. Ejemplo:

8.4 Análisis Forense de las evidencias y presentación de los resultados

8.4.1 Identificación de los buzones de correo electrónico.

Como hemos explicado anteriormente, se ha obtenido una imagen forense del ordenador personal del Sr. Ejemplo

Con la ayuda de herramientas especializadas de Tecnología Forense hemos procedido a identificar y extraer de forma automatizada todos los buzones de correo electrónico y copias de seguridad de los mismos almacenados en la imagen forense del ordenador del Sr. Ejemplo

A continuación se incluye un listado con los buzones de correo identificados

Cuadro 3: Relación de Buzones de correo y/o copias de seguridad de los mismos

Número de evidencia	Buzón de correo	Ubicación
EJEMPLO-A002	Archive.pst	D:\Exportados\EmailBruto\Administrador\archive.pst
EJEMPLO-A002	Backup.pst	D:\Exportados\EmailBruto\Administrador\backup.pst
EJEMPLO-A002	outlook.pst	D:\Exportados\EmailBruto\Administrador\Outlook.pst
EJEMPLO-A002	outlook.pst	D:\Exportados\EmailBruto\JOSEHDantiguo\outlook.pst

Fuente: Elaboración propia Lazarus

8.4.2 Recuperación de información borrada.

Con la ayuda de herramientas especializadas de Tecnología Forense hemos procedido a identificar y en los casos que ha sido posible, reconstruir la información que había sido eliminada de los buzones de correo identificados en la imagen forense del ordenador de REE

Para el procedimiento de recuperación de información se han utilizado entre otras, las siguientes herramientas forenses: Encase Forensic Edition 6.15 y Nuix.

Tras el análisis forense realizado sobre los buzones de correo identificados en el cuadro anterior han podido ser recuperados 189 correos electrónicos que habían sido borrados.

8.4.3 Identificación de las comunicaciones con el Banco de EJEMPLO

Una vez identificados todos los buzones de correos existentes y recuperados los e-mails borrados procedimos a identificar mediante la ayuda de herramientas forenses específicas para el análisis de correo electrónico todas las comunicaciones realizadas con el Banco de EJEMPLO.

En los archivos de correo analizados se identificaron los siguientes dominios de correo pertenecientes al Banco de EJEMPLO:

- @ejemplo.com

Y un dominio erróneo derivado de emails enviados a una dirección equivocada provocado posiblemente por un error en la escritura

- @ejemplo.com

En el **Anexo I** se incluye en un CD una carpeta con todos los correos electrónicos enviados o recibidos desde los dominios arriba indicados

8.5.2 Identificación de los correos electrónicos relevantes para el caso

Los contenidos de los buzones de correo identificados así los correos electrónicos borrados que han podido ser recuperados, han sido puestos a disposición del Sr. Ejemplo y sus asesores legales para su revisión por las personas competentes.

El Sr. Ejemplo y sus asesores legales, han identificado aquellos correos que han considerados más representativos para el caso.

En el **Anexo II,** se incluyen en un CD todos los correos relevantes identificados por el Sr. Ejemplo y sus asesores legales (106 correos).

A modo ilustrativo en el **Anexo III** se incluyen impresos algunos de los correos más relevantes identificados por el Sr. Ejemplo.

8.5.3 Verificación de la integridad y autenticidad de los correos electrónicos.

Con el fin de verificar la integridad y autenticidad de los correos electrónicos considerados relevantes para este caso, hemos revisado la configuración y estructura a bajo nivel de los diferentes buzones de correo identificados en la imagen forense del ordenador de REE con el fin de comprobar que no existen indicios de que hayan podido ser manipulados.

Se han analizado los metadatos incluidos en los archivos de correo y las fechas de creación y modificación de cada correo en el propio buzón. Así mismo hemos extraído y analizado las cabeceras de los correos considerados relevantes por los asesores legales de REE para verificar el origen y destino de los mismos y hemos podido comprobar que han sido enviados o recibidos por los usuarios originales configurados en el buzón de correo

Por ello, podemos concluir que no existe ninguna duda acerca de la integridad y autenticidad de los correos y que hemos verificado que todos ellos han sido enviados desde la cuenta de correo de REE y no existe ningún indicio de que estos puedan haber sido manipulados.

- De forma similar, se describen los resultados del análisis forense llevado a cabo en los sistemas de información del Banco Ejemplo:

8.5 Análisis forense de las evidencias digitales presentes en los sistemas de información del Banco de EJEMPLO.

Como parte del encargo de trabajo del Sr. Ejemplo y tal y como se recoge en nuestra propuesta de servicios profesionales, se nos pedía identificar y presentar las evidencias digitales, que pudiesen hallarse en los sistemas de información del Banco de EJEMPLO, relativas a las comunicaciones mantenidas con el Sr. Ejemplo y su familia.

A continuación se detallan las evidencias digitales, obtenidas en los sistemas del banco y el análisis forense realizado sobre las mismas:

8.5.1 Obtención de la imagen forense de las evidencias digitales presentes en los sistemas de información del Banco de EJEMPLO.

La toma de evidencias se produjo en las oficinas del Banco en la localidad de EJEMPLO y fueron realizadas por personal especialista en prueba digital de Lazarus LFS, en presencia de testigos de la propia empresa tal y como figuran en las actas de copiado que se aportan como Documento 1 de este informe.

La adquisición se realizó mediante el empleo de un equipo especializado de análisis forense denominado FTK Imager y el análisis forense se realizó con el software Encase Forensic versión 6.4.

La relación y numeración de las imágenes originales y secundarias puede verse a continuación:

Cuadro 4: Relación de evidencias obtenidas en los sistemas del Banco Ejemplo

Número de evidencia	Descripción y tipo de evidencia	Descripción y tipo del soporte digital	Ubicación
EJEMPLO-A004	ORIGINAL	Información disponible en los sistemas informáticos del Banco	Laboratorio Forense de Lazarus
EJEMPLO-A005	IMAGEN PRIMARIA TARGET	HDD: Western Digital S/N: WD-WXB1AA023402	Archivo LFS
EJEMPLO-A006	IMAGEN SECUNDARIA BACKUP	HDD: Western Digital S/N: WD-WXB1AA037923	Archivo LFS

Fuente: Actas de copiado (Documento 1).

La relación de "Códigos Hash de Adquisición" obtenidos puede verse en el Cuadro1: Evidencias digitales y códigos Hash de adquisición y verificación en el apartado 5 de este informe.

En la sección 5 de las actas de copiado, que se adjuntan en el **Documento 1,** pueden verse las actas y documentación de la cadena de custodia de cada una de las imágenes forenses obtenidas.

8.5.4 Autorizaciones

Siguiendo nuestros procedimientos internos se solicitó la autorización expresa del Banco Ejemplo para la obtención de las evidencias digitales objeto de este informe.

Adjuntamos en el **Documento 3** los procedimientos de solicitud de información, el albarán de entrega de la información y el acuerdo de confidencialidad firmado con el Banco de EJEMPLO.

8.5.5 Identificación de la información disponible en los sistemas de información del Banco Ejemplo.

Con el objeto de dar cumplimiento al requerimiento judicial para acceder a las dependencias del Banco Ejemplo y presentar las evidencias electrónicas relevantes al caso que pudieran existir en sus sistemas informáticos, elaboramos un listado con la información requerida por estos peritos al banco. Dicho listado puede verse en el **Documento 3** anexo a este informe.

Los responsables del Banco Ejemplo de acuerdo al listado previo identificaron la información disponible en sus sistemas. El albarán con el listado de la información puesta a nuestra disposición por el banco se encuentra anexo en el Documento 3

A continuación y a modo explicativo se incluye un listado con la información disponible en los sistemas del banco.

Información relevante al caso disponible en los sistemas del Banco:

- Archivo .pst con los correos electrónicos del empleado del Banco Ejemplo JEE con la familia Ejemplo.
- Log del servidor de correo con los registros de los correos enviados y recibidos a las direcciones de correo de la familia Ejemplo.
- Log del gestor documental con los registros de la incorporación de los Test de conveniencia de la Familia Ejemplo a dicha aplicación.
- Log de la aplicación MIFID del terminal financiero con la información relacionada con los test de conveniencia de la familia Ejemplo.
- Documentos en formato Word correspondiente a los contratos (previos a la firma)
- Según fuimos informados por los responsables técnicos del Banco, los logs del terminal financiero correspondientes a la apertura de los productos y cuentas contratados, no pudieron ser localizados por los técnicos de Banco Ejemplo por lo que no han podido ser analizados en este informe.

8.5.6 Análisis forense de las evidencias digitales obtenidas en los sistemas de información del Banco Ejemplo.

Análisis de los correos electrónicos:

Realizamos una imagen forense de todos los correos electrónicos intercambiados entre el empleado del Banco Juan Ejemplo Ejemplo (en adelante el Sr. Ejemplo o JEE) y la familia Ejemplo.

Dichos correos electrónicos se encontraban en una carpeta denominada "Familia Ejemplo"

Hemos realizado un análisis de las fechas incluidas en os metadatos de los correos y hemos podido verificar que estas se corresponden con las fechas de envío y/o recepción de los correos por lo que no existen indicios de que estos hayan sido manipulados o alterados.

Así mismo, hemos podido verificar que los correos aportados se corresponden con los registrados en el Log del servidor de correo, por lo que se puede afirmar que los correos aportados conforman la totalidad de las comunicaciones mantenidas entre dicho empleado y los diferentes miembros de la Familia Ejemplo.

A continuación se incluye un listado de todos los correos intercambiados entre el Sr. Ejemplo y la familia Ejemplo y las fechas incluidas en los metadatos analizados:

Correos electrónicos

Title / Subject	Content Last Modified	Content Created	Sent	Received
	15/07/2010	15/07/2010	15/07/2010	15/07/2010
RE: anulación plazo fijo	8:50	8:48	8:50	8:50
RV: NO REENEJEMPLOR: Posible	29/08/2008	29/08/2008	29/08/2008	29/08/2008
Cancelación Depos Estructurados	12:19	11:40	11:41	11:41

Continúa una relación de 120 correos adicionales que se omiten por brevedad.

El informe con el resultado completo de todos los datos analizados para cada uno de los correos puede verse en el **Anexo III.**

Así mismo, En dicho anexo se incluyen los originales de los correos electrónicos entre la Familia Ejemplo y el Banco de EJEMPLO y el log del registro del servidor de correo del Banco.

Análisis de los archivos informáticos de los contratos:

Hemos realizado una imagen forense de los archivos en formato Word que fueron utilizados para preparar los impresos para la firma de los contratos de la Familia Ejemplo

Hemos analizados los metadatos existentes en los archivos electrónicos y hemos podido comprobar que las últimas fechas de modificación de dichos archivos han sido el 3 de junio y el 26 y 27 de mayo de 2008

A continuación se incluye el listado de los archivos correspondientes a los contratos de la familia Ejemplo y las fechas de creación y modificación incluidas en los metadatos:

Contratos

Name	Content Last Modified	Content Created	File Last Modified
MARIA EJEMPLOEJEMPLO_36245.doc	03/06/2008 8:56	27/05/2008 10:54	03/06/2008 8:56
MARIA EJEMPLOEJEMPLO_36258.doc	27/05/2008 9:12	26/05/2008 16:37	27/05/2008 9:12
JOSE EJEMPLOEJEMPLO_36245.doc	03/06/2008 10:24	03/06/2008 10:15	03/06/2008 10:24
ANA MARIA EJEMPLO_36245.doc	03/06/2008 10:15	03/06/2008 10:11	03/06/2008 10:15
ANA MARIA EJEMPLO_36258.doc	26/05/2008 16:50	26/05/2008 16:20	26/05/2008 16:50
ANA MARIA EJEMPLO_36245.doc	03/06/2008 10:10	03/06/2008 9:29	03/06/2008 10:10
ANA MARIA EJEMPLO _36258.doc	26/05/2008 16:53	26/05/2008 16:52	26/05/2008 16:53

El **Anexo IV** se incluye en un CD los archivos en formato Word de los contratos de la Familia Ejemplo

Análisis de los Test de Conveniencia:

Hemos realizado una imagen forense de los archivos en formato PDF de los test de conveniencia de la Familia Ejemplo

Los archivos fueron generados desde la plataforma del gestor documental del Banco en presencia nuestra, por lo que los metadatos existentes en los ficheros electrónicos no aportan información útil para fijar la fecha de creación de los ficheros ya que esta corresponde con la fecha de nuestro acceso a las instalaciones del Banco

Con el fin de poder analizar las fechas de creación y modificación de los Test de Conveniencia, analizamos los registros de la plataforma del Gestor Documental que contenía los mencionados archivos así como los registros de la aplicación MIFID del Banco que según fuimos informados por los responsables del Banco, es la aplicación utilizada para gestionar este tipo de documentación de los clientes del Banco.

A continuación se muestra un resumen con las fechas de creación de los documentos incluidos en el registro del gestor documental:

tipo_documento	clave_interna	codigo_documento	event-date	operacion
TestConocimiento	11775728	**000860609**|21/05/2008|121740	**2008-06-11** 12:18:29.0	**crearDocumento**
TestConocimiento	11725070	**000908187**|21/05/2008|150025	**2008-06-06** 15:01:40.0	**crearDocumento**
TestConocimiento	11776696	**002667144**|21/05/2008|132521	**2008-06-11** 13:25:48.0	**crearDocumento**
TestConocimiento	11791377	**001472238**|21/05/2008|145434	**2008-06-12** 14:54:58.0	**crearDocumento**
TestConocimiento	11791377	**001472238**|21/05/2008|145434	**2008-06-12** 14:55:02.0	**crearDocumento**

A continuación se muestra un resumen con la fecha y hora del alta del Test y la firma en la aplicación MIFID según puede verse en los registros de la propia aplicación:

NUMERO INTERNO PERSONA	DIA / HORA FIRMA TEST	FECHA / HORA ALTA TEST CONVENIENCIA
860609	**2008-05-26**-12.01.06.053474	**2008-05-26**-12.00.36.503444
908187	**2008-05-26**-12.05.40.755286	**2008-05-26**-12.05.12.909283
2667144	**2008-05-26**-12.08.13.609387	**2008-05-26**-12.07.54.476879
1472238	**2008-05-26**-12.11.52.849561	**2008-05-26**-12.11.35.663806

El **Anexo V** se incluye en un CD los registros en formato Excel de la plataforma del Gestor Documental y de la aplicación MIFID con relación a los Test de Conveniencia de la Familia Ejemplo , así como los propios archivos .pdf generados en nuestra presencia por el banco.

- Por último, se muestra en su integridad el apartado 9, que presenta las conclusiones del informe pericial:

9.- CONCLUSIONES

De acuerdo con los resultados de nuestro trabajo, presentados en el cuerpo de este informe, las principales conclusiones que hemos obtenido al respecto son las siguientes:

9.1 **Hemos obtenido imágenes forenses de** todos los equipos informáticos cubiertos en el alcance de este informe y que se describen a continuación:

- **Ordenador Personal de trabajo propiedad del Sr. Ejemplo.**
- **Buzón de correo personal del Sr Ejemplo**

9.2 **Las imágenes han sido obtenidas en presencia de** los **testigos**: Dª Susana Ejemplo, asesora legal del Sr. Ejemplo y D. Manuel Ejemplo Socio Director del Laboratorio de tecnología forense de Lazarus Technology.

9.3 **Las imágenes forenses han sido obtenidas y verificadas por especialistas en tecnología forense de Lazarus Technology**.

9.4 **Las imágenes obtenidas han estado bajo custodia en todo momento y la cadena de custodia se encuentra formalmente documentada** en el documento 1, anexo a este informe. A la fecha de entrega de este informe, las imágenes se encuentran almacenadas en custodia en el archivo de las oficinas de Lazarus Technology.

9.5 **El Sr. Ejemplo y sus asesores legales han seleccionado 10 correos enviados y/o recibidos en su buzón de correo electrónico como especialmente relevantes para este caso**, estos son:

- Correo de fecha" martes, 20 de mayo de 2008 13:49" con el campo asunto "Borrador Presentación" y archivo adjunto: "PTA FAMILIA EJEMPLO .pdf*"*
- Correo de fecha "miércoles 29/10/2008 13:59" con el campo asunto RV: Perfil MIFID y archivos adjunto: "Familia EjemploEjemplo.pdf; PerfilMIFID.pdf; PerfilMIFID-1.pdf"
- Correo de fecha "miércoles 21/05/2008 17:33" con el campo asunto Confirmación cierre estructurados
- Correo de fecha "martes 02/09/2008 12:49" con el campo asunto RE: Confirmación cierre estructurados
- Correo de fecha "jueves 12/06/2008 6:06" con el campo asunto RE: Confirmación cierre estructurados
- Correo de fecha "martes 11/11/2008 14:03" con el campo asunto RE: Familia Ejemplo -Ejemplo
- Correo de fecha "miércoles 10/12/2008 21:43" con el campo asunto RV: estruturados familia Ejemplo Ejemplo y archivo adjunto: "Burofax BSA 28.11.2008.pdf*"*
- Correo de fecha "jueves 11/12/2008 19:58" con el campo asunto RV: estruturados familia Ejemplo Ejemplo y archivo adjunto: "Burofax BSA 28.11.2008.pdf*"*
- Correo de fecha "martes 21/10/2008 20:38" con el campo asunto RV: Familia Ejemplo -Ejemplo
- Correo de fecha "martes 11/11/2008 14:42" con el campo asunto RV: Perfil MIFID

Los correos seleccionados junto con sus archivos adjuntos se encuentran anexos a este informe pericial, para su revisión por las personas competentes.

9.6 **Hemos realizado un análisis forense sobre los correos seleccionados y no existe ninguna duda sobre su integridad y autenticidad**. Por lo que constituyen a nuestro juicio una copia fiel de la información original.

9.7 **Hemos accedido a las instalaciones del Banco de EJEMPLO, y obtenido una imagen forense de la información disponible en los sistemas del Banco relativa a la documentación y comunicaciones entre el Banco y el Sr Ejemplo y su familia**

9.8 La información disponible en el banco se compone de:

- Correos electrónicos entre el Banco y la Familia Ejemplo
- Documentos en formato Word utilizados para elaborar los contratos
- Test de Conveniencia firmados por la familia Ejemplo y preparados y almacenados en las aplicaciones informáticas del banco.

9.9 Hemos analizado los metadatos incluidos en archivos en formato Word que fueron utilizados para preparar los impresos para la firma de los contratos de la Familia Ejemplo **y hemos podido verificar las fechas en que estos fueron creados y firmados en los sistemas del Banco.**

A continuación se resumen las fechas de creación y modificación de los ficheros de los contratos

Contratos

Name	Content Last Modified	Content Created	File Last Modified
MARIA EJEMPLO_36245.doc	03/06/2008 8:56	27/05/2008 10:54	**03/06/2008** 8:56
MARIA EJEMPLO_36258.doc	27/05/2008 9:12	26/05/2008 16:37	**27/05/2008** 9:12
JOSE EJEMPLO_36245.doc	03/06/2008 10:24	03/06/2008 10:15	**03/06/2008** 10:24
ANA MARIA EJEMPLO_36245.doc	03/06/2008 10:15	03/06/2008 10:11	**03/06/2008** 10:15
ANA MARIA EJEMPLO_36258.doc	26/05/2008 16:50	26/05/2008 16:20	**26/05/2008** 16:50
ANA MARIA EJEMPLO_36245.doc	03/06/2008 10:10	03/06/2008 9:29	**03/06/2008** 10:10
ANA MARIA EJEMPLO_36258.doc	26/05/2008 16:53	26/05/2008 16:52	**26/05/2008** 16:53

9.10 **Hemos analizado** los registros internos de las aplicaciones informáticas del banco que contienen **los Test de Conveniencia** firmados por la familia Ejemplo **y hemos podido verificar las fechas en que estos fueron creados y firmados en los sistemas del Banco.**

A continuación se muestra un resumen con las **fechas de creación de los documentos** incluidos en el registro del **gestor documental**:

codigo_documento	event-date	operacion
000860609|21/05/2008|121740	**2008-06-11** 12:18:29.0	**crearDocumento**
000908187|21/05/2008|150025	**2008-06-06** 15:01:40.0	**crearDocumento**
002667144|21/05/2008|132521	**2008-06-11** 13:25:48.0	**crearDocumento**
001472238|21/05/2008|145434	**2008-06-12** 14:54:58.0	**crearDocumento**

Y a continuación se muestran un resumen con la **fecha y hora del alta del Test y la firma en la aplicación MIFID**

NUMERO INTERNO PERSONA	DIA / HORA FIRMA TEST	FECHA / HORA ALTA TEST CONVENIENCIA
860609	**2008-05-26**-12.01.06.053474	**2008-05-26**-12.00.36.503444
908187	**2008-05-26**-12.05.40.755286	**2008-05-26**-12.05.12.909283
2667144	**2008-05-26**-12.08.13.609387	**2008-05-26**-12.07.54.476879
1472238	**2008-05-26**-12.11.52.849561	**2008-05-26**-12.11.35.663806

Este informe pericial ha sido preparado exclusivamente para los fines descritos en la sección 3 de este informe, por lo que no debería ser distribuido a terceras partes distintas de los Tribunales Competentes, las partes implicadas en el Procedimiento y sus asesores legales. En consecuencia, este informe no debe ser utilizado para fines distintos a los descritos, por lo que no asumimos responsabilidad profesional alguna frente a personas distintas de los usuarios arriba indicados que, en su caso, pudieran tener acceso a este informe sin mediar nuestro consentimiento previo por escrito.

Bibliografía

1. Álvarez-Cienfuegos Suarez, J. Mª. *Las obligaciones concertadas por medios informáticos y la documentación*. La Ley, 1992 nº 4
2. Bacigalupo, Enrique. *El delito de Falsedad Documental*. Ed. Dykinson, Madrid, 1999.
3. Caloyannides, Michael A. *Computer Forensics and Privacy*. Artech House Inc. 2001
4. Cosic, Jasmin. *A Framework to (Im)Prove Chain of Custody in Digital Investigation Process*. Proceedings of the 21st Central European Conference on Information and Intelligent Systems, 2010
5. Delgado Martín, Joaquín. *La prueba electrónica en el proceso penal*. Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013
6. García, Paloma. *Normas para las evidencias electrónicas*. Revista de la Normalización y la Certificación. Nº 287. Noviembre 2013 http://www.aenor.es/revista/completos/287/#/6/
7. Gervilla Rivas, Carles. *Metodología para una Análisis Forense*. TFM Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC). UOC – INCIBE. Diciembre 2014. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf
8. Gimeno Sendra, Vicente. *Derecho Procesal Civil. El proceso de declaración. Parte General*. Colex 2010. 3ª edición
9. Gimeno Sendra, Vicente. *Manual de Derecho Procesal Penal*. Colex. 2010. 2ª edición
10. Illán Fernández, José María. *La Prueba Electrónica, Eficacia y Valoración en el Proceso Civil. Aranzadi Thomson Reuters*. Primera Edición, 2009.
11. López Rivera, Rafael. *Peritaje Informático y Tecnológico. Un enfoque teórico-práctico*. ISBN: 9788461608959. www.peritoit.com. 2012
12. M. Reith, C. Carr, G. Gunsch. *An examination of digital forensic models*. International Journal of Digital Evidence. Fall 2002, Volume 1, Issue 3 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.13.9683
13. Marqués-Arpa, Tomás. *Cadena de Custodia en el Análisis Forense. Implementación de un Marco de Gestión de la Evidencia Digital*. RECSI 2014.

http://web.ua.es/en/recsi2014/documentos/papers/cadena-de-custodia-en-el-analisis-forense-implementacion-de-un-marco-de-gestion-de-la-evidencia-digital.pdf

14. Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley. *Recovering and examining computer forensic evidence* October 2000. Volume 2, Nr 4
15. Montón Redondo. *Medios de reproducción de la imagen y el sonido. La prueba*. CGPJ, Madrid. 2000
16. Pérez Gil, Julio. *Prueba electrónica y prueba documental en el proceso civil: los límites de su equivalencia funcional*. Suplemento de Derecho Procesal de ElDial.com. 2006

Normativa[29]

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

[29] Todos los hiperenlaces se refieren al texto consolidado de las distintas leyes en la fecha de este trabajo

Jurisprudencia

1. STC 173/2011, de 7 de noviembre de 2011
   http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/22621
2. STC 53/2006, de 27 de febrero de 2006
   http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/5655
3. STC 153/2004, de 20 de septiembre de 2004
   http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/5158
4. STS 2047/2015 de 19 de mayo de 2015
   http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7390234
5. STS 2743/2013 de 17 de mayo de 2013
   http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6737734
6. STS 8316/2012 de 3 de diciembre de 2012
   http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6589204
7. STS 8876/2011 de 6 de octubre de 2011
   http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6234178
8. STS 6216/2011 de 16 de junio de 2011
   http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6143672
9. STS 1323/2011 de 8 de marzo de 2011
   http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=5908468
10. STS 6007/2008 de 29 de octubre de 2008
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=3425775
11. STS 4315/2008 de 18 de julio de 2008
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=43498
12. STS 6128/2007 de 26 de septiembre de 2007
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=326542
13. STS 7208/1999 de 15 de noviembre de 1999
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=2385479
14. ATS 1800/2013 de 14 de febrero de 2013
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6651360
15. ATS 2197/2012 de 9 de febrero de 2012
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=6309488
16. STSJ AND 2248/2014 de 6 de marzo de 2014
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7041998
17. STSJ PV 1118/2012 de 17 de abril de 2012
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6393993
18. SAP B 1301/2008 de 29 de enero de 2008
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=159029
19. SAP CA 122/2014 de 28 enero de 2014
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7007287
20. SAP GR 391/2013, de 26 de abril de 2013
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6780947
21. SAP M 12497/2013 de 24 de julio de 2013
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6823068
22. SAP MA 1/2011 de 31 de marzo de 2011
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=5983937
23. SAP PO 18/2014 de 10 enero de 2014
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6943951
24. AAP M 18559/2011 de 13 de diciembre de 2011
    http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=6275024

Normas técnicas

1. RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP). 2001. https://www.ietf.org/rfc/rfc3161.txt
2. RFC 3227 Guidelines for Evidence Collection and Archiving. 2002. https://www.ietf.org/rfc/rfc3227.txt
3. ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en
4. ISO/IEC 27042 Guidelines for the analysis and interpretation of digital evidence https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en
5. UNE 71505-1 Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051411
6. UNE 71505-2 Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051412
7. UNE 71505-3 Parte 3: Formatos y mecanismos técnicos. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051413
8. UNE 71506 Metodología para el análisis forense de las evidencias electrónicas http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414
9. UNE 197001 Criterios generales para la elaboración de informes y dictámenes periciales http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0046980