Grant Thornton

Ir a la web

Compliance Advisory LAB

Investigación sobre Compliance, *Forensic* y R.P.P.J. de Grant Thornton

Report 8

La «Evidencia Digital»: tipos de procedimientos de análisis y configuración

Fernando Lacasa Cristina
Rafael Aguilera Gordillo
Codirectores del Compliance Advisory LAB

Septiembre 2022

Report 8

La «Evidencia Digital»: tipos de procedimientos de análisis y configuración

¿Cuál es el papel que juega la evidencia digital en el actual panorama empresarial?

¿Cómo se desarrolla el análisis de la evidencia digital?

¿En qué consiste el conocido como procedimiento eDiscovery?

¿De qué fases se componen los protocolos de extracción y análisis realizados por los departamentos especializados en Forensic?

La «evidencia digital» se ha convertido en un elemento primordial, tanto en el marco de las investigaciones internas corporativas como en los procesos judiciales. A pesar de ello, muchos de sus aspectos clave siguen siendo muy poco conocidos para los profesionales ligados al ámbito del Compliance o al asesoramiento legal corporativo. Así, suele desconocerse la metodología de análisis aplicada a la evidencia digital, cada fase que la conforma, numerosos conceptos utilizados o los sujetos expertos en Forensic que intervienen en esta tipología de procedimientos (analistas y técnicos informáticos).

En el presente *report* del Compliance Advisory LAB se abordarán aspectos fundamentales sobre el análisis de la evidencia digital. El objetivo es ofrecer información relevante para aquellos profesionales que detentan responsabilidades ligadas a la ejecución de «sistemas de *compliance*» o «sistemas internos de información». Sin duda, este texto les ayudará a tener una imagen más nítida sobre este tipo de procesos, lo que repercutirá favorablemente a la hora de adoptar mejores decisiones cuando se encuentren en escenarios que requieran de este tipo de estudios.

El análisis de la evidencia digital en ento corporativos puede tener lugar en distintos contextos (p. ej.: ante la apreciación directa de un posible incumplimiento, a raíz de la recepción de un aviso en el canal de denuncias o sistema interno de información, cuando se ha incoado una investigación por parte de los poderes públicos, etc.); en cualquier caso, siempre que se respete el marco legal y la doctrina jurisprudencial que se ha ido erigiendo por el Alto Tribunal en materia de licitud probatoria, protección del derecho a la intimidad y expectativa de privacidad, la legitimidad de este tipo de actuaciones queda fuera de toda duda.

Entre el **amplio elenco de preceptos que pueden encontrarse en nuestro ordenamiento jurídico para dar soporte a esta tipología de actuaciones indagatorias**, pueden citarse, entre otros muchos, los Arts. 33 y 38 de la Constitución, Art. 225 de Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital o el Art. 20 del Estatuto de los Trabajadores[1]. Este último, en su apartado 3, señala: «*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad*». Sobre tales facultades del empresario, cabe señalar lo dispuesto por el Tribunal Constitucional en sentencia número 241/2012:

«*... en el marco de las facultades de autoorganización, dirección y control correspondientes a cada empresario, "no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales"...*»

Asimismo, en la esfera jurídico-penal, el deber de control y supervisión por parte del empresario para evitar que las fuentes de riesgo que implican la actividad corporativa deriven en delitos que lesionen bienes jurídicos (incurriendo en posibles responsabilidades penales) no solo amparan actuaciones indagatorias, sino que constituyen un claro incentivo para mantener una actitud especialmente proactiva, bien por parte del empresario, bien por parte de profesionales expertos en quien este delegue algunas de sus funciones originarias (p. ej.: *compliance officer*, responsables del sistema interno de información o canal de denuncias, etc.).

De hecho, puede constatarse cómo los poderes públicos están promoviendo que las propias empresas, asociaciones, fundaciones, etc. refuercen su capacidad de vigilancia y detección de incumplimientos. El propio contenido del Art. 31 bis del Código Penal viene a impulsar este particular, siendo particularmente relevantes el cuarto y sexto de los requisitos[2] que ha de satisfacer todo programa de prevención o, en su caso, sistema de *compliance*, para poder acogerse a la -trascendental- exención de responsabilidad penal de la persona jurídica (igualmente, resulta oportuno señalar la relevancia de lo contemplado en la condición 4a del apartado 2 de este mismo precepto). Por su parte, el Art. 31 quater C.P. también vienen a reforzar la importancia de las actuaciones indagatorias realizadas por la propia organización, en tanto que señala como circunstancias atenuantes específicamente aplicables a las personas jurídicas la comunicación o confesión de la infracción cometida en el seno de la organización a las autoridades y la colaboración en el proceso aportando evidencias nuevas y decisiva[3].

La Fiscalía General del Estado ahonda en lo expuesto cuando en su Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015[4] vienen a valorar muy

1. Este particular ha sido ratificado, en multitud de ocasiones por el Tribunal Supremo; resultan especialmente significativas las siguientes manifestaciones realizadas por el Alto Tribunal en su sentencia número 715/2021 de 22 de abril: «*El supuesto que hoy centra nuestra atención es un ejemplo paradigmático de esa fricción generada por el derecho del trabajador a su propia intimidad y la facultad del acusado, el empresario Manuel , de fiscalizar el uso adecuado de los elementos productivos puestos a disposición de su empleado. Ambos derechos tienen un reconocimiento normativo explícito. En efecto, las leyes laborales otorgan al empresario la capacidad de organización del trabajo. Además, le reconocen la facultad de control y vigilancia sobre el cumplimiento contractual -cfr. arts. 5 a) y c) y 20.1.2 y 3 del Estatuto de los Trabajadores aprobado por RDL 2/2015, 23 de octubre, que derogó el RDL 1/1995, 24 de marzo-. En definitiva, el empresario goza de la capacidad para adoptar las medidas que aseguren la adecuada utilización del material puesto a disposición del trabajador. Y este poder de dirección, imprescindible para la buena marcha de la organización productiva, no es ajeno a los derechos proclamados en los arts. 33 y 38 de la CE (cfr. SSTC 170/2013; 98/2000; 186/2000 y 241/2012, entre otras)...*»

2. Apartado 5 del Art. 31 bis C.P.: «*4.o Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.[...]*

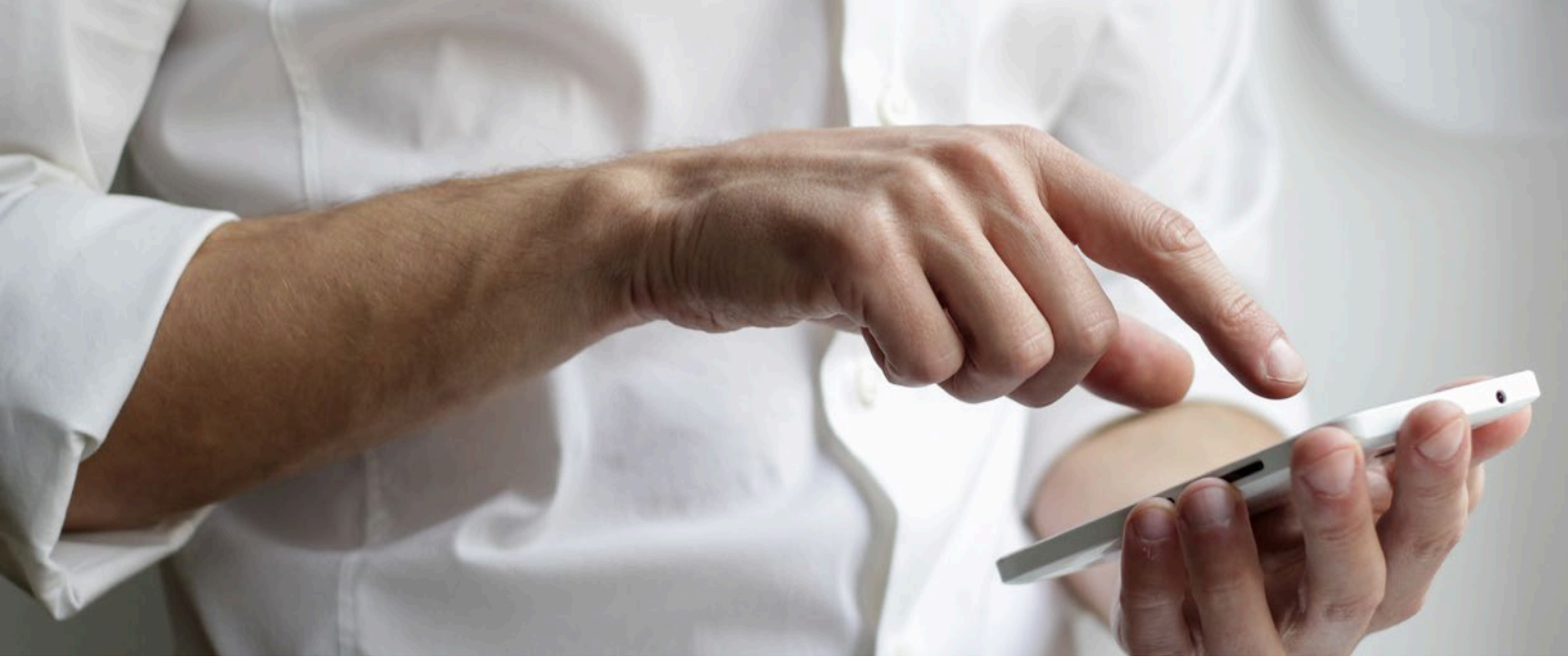
6.o Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.».

3. Recordemos que la literalidad de las letras a) y b) del artículo 31 quater contempla, como atenuantes para las personas jurídicas: «*Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:*

a) Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades.

b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos. [...]»

4. Recurso disponible en: https://www.boe.es/buscar/doc.php?id=FIS-C-2016-00001



positivamente la capacidad de la persona jurídica para detectar incumplimientos (llegando a interpretar como circunstancias eximentes aquellas que, en puridad, tendrían encaje como atenuantes). Así, en el apartado «5.6 Criterios para valorar la eficacia de los modelos de organización y gestión» se dice lo siguiente:

«Sexta.- Si bien la detección de delitos no está expresamente incluida en la enunciación ni en los requisitos de los modelos de organización y gestión, forma parte, junto con la prevención, de su contenido esencial. Teniendo en cuenta que cualquier programa de prevención, por eficaz que sea, soportará un cierto riesgo residual de comisión de delitos, la capacidad de detección de los incumplimientos lucirá como un elemento sustancial de la validez del modelo.

En consecuencia, los Sres. Fiscales concederán especial valor al descubrimiento de los delitos por la propia corporación de tal manera que, detectada la conducta delictiva por la persona jurídica y puesta en conocimiento de la autoridad, deberán solicitar la exención de pena de la persona jurídica, al evidenciarse no solo la eficacia del modelo sino su consonancia con una cultura de cumplimiento corporativo.»

«Novena.- Las actuaciones llevadas a cabo por la persona jurídica tras la comisión del delito han de ser igualmente evaluadas. La adopción de medidas disciplinarias contra los autores o la inmediata revisión del programa para detectar sus posibles debilidades, introduciendo en su caso las necesarias modificaciones, son muestra del compromiso de los dirigentes de la corporación con el programa de cumplimiento.

Del mismo modo, la restitución, la reparación inmediata del daño, la colaboración activa con la investigación o la aportación al procedimiento de una investigación interna, sin perjuicio de su consideración como atenuantes, revelan indiciariamente el nivel de compromiso ético de la sociedad y pueden permitir llegar a la exención de la pena. Operarán en sentido contrario el retraso en la denuncia de la conducta delictiva o su ocultación y la actitud obstructiva o no colaboradora con la justicia.»

La Directiva europea conocida como *directiva whistleblowing o de protección al denunciante*[5] constituye uno de los más recientes ejemplos de esta corriente en la cual los poderes públicos vienen a reforzar o subrayar la trascendencia de que las organizaciones cuenten con una autorregulación que contemplen sistemas adecuados para alertar, detectar y reaccionar adecuadamente frente a incumplimientos cometidos en su seno. La citada Directiva impone a los Estados que establezcan obligaciones normativas para que, tanto las administraciones públicas como los agentes privados, dispongan de canales adecuados para trasladar avisos sobre incumplimientos y mecanismos de protección al denunciante o informante. Como resulta conocido, en España tenemos un ***Anteproyecto de Ley de Protección al Informante***[6] que tiene por objeto (una vez se apruebe por el Congreso) transponer la *directiva whistleblowing*, pero que profundiza en las obligaciones y extiende el ámbito material originariamente fijado en la directiva[7]. Como se expuso en el Report 7 del Compliance Advisory LAB, la aprobación definitiva de este texto conllevará la adopción de canales para informar o alertar de posibles irregularidades (o como el Anteproyecto los denomina: «sistema interno de información») en todo tipo de organizaciones con más de 49 empleados, lo que va a provocar, irremediablemente, un aumento generalizado de las actuaciones de indagación o investigaciones internas corporativas originadas por la recepción de ese tipo de avisos.

Al margen de las disposiciones que promueven actuaciones de indagación realizadas a iniciativa de las propias organizaciones, los resultados de este tipo de acciones ofrecen a los tomadores de decisiones mayor información sobre qué

5. Directiva 2019/1937 del Parlamento y del Consejo de fecha 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Recurso disponible en: https://www.boe.es/doue/2019/305/L00017-00056.pdf

6. Denominado Anteproyecto de Ley para proteger a las personas que informen sobre infracciones normativas corrupción y de lucha contra la corrupción. Recurso disponible en: https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/APL%20INFORMANTES%20TRaMITE%20AUDIENCIA%20E%20INFORMACION%20PuBLICA_0803.pdf

7. Para profundizar en el contenido de dicho anteproyecto, en los efectos que va a generar sobre los sistemas de *compliance* y en los interrogantes que suscita vid. Report 7 «SISTEMA INTERNO DE INFORMACIÓN»: LA PRÓXIMA -GRAN- OBLIGACIÓN PARA TODA PERSONA JURÍDICA O FÍSICA CON MÁS DE 49 TRABAJADORES.

sucedió exactamente, lo que posibilita adoptar las estrategias más adecuadas, tanto en una vertiente interna (*ad intra*) como externa, en relación con los poderes públicos u otros agentes (ad extra). Además, en el concreto ámbito que ahora nos ocupa, la evidencia digital recabada puede hacerse valer en procesos civiles, penales, laborales, etc. La aportación en los tribunales de la evidencia digital extraída por las corporaciones o particulares podrá desplegar distintos efectos en materia probatoria según la estructura, contenido, la acreditación de su integridad. Sobre el primer ámbito, resulta oportuno traer a colación lo señalado por Delgado Martin respecto a la prueba digital[8]:

«… fuente de obstáculos radica en la fiabilidad de la prueba digital, es decir, la acreditación de su autenticidad e integridad, especialmente cuando la prueba es impugnada por alguna o varias de las partes en el proceso. Son bien recibidos todos los esfuerzos de estandarización y protocolización de actuaciones en el ámbito de la investigación pública; y en las investigaciones privadas están llamados a jugar un papel fundamental los servicios electrónicos de confianza regulados en el Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE). ***Este Reglamento ha sido desarrollado en España por la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza; destacando especialmente la nueva redacción dada al artículo 326 de la Ley de Enjuiciamiento Civil…»***.

En la jurisdicción penal, los criterios de validez como prueba en el proceso de la -evidencia digital recabada- han sido detalladamente analizados en la célebre STS núm. 489/2018 de 23 de octubre, donde se analizan conceptos como «expectativa de privacidad» y «utilizabilidad» de la evidencia. Otras sentencias relevantes son la STS núm. 56/2022 de 24 de enero y la STS 328/2021 de 22 abril. En materia general de ilicitud probatoria de evidencias de particulares destaca la STS 116/2017 de 23 de febrero y la STC (Pleno) 97/19 de 16 de julio. Por otro lado, cabe traer a colación lo señalado por Armenta Deu respecto a los criterios para una válida aportación al proceso penal de la evidencia digital como correos electrónicos, documentos de redes, etc.[9]:

«-cumplir los presupuestos de las medidas limitativas de derechos fundamentales;

-aportarse al proceso mediante un medio probatorio adecuado: en formato papel, como documento electrónico; y a través de copia del disco duro o del disco duro del servidor al que llegó el correo electrónico, con su correspondiente código hash calculado ante fedatario público; acompañándose del correspondiente informe, cuyas conclusiones podrán incorporarse mediante prueba pericial; o recurriendo a algún «prestador de servicio de confianza», conforme a lo dispuesto en el Reglamento UE/910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior;
-salvaguardar la cadena de custodia (arts. 777.2,1,II y III LECrim), y
-reproducirse correctamente en el juicio (art. 797,2,1,II y III LECrim.».

En materia laboral, resulta particularmente relevante la STS núm. 119/2018 de 8 de febrero y son también importantes[10] las siguientes sentencias del Tribunal Constitucional: SSTC 57/1994 y STC 143/1994. En todo caso, las actuaciones indagatorias que extraigan datos de naturaleza digital deben prestar especial atención a lo recogido en el Art. 20 bis del Estatuto de los Trabajadores, que dispone lo siguiente: «*Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales*».

Por su parte, el Art. 87 Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tras reconocer el derecho de los trabajadores a la protección de su intimidad en el uso de los dispositivos digitales de la empresa, permite a la corporación el acceso a esta tipología de dispositivos a los efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de los mismos. El límite, conforme a la doctrina jurisprudencial supracitada, es ofrecer seguridad a los empleados acerca de su expectativa de intimidad del uso de tales dispositivos, mediante la previa fijación de los criterios

8. DELGADO MARTIN, J.; «Reflexiones sobre el estado actual de la transformación digital de la justicia», en Revista Acta Judicial, (8), 2021, pp. 27-43

9. ARMENTA DEU, T.; «Regulación legal y valoración de prueba digital…», en Revista de Internet, Derecho y Política, UOC, 2018, pp. 72. Esta autora sostiene los siguiente: «*Cuestión diferente será la valoración que corresponda a cada uno de los medios probatorios y la eventual valoración conjunta, aplicando las reglas de la sana crítica, o lo que es igual, el principio de libre valoración (art. 741 LECrim) y el resultado final. Aspectos que dependen, a su vez, del medio probatorio incorporado al proceso, su autenticidad la postura procesal de las partes…"[…]*

La impugnación de la autenticidad o integridad por alguna de las partes revertirá en la necesidad de acreditar los hechos mediante otro medio probatorio, que atendidas las complejidades técnicas suele ser la pericia, aunque no solo.»

10. A este respecto, también es útil la STSJ Madrid de 8 de julio de 2019.

de utilización de estos medios de trabajo y la concreción de los posibles usos privados, que deberán ser previamente comunicado a los empleados. Asimismo, en caso de apreciarse una irregularidad con posible relevancia penal, la empresa puede sancionar a su empleado sin tener que esperar a la finalización del proceso penal que se hubiera incoado como consecuencia de los mismos hechos. Así lo expone la STS de 9 de febrero de 2017 cuando afirma:

«La sanción constituye una facultad del empleador, el cual, incluso si entendiera innecesaria o irrelevante su depuración penal -firme o no-porque, por ejemplo, considerara que dispone de elementos de prueba suficientes para acreditar los hechos imputados al trabajador (desde luego, es el empresario el obligado a acreditarlos), puede proceder a sancionar -o no-antes o después del inicio de cualquier trámite penal».

Al margen de las particularidades de cada jurisdicción, un factor determinante a tener en cuenta a la hora de valorar la evidencia digital es no obviar el carácter sensible de ciertos datos y examinar si es resultado de un adecuado *test de proporcionalidad*[11] (a tal efecto, resulta determinante atender a los criterios de la doctrina Barbulescu). Es decir, para una adecuada extracción y análisis de la evidencia digital resulta absolutamente necesario contar con profesionales expertos en este tipo de actuaciones y disponer de unos procedimientos rigurosos y actualizados.

Pues bien, como apuntábamos al comienzo de este *report*, a continuación, vamos a exponer los aspectos clave y fases de tres complejos procedimientos de análisis de la evidencia digital:

- **Procedimiento de análisis de evidencia digital eDiscovery;**
- **Procedimiento de análisis para la obtención de conclusiones;**
- **Procedimiento de confirmación de hipótesis.**

A este respecto, resulta pertinente subrayar que el procedimiento de análisis de evidencia digital mediante eDiscovery es el proceso de referencia y el que tiene mayor relevancia. Es este el que cuenta con amplio reconocimiento y sobre el que puede encontrarse abundante literatura, especialmente en el mundo anglosajón. No en vano se trata del procedimiento más utilizado por los equipos o departamentos de Forensic en esas jurisdicciones.

El segundo de los procedimientos que se va a exponer, el procedimiento de análisis para la obtención de conclusiones, también es aplicado por estos departamentos especializados, sobre todo en la elaboración de informes periciales, siendo su uso mucho más frecuente en España. Finalmente, el tercero de los procedimientos que se va a abordar, aquel referido como procedimiento de confirmación de hipótesis, tiene cariz de propuesta. Y es que, aunque no cuente con suficiente bagaje en el terreno empírico, podría jugar un relevante papel en determinadas circunstancias.

11. Recordemos, en este marco, la aplicación de medidas restrictivas han de aplicarse bajo la observancia del conocido como test de proporcionalidad: -juicio de idoneidad; -juicio de necesidad, y -juicio de proporcionalidad (en sentido estricto).

1. Análisis de evidencia digital mediante «eDiscovery».

El procedimiento nuclear o "primer" procedimiento de análisis de la evidencia digital que se va a exponer es el conocido como **eDiscovery** (o Electronic Discovery). Este proceso tiene como propósito la identificación, recopilación y descarte de archivos informáticos de un "universo de datos" extenso, al objeto de buscar, recuperar y presentar los materiales más relevantes de aquel. A tal efecto, se recurre a la utilización de métodos de identificación de documentos que posibiliten su examen, a través de la aplicación de criterios de búsqueda, selección y descarte. Asimismo, resulta conveniente que el proceso incorpore métricas que posibiliten una cuantificación de precisión e integridad del resultado final[12]. En consecuencia, se trata de un **método de extracción de documentación relevante que nos permite pasar de un colosal volumen de información (que imposibilita a las partes o al tribunal realizar una valoración de su contenido) a otro volumen final que sí permite su estudio y valoración**.

El «Electronic Discovery Reference Model» (EDRM, en adelante) supone una de las aportaciones metodológicas más importantes a nivel internacional en el marco del procedimiento eDiscovery[13]. EDRM constituye una comunidad de profesionales especializados[14] y con amplia experiencia profesional que desarrollan marcos o estándares de actuación en este campo, por lo que goza de una aceptación generalizada.

Como se apuntaba, el procedimiento viene a reducir el «volumen» (número de elementos originariamente existentes en la evidencia digital recabada) al mismo tiempo que va incrementando el grado de «relevancia media» de los datos que permanecen. Por «relevancia media» de los datos que radican en la evidencia digital debemos entender aquellos datos importantes o que guardan vínculos con el objeto del análisis[15]. En estas operaciones es capital que se minimice el número de elementos relevantes que, en ese proceso de simplificación, puedan pasarse por alto o perderse.

Se trata de buscar y retener documentos de relevancia que estén ligados al caso concreto. En consecuencia, el grado de conocimiento que se tenga sobre el caso influirá e influye a la hora de obtener mayor o menor información de ese mar de documentos recabados. Cuanto más conocimiento del caso, más información relevante podrá recabarse -y así progresivamente-. Puede percibirse, por tanto, como un proceso iterativo y en ciclo.

Asimismo, la propia idiosincrasia de este procedimiento viene a reafirmar que no se realiza un análisis prospectivo en la evidencia digital recabada. Y es que, la dinámica de este procedimiento persigue la búsqueda de información relevante de un caso concreto a través de la noción «relevancia media» (si se carece de dicha variable ligada al caso concreto, este procedimiento no puede llevarse a cabo).

Los profesionales con mayor **protagonismo en este procedimiento son los conocidos como «analistas», aunque también resulta esencial el papel de los técnicos informáticos o expertos en el uso de las herramientas utilizadas en este procedimiento** (p. ej.: *Relativity*[16], *Nuix*[17], etc.). En las siguientes páginas se expondrán las fases del procedimiento de eDiscovery; a este respecto cabe indicar que, mientras que los analistas juegan un papel especialmente trascendental en la fase de identificación, revisión y análisis, los técnicos informáticos lo hacen en las fases de identificación, preservación, adquisición, procesamiento y producción (ofreciendo, además, un importante soporte durante todas las fases).

12. The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fourth Edition, 2014. https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary
13. https://edrm.net/resources/frameworks-and-standards/edrm-model/
14. https://edrm.net/
15. Dado que aquellos datos ligados a la materia del análisis se encuentran inmersos en un conjunto amplísimo de datos (de hecho, es habitual que se encuentren entre millones de elementos que no guardan relación en el objeto del examen), la relevancia media tiende a cero.
16. https://www.relativity.com/
17. https://www.nuix.com/solutions/corporations/ediscovery

El resultado del proceso será un elenco de documentos obtenidos del conjunto de la evidencia digital que son relevantes para el caso en cuestión. A su vez, junto con tales documentos, han de entregarse los trabajos realizados en cada fase, los criterios y procedimientos de búsqueda aplicados.

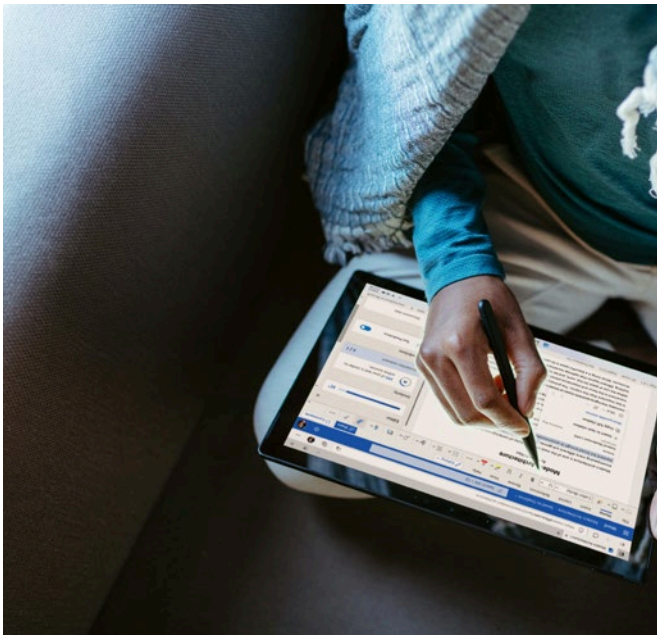
En este sentido, resulta muy importante subrayar que en el procedimiento eDiscovery las decisiones tomadas por los analistas pueden originar que varíe notablemente el resultado final del procedimiento. Las fases de identificación, revisión o análisis son aquellas especialmente susceptibles de generar modificaciones que influyan en el resultado final. Y es que, cualquier decisión tomada para seleccionar -o, en su caso, desechar- elementos va a resultar trascedente. Por tanto, se tratan de decisiones que deben ser razonadas y que han de ser sometidas a «contradicción» en el foro o sede judicial correspondiente.

A continuación, pasamos a describir las fases del procedimiento de eDiscovery. A tal efecto -y para facilitar su comprensión-, las ilustramos mediante el siguiente gráfico.

A Fase de Identificación

La finalidad de esta primera fase es la identificación y validación de las fuentes potenciales de evidencia digital relevante. Para ello hay que conocer los datos iniciales de la cuestión a responder e identificar i) las herramientas y bases de la empresa y ii) las personas y los equipos electrónicos relacionados con ellas que puedan contener la información relacionada con el caso (EDRM, 2010)[18]. Esto evidentemente implica el conocimiento de la estructura y herramientas del sistema informático de la empresa o institución, así como los datos existentes sobre los hechos, sus implicaciones legales y su estructura organizativa formal e informal.

Una vez identificada la información objeto de análisis –independientemente del soporte en el que se encuentre-, se habrá reducido el volumen de los datos de la todavía potencial «evidencia digital», y se ha incrementado la relevancia media de los mismos, al desechar muchos equipos y sistemas no relacionados con el objeto del análisis. Para ello, la metodología prevé, entre otros análisis, entrevistas a las personas identificadas como relevantes, con la finalidad de conocer sus funciones, estructura de datos en sus herramientas informáticas (AENOR, 2016)[19], su conocimiento e intervención en el objeto del análisis y, especialmente, en qué tipo de documentos, archivos o bases puede encontrarse la información buscada. Por último, hay que comprobar que en todos los casos, las fuentes de información estén relacionadas con el objeto del análisis y son accesibles desde un punto de vista técnico y legal, a lo que el procedimiento EDRM denomina "certificación" (EDRM, 2010)[20].



18. EDRM. 2010. Identification Guide. EDRM. https://edrm.net/resources/frameworks-and-standards/edrm-model/identification/
19. UNE-ES ISO/IEC 27037:2016. Tecnología de la Información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas. 2016.
20. EDRM. 2010. Identification Guide. EDRM. https://edrm.net/resources/frameworks-and-standards/edrm-model/identification/

B Fase de Preservación

Esta fase no está muy desarrollada en el modelo, al depender en gran medida de las particularidades de las fuentes potenciales de información identificadas y de las circunstancias especiales del caso. La finalidad de esta fase es la de establecer las medidas necesarias para evitar que la información pueda ser modificada o destruida (EDRM, 2010)[21]. Es en este momento cuando comienza la cadena de custodia de los dispositivos identificados. Normalmente estos dispositivos se precintan y custodian hasta que es posible realizar la siguiente fase (AENOR, 2013)[22], pero la variedad de situaciones existentes hace que las medidas a tomar y su intensidad sean muy diferentes en cada caso. A modo de ejemplo, toda la información que actualmente tienen en las compañías en «la nube» o en los mismos servidores de aplicaciones o ficheros no pueden ser precintados pero si deben aplicarse medidas para la preservación de la información que contienen.

C Fase de Adquisición

Esta fase tampoco se encuentra muy desarrollada al ser eminentemente técnica y depender en cierta medida de normativas e instituciones de cada país y de la evolución constante de la tecnología. Por otra parte, la parte técnica esta descrita y normada en gran número de publicaciones. Su finalidad es la adquisición de la potencial «evidencia digital» relevante de forma que cumpla con las exigencias legales, de proporcionalidad, eficiencia y concreción (no prospectiva) que el caso y la finalidad del análisis requieran (AENOR, 2013)[23] manteniendo en todo momento la integridad de la información adquirida y garantizando la no alteración o manipulación de ésta. Es frecuente la adquisición de los dispositivos informáticos ante fedatario público, o ante testigos, dejando una copia bajo depósito en la notaría. También el uso de la huella digital[24] u otros procedimientos que garantizan la citada no manipulación de esta, y verificación, si fuera necesario, por la otra parte (EDRM, 2010)[25].

Estas dos últimas fases son eminentemente técnicas y, aunque imprescindibles para el análisis, no forman parte de este estrictamente hablando desde nuestro punto de vista, puesto que no disminuyen el volumen ni aumentan la relevancia media.

D Fase de Procesamiento

La fase de Procesamiento todavía es una fase técnica, si bien ya empieza a enfocarse el trabajo de acuerdo con las finalidades del proyecto. En este sentido la finalidad de esta fase es la de identificar los ítems de la «evidencia digital» apropiados para una revisión de acuerdo con la finalidad del proyecto (EDRM, 2010)[26]. Esta fase se lleva a cabo mediante herramientas informáticas forenses muy avanzadas que permiten la identificación de los metadatos, la normalización de los formatos, el indexado (identificación de texto) de todos los elementos (metadatos y contenido) de manera que se pueda realizar la búsqueda posterior. También se aplican técnicas de reconocimiento de texto de aquellas imágenes o documentos PDF que puedan contenerlos, como escrituras que estén en formato de imagen sin texto reconocido.

En esta fase sí se produce un avance importante en el proceso de reducción del volumen de la evidencia y aumento de su relevancia, puesto que se excluyen todos aquellos elementos que no contienen información útil para el proyecto, como por ejemplo archivos de sistema o archivos conocidos. Posteriormente se procede a la eliminación de duplicados, por ejemplo, de los mensajes que puedan encontrarse repetidos por aparecer varias veces en una cadena de correos (EDRM, 2010)[27] o en diferentes fuentes de información de las que conforman la «evidencia digital».

E Fase de Revisión

La revisión de documentos es la fase más crítica del proceso, y se utiliza para identificar documentos que puedan tener trascendencia para el caso concreto. Es el momento en el que el equipo de análisis puede comenzar a obtener una mayor comprensión de las cuestiones fácticas en un caso y donde las estrategias de búsqueda pueden surgir y comenzar a desarrollarse en función del tipo de información que se encuentra en la «evidencia digital» y en otras fuentes de información que conformen nuestra investigación (i.e. registros oficiales, fuentes abiertas, contabilidad…). Inevitablemente, se implementarán diferentes estrategias para revisar los documentos en preparación para la producción, sin embargo, el hilo común es la necesidad (a) de comprender el alcance de la revisión, (b) de establecer la supervisión y los procedimientos para gestionar los revisores y (c) seleccionar el proveedor, las herramientas y la plataforma adecuados para la revisión (EDRM, 2010)[28].

21. EDRM. 2010. Preservation Guide. [En línea] 2010. [Citado el: 20 de 11 de 2021.] https://edrm.net/resources/frameworks-and-standards/edrm-model/preservation/
22. EDRM. 2010. Identification Guide. EDRM. https://edrm.net/resources/frameworks-and-standards/edrm-model/identification/
23. UNE 71506: 2013 Teconologías de la Información (TI). Metodología para el anállisis forense de evidencias electrónicas. Norma Española. 2013.
24. Secuencia de valores resultado de aplicación de una función *hash* a un fichero electrónico (UNE 71505-1. Tecnologías de la Información. Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. 2013).
25. EDRM. 2010. Collection Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/collection/
26. EDRM. 2010. Processing Guide. 2010. https://edrm.net/resources/frameworks-and-standards/edrm-model/processing/
27. EDRM. 2010. Processing Guide. 2010. https://edrm.net/resources/frameworks-and-standards/edrm-model/processing/
28. EDRM. 2010. Review Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/review-guide/

En todo caso, esta fase de revisión viene a ser la preparación y planificación de la fase de análisis, y para ello, tras el procesamiento de la información, se hacen pruebas sobre el conjunto de la evidencia para ver volúmenes de documentos, resultados respecto a determinadas búsquedas, custodios y volumen de elementos a ellos pertenecientes, flujos de información en cuanto a las comunicaciones, mayores emisores y receptores, volumen total de elementos que arroja la herramienta informática forense fruto de búsquedas iniciales con términos y estrategias de búsqueda relacionadas con el objeto del proyecto, etc. Toda esta operativa permite al analista un mayor conocimiento de la evidencia, de forma general, de manera que le permita establecer la estrategia de búsqueda (o DRS – Digital Review Strategy).

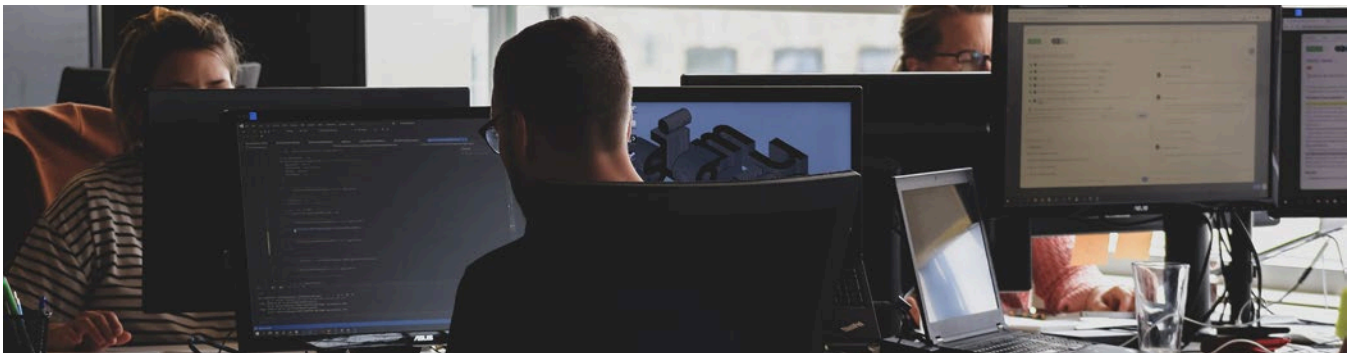
F Fase de Análisis

La fase de Análisis consiste principalmente en la aplicación de los criterios de selección de los elementos que tienen relación con el proyecto, o bien los criterios de descarte de aquellos que no tengan esta relación, todo ello con la información existente hasta el momento, que puede provenir de entrevistas, informes de hechos, términos de búsqueda, lista de custodios, sus biografías y vinculaciones, listado de personas relacionadas con los hechos, cronología de hechos y documentos procesales (EDRM, 2010)[29]. Estos criterios se van perfeccionando a medida que se va conociendo más información tanto del propio análisis como de fuentes externas a la investigación (Association of Chief Police Officers, 2012)[30].

El objetivo es extraer del conjunto de la evidencia digital el subconjunto relevante de documentos para su revisión y producción final de una manera legalmente defendible y razonable, si bien al tratarse de datos no estructurados[31] se agravan las dificultades para aplicar de forma eficaz una estrategia de búsqueda de documentos que no se conocen antes de la búsqueda (GENE EAMES, 2010).

Como se señala en el EDRM White Paper «El objetivo de cualquier criterio de selección de la evidencia electrónica es un resultado de búsqueda en el que se logre una buena recuperación y una buena precisión: que el resultado de la revisión sea una alta tasa de respuesta, acompañado de una garantía razonable de que todo lo que se suponía que debía revisarse se ha incluido de hecho para la revisión» (GENE EAMES, 2010)[32], señalándose que esto se consigue principalmente a través de la iteración, esto es, «el proceso debe iterar a través de múltiples intentos para realizar la búsqueda correctamente. Al probar los datos (tanto lo que se selecciona como lo que no se selecciona), se puede mitigar el riesgo de que falten datos sistemáticamente y crear documentación sobre la razonabilidad del proceso, mientras que al mismo tiempo se reduce la cantidad de dinero desperdiciado en el procesamiento y revisión de documentos irrelevantes».

Durante toda esta fasese realiza el análisis de los elementos a través de su lectura y la clasificación en determinadas categorías, de acuerdo con el objeto del trabajo, como pueda ser su calificación respecto a su importancia o interés, o bien por su temática, o cualquier otro tipo de clasificación útil para la finalidad del proyecto.



29. EDRM. 2010. Analysis Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/analysis/

30. Association of Chief Police Officers. 2012. ACPO Good Practice Guide for Digital Evidence. Londres : Police Central e-crime Unit, 2012.

31. Aquellos en los que «las aplicaciones utilizadas para crear estos archivos no tienen restricciones en cuanto al contenido. Un usuario puede incluir cualquier tema, incluir cualquier número de temas diferentes y no se limita a ningún vocabulario, ortografía, gramática o estilo de escritura general en particular. El lenguaje contenido en los documentos de texto incluye matices, ambigüedades e inexactitudes. La mayoría de los documentos que se encuentran en la evidencia digital no se han sometido a ninguna revisión editorial ni se les han impuesto restricciones sobre el uso del vocabulario» (GENE EAMES, 2010), traducción de los autores. GENE EAMES, D.J., D'AMBRA, G. y A. 2010. "Once is Not Enough: The Case for Using an Iterative Approach to Choosing and Applying Selection Criteria in Discovery". EDRM White Paper. 2010.

32. GENE EAMES, D.J., D'AMBRA, G. y A. 2010. "Once is Not Enough: The Case for Using an Iterative Approach to Choosing and Applying Selection Criteria in Discovery". EDRM White Paper. 2010.

G Fase de Producción

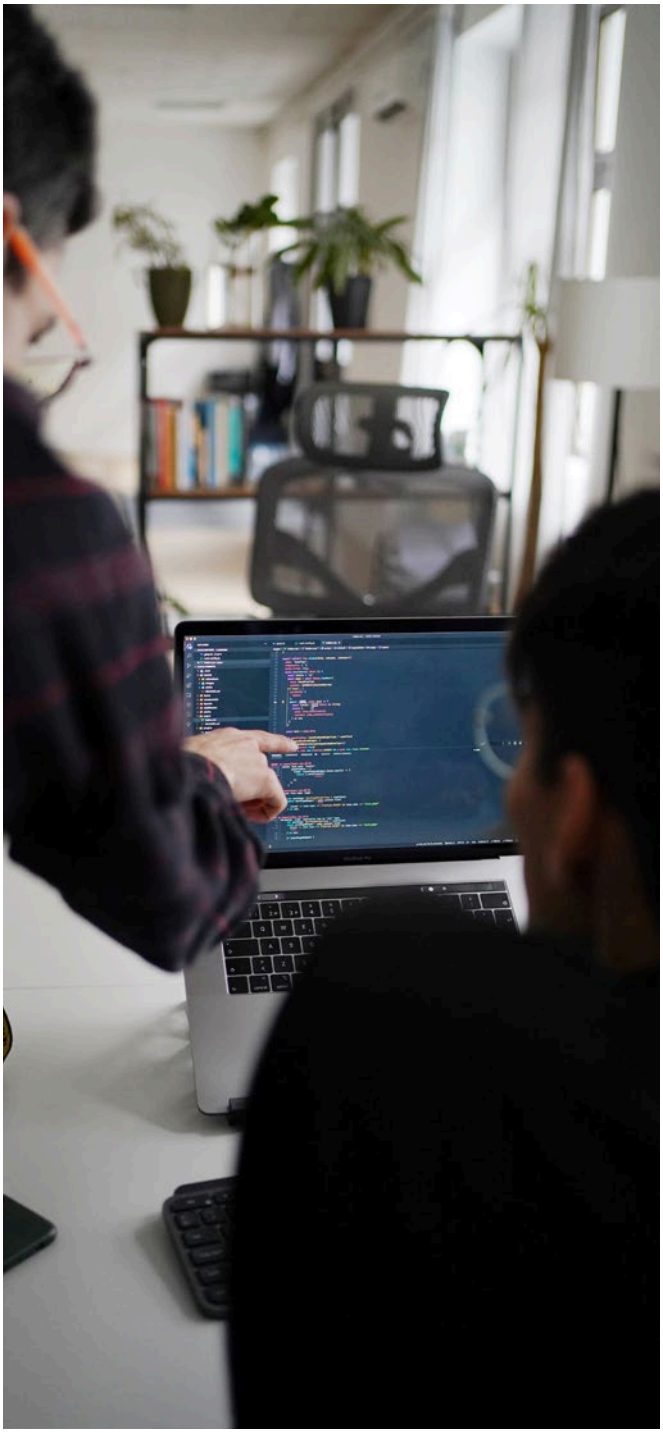
En esta fase se desarrolla el procedimiento de clasificación y obtención de los resultados del análisis de la evidencia digital, para posteriormente, presentarlo a terceros de forma que toda la información esté adecuadamente referenciada, sea legible y pueda ser analizada (EDRM, 2010)[33] sin perder su integridad (AENOR, 2013)[34]. Esta fase en derecho anglosajón suele estar pactada entre las partes, en cuanto al formato del intercambio y consiste especialmente en la recopilación de los documentos que han resultado relevantes para el proyecto.

H Fase de Presentación

En cuanto a la fase de presentación, viene a ser más una cuestión formal, o bien referida a las circunstancias de la presentación, como pueda ser la presentación en un juicio, o bien la emisión del resultado del trabajo al tribunal y a las partes, o la exposición a la empresa que ha encargado el análisis para una investigación interna (EDRM, 2010)[35].

En el informe final debe figurar la reseña y documentación relativa a todo el procedimiento, haciendo hincapié en los criterios y decisiones tomadas respecto a la selección de documentos (National Institute of Justice and National Institute of Standards and Technology, Office of Law Enforcement Standards, 2004)[36].

Por último, hay que señalar que en esta fase final es necesario presentar también el trabajo realizado en cada fase, con expresión concreta de los criterios y procedimientos de búsqueda empleados, así como de los controles aplicados para garantizar la adecuación de los resultados (The Sedona Conference, 2014)[37].



33. EDRM. 2010. Production Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/production/

34. UNE 71506. Tecnologías de la Información. Metodología para el análisis forense de las evidencias electrónicas. 2013.

35. EDRM. 2010. Presentation Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/presentation-guid/

36. National Institute of Justice and National Institute of Standards and Technology, Office of Law Enforcement Standards. 2004. *Forensic Examinatios of Digital Evidence: A Guide por Law Enforcement.* Washington : Office of Justice Programs, National Institute of Justice, 2004.

37. The Sedona Conference. 2014. The Sedona Conference Commentary on Achieving Quality in the eDiscovery Process. The Sedona Conference Journal. Sedona, Phonix, Arizona, EEUU, 2014. Vol. 15.

2. Análisis de evidencia digital para la «obtención de conclusión»

El procedimiento de análisis de «evidencia digital» para la obtención de una conclusión o hipótesis es sustancialmente coincidente con el procedimiento eDiscovery. A la fase de presentación se llega tras la correspondiente compilación y análisis de información relevante extraída del conjunto de la «evidencia digital». Sin embargo, en este caso se parte de la ausencia de una hipótesis sólida y suele darse en supuestos donde la información existente deviene, total o mayoritariamente, de la «evidencia digital».

En este escenario, se sigue el procedimiento eDiscovery completo en todas y cada una de sus fases hasta el punto del análisis. En este punto, donde se llega a los documentos relevantes para el caso concreto, se extrae la conclusión a resultas de aplicar la fase de elaboración (en lugar de pasar a las de producción y presentación). Esta dinámica va a resultar mucho más fácil de entender cuando, en las páginas siguientes, se proceda al desglose de las fases y subfases que configuran este procedimiento.

La fase capital de este procedimiento es la fase de elaboración y, dentro de esta, la subfase de interpretación. Como el lector va a poder extraer, el resultado del procedimiento es un informe de inteligencia que cuenta con el conjunto de la «evidencia digital» como soporte que ha servido para su elaboración. Por supuesto, los agentes que intervienen en el procedimiento que ahora nos ocupa son los analistas y los técnicos informáticos, es decir, los mismos que protagonizan el procedimiento eDiscovery. No obstante, cabe incidir en que, por la naturaleza de este proceso, se exige un mayor nivel de conocimiento e implicación a los analistas, que son los responsables de elaborar un «informe de conclusiones» debidamente fundado.

Seguidamente, se van a exponer las fases que conforman el procedimiento de obtención de una conclusión. Al objeto de favorecer la explicación se acompaña el siguiente gráfico que contiene dichas etapas.

A Fases comunes con el procedimiento de eDiscovery

El procedimiento de eDiscovery resulta aplicable a este otro procedimiento de obtención de hipótesis, pues es preciso llegar a la documentación relevante para poder realizar el análisis y obtener la conclusión. Quedan, por tanto, incluidas las fases de Revisión y de Análisis previos a la obtención de dicha documentación dentro de las que coinciden con el procedimiento de eDiscovery.

B Fase de Elaboración

La Fase de Elaboración comienza en el momento en que se llega a un volumen suficientemente reducido de elementos que tienen una relevancia media muy elevada. Esta fase es en la que se realiza el estudio concreto y detallado de cada uno de los elementos finalmente seleccionados. La metodología utilizada con mayor o menor ortodoxia es el denominado ciclo de inteligencia. Es a partir de esta documentación cuando nace un nuevo análisis, al que denominaremos fase de Elaboración, por ser una de las partes del Ciclo de Inteligencia (JORDÁN, 2016)[38].

Pues bien, de las cuatro fases que tiene el ciclo de inteligencia (Dirección, Obtención, Elaboración y Difusión) ya señaladas, la fase de Elaboración es aquella que especialmente se utiliza en este momento.

Ciclo de inteligencia (Centro Nacional de Inteligencia, CNI)

El Ciclo de Inteligencia tiene en su Fase de Elaboración, cuatro subfases (Centro Nacional de Inteligencia, 2021)[39] a su vez, que aparecen en verde en el gráfico, las subfases de Valoración, Análisis, Integración e Interpretación.

- La subfase de ***Valoración*** conlleva la ya señalada anteriormente de determinar la pertinencia, la fiabilidad o credibilidad y la exactitud[40] de la información que aporta el elemento concreto analizado (JIMÉNEZ VILLALONGA, 2020)[41]:
  - La «pertinencia» tiene como finalidad la valoración de si la información tiene relación con el caso.
  - La «fiabilidad» tiene como finalidad comprobar la veracidad de la información de acuerdo con su origen.
  - La «exactitud» cuya finalidad es la de comprobar la veracidad de la información de acuerdo con su contenido, normalmente a través de la comparación con otras informaciones provenientes de otras o de la misma fuente.
- La subfase de ***Análisis***[42] conlleva la identificación de los diferentes aspectos concretos del documento analizado, de forma pormenorizada, identificándolos de acuerdo con su naturaleza.
- La subfase de ***Integración*** lo que hace es poner en relación todos los aspectos identificados tanto en el concreto elemento analizado, estudiando sus vinculaciones y relaciones internas, como con la información proveniente de otras fuentes.
- Por último, la subfase de ***Interpretación***, pone este elemento en relación con el resto de los elementos ya analizados, obteniendo así inteligencia que permitirá el análisis de otros elementos con el conocimiento adquirido del análisis de los anteriores, en esta subfase se van estableciendo hipótesis de trabajo que van transformándose a medida que se van a analizando nuevos datos.

El resultado final proviene de la interpretación del último de los elementos relevantes analizados, y viene a ser la conclusión.

C Fase de Producción

Esta fase coincide con la fase de Producción del procedimiento de eDiscovery, con relación a los documentos relevantes, y especialmente respecto a aquellos en los que se fundamenten las conclusiones obtenidas.

D Fase de Presentación

En este caso también el fruto de esta fase final será un *informe* (informe de análisis documental o, en su caso, informe de inteligencia), en el que se presentan las conclusiones obtenidas y su soporte documental.

38. JORDÁN, J. 2016. "Una revisión del Ciclo de Inteligencia". Global Strategy. https://global-strategy.org/una-revision-del-ciclo-de-inteligencia-2/

39. https://www.cni.es/la-inteligencia/elaboracion

40. En los procesos de inteligencia en esta subfase también se valoran la oportunidad, que tiene por objeto comprobar si la información valorada puede ser útil en el espacio temporal para su uso futuro si bien en el análisis de la «evidencia digital» consideramos que no es aplicable, puesto que nos referimos exclusivamente a hechos pasados. En JIMÉNEZ VILLALONGA, R. 2020. "El ciclo de Inteligencia: una explicación didáctica". Global Strategy. https://global-strategy.org/el-ciclo-de-inteligencia-una-explicacion-didactica/

41. *Ibid.*

42. No confundir con la *fase de análisis* del modelo EDRM para el E-Discovery. La subfase de análisis pertenece a la fase de elaboración del ciclo de inteligencia.

3. Análisis de evidencia digital de «confirmación de hipótesis».

Por último, cuando previamente se dispone de información no digital con un contenido y características que permitan extraer una hipótesis sobre un caso, resulta habitual que los analistas expertos la deduzcan u obtengan antes de proceder al análisis de la «evidencia digital». Asimismo, pueden darse supuestos donde existan cuestiones concretas o parciales que merezcan comprobación o contraste a través del examen de la «evidencia digital». Pues bien, en ambos supuestos podría tener cabida un protocolo o **procedimiento de análisis de la «evidencia digital» de confirmación de hipótesis**.

Bajo esta propuesta de procedimiento, **el resultado final del análisis es la confirmación (o, en su caso, la refutación) de la hipótesis inicialmente erigida sobre el conocimiento obtenido por otras fuentes**. Este resultado dependerá de si se han localizado en la «evidencia digital» elementos que permitan corroborar la hipótesis. Por lo tanto, a diferencia de lo que sucede con el procedimiento eDiscovery, el resultado no estaría constituido por el elenco de documentos ligados o vinculados al caso concreto, sino por la propia ratificación o negación de la hipótesis inicialmente apuntada.

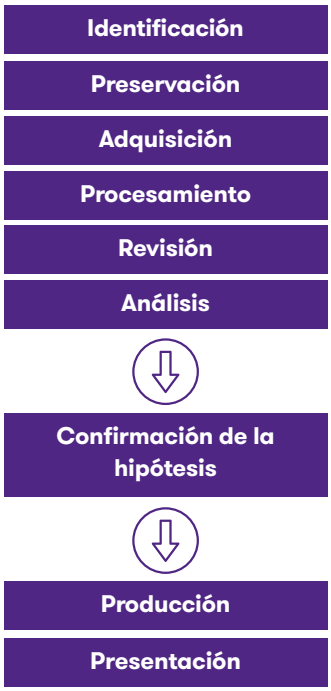
Las fases de este proceso de confirmación de hipótesis serían similares al eDiscovery hasta la fase denominada análisis. En ese punto, extraídos un conjunto de elementos con alta relevancia media del total de la «evidencia digital», se procedería al estudio de estos. Dicho estudio tendría como propósito dilucidar si cada elemento extraído permite ratificar, rechazar o perfilar la hipótesis. Así, nos encontraríamos con la siguiente clasificación de elementos:

- **Elementos «confirmatorios»**: aquellos que tiene un contenido que guarda coherencia con la hipótesis previa.
- **Elementos «matizadores»**: aquellos cuyo contenido no rechazan la hipótesis, sino que vienen a precisarla o variarla en algunos de sus extremos.
- **Elementos «contradictorios»**: aquellos que resultan incompatibles con la conjetura o hipótesis realizada, dicha incoherencia viene a determinar que, de ser cierta la hipótesis, no puedan darse este tipo de elementos.
- **Elementos «neutros»**: aquellos que se encuentran desvinculados de la hipótesis.

Del conjunto de elementos extraídos, el analista procede al examen de aspectos clave como el número, fiabilidad y exactitud de tales elementos. La calidad del análisis y, en consecuencia, de la conclusión, penderá de este examen. Por ello, es importante que el analista elabore la conclusión final incorporando una explicación sobre la credibilidad y exactitud de los elementos estudiados. En este marco son susceptibles de ser sometidas a contradicción, además de aquellas señaladas para el eDiscovery, las asociadas a la determinación de si un elemento es contradictorio, neutro, matizador o confirmatorio[43].

Por último, vamos a concretar las fases de este procedimiento de confirmación de hipótesis (se adjunta gráfico con las etapas que lo constituyen):

43. Asimismo, podrán darse supuestos en los que, por ejemplo, se ha extraído un elemento contradictorio. En tales casos, factores como la exactitud y fiabilidad resultaran especialmente determinantes para la defensa del criterio del analista.



A Fases coincidentes con aquellas contenidas dentro del procedimiento «eDiscovery»

Una parte relevante de las fases expuestas para el eDiscovery son coincidentes con la que estamos señalando en este apartado. Así, las fases de Identificación, Preservación, Adquisición y Procesamiento iniciales coinciden en su totalidad. Ello guarda una lógica: las referidas etapas son eminentemente técnicas y la finalidad es disponer de los archivos de forma que pueda iniciarse adecuadamente el análisis de los elementos que sean relevantes para el caso.

Nos encontramos, por tanto, en este punto con una «evidencia digital» obtenida adecuadamente, que incluye los dispositivos que pueden contener información relacionada con el caso, donde los elementos de la evidencia ya se han tratado y se han eliminado los duplicados, por lo que estamos en el momento de pasar a la siguiente fase, donde comienzan a gestarse los **criterios de búsqueda y de descarte** (EDRM, 2020)[44].

La descripción de las siguientes fases se refiere por tanto a la revisión, análisis, producción y presentación del procedimiento en que se dispone de hipótesis de trabajo, puesto que en los otros casos se seguiría el procedimiento ya descrito en el eDiscovery.

B Fase de Revisión

Esta fase es la de estudio y análisis general de evidencia digital, de manera que su conocimiento tras las fases anteriores nos permita pasar a la fase de análisis con una estrategia de búsqueda coherente con la hipótesis que queremos comprobar. Parece claro que la estrategia de selección de elementos de la «evidencia digital» para la confirmación de una hipótesis de trabajo no será la misma que la estrategia que busque encontrar todos los elementos relevantes para el caso existentes en la «evidencia digital» (EDRM, 2010)[45].

También en este caso, la fase de revisión viene a ser la preparación y planificación de la fase de análisis, y de nuevo, tras el procesamiento de la información, se hacen pruebas sobre el conjunto de la evidencia para ver entre otras cuestiones:

- Volúmenes de documentos que aparecen como resultado de búsquedas con diferentes criterios relacionados con la hipótesis establecida, así como los resultados en sí.
- Volumen de elementos de los custodios en relación con la información y con las asunciones de la propia hipótesis.
- Flujos de información en cuanto a las comunicaciones, mayores emisores y receptores, de acuerdo con las asunciones de la hipótesis.

Toda esta operativa permite al analista un mayor conocimiento de la evidencia, en relación con la hipótesis, de forma que le permita establecer la estrategia de búsqueda a través de la siguiente fase.

C Fase de Análisis

No varía sustancialmente, en cuanto a su naturaleza, esta fase respecto a la de eDiscovery (EDRM, 2010)[46], si bien, como sucede en la fase de revisión, debe estar enfocada a la comprobación de la hipótesis de trabajo. Por tanto, los criterios y términos de búsqueda deben buscarse en la propia hipótesis, en sus términos, personas, asunciones, plazos y relaciones.

Una vez llegados al final de esta fase de Análisis, cuando hemos obtenido un conjunto de elementos con un reducido volumen, pero de alta relevancia media, se pasa a su estudio. En este caso el estudio tiene la finalidad de determinar si el elemento confirma, matiza o contradice la hipótesis sujeta a comprobación, y así debe clasificarse cada elemento.

Serán clasificados como **"Confirmatorios" aquellos elementos cuyo contenido sea coherente con la hipótesis de trabajo**. Por su parte, serán clasificados como

44. https://edrm.net/
45. EDRM. 2010. Review Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/review-guide/
46. EDRM. 2010. Analysis Guide. https://edrm.net/resources/frameworks-and-standards/edrm-model/analysis/

“Matizadores” aquellos otros que introduzcan matices a la hipótesis, por ejemplo, ampliando detalles, pero que no la contradigan. Se calificarán como **“Contradictorios” aquellos otros que sean incoherentes con la hipótesis de trabajo, de manera que no puedan coexistir ambos bajo la hipótesis de que ambos fueran verdad**. Por último, nos estarían los elementos que denominaríamos **“Neutros”, que no tienen relación con la hipótesis.**

Hay que analizar posteriormente en detalle tanto el número de los confirmatorios como de los de matización frente a los contradictorios. Especialmente hay que valorar la fiabilidad y exactitud de los confirmatorios y de los contradictorios, puesto que, por ejemplo, no es lo mismo que confirme o contradiga una hipótesis de trabajo financiera el director financiero de la compañía que un responsable comercial local. En todo caso, el peso de los elementos contradictorios, incluso de uno solo si es clasificado como exacto y creíble, obliga a cuestionar la validez de la hipótesis de trabajo.

No es intrascendente el número o, mejor dicho, la proporción de documentos que aparecen clasificados como Neutros, ya que dicha proporción será un importante indicador de la bondad y exactitud de la selección realizada y, por lo tanto, del análisis y por ende de la conclusión final.

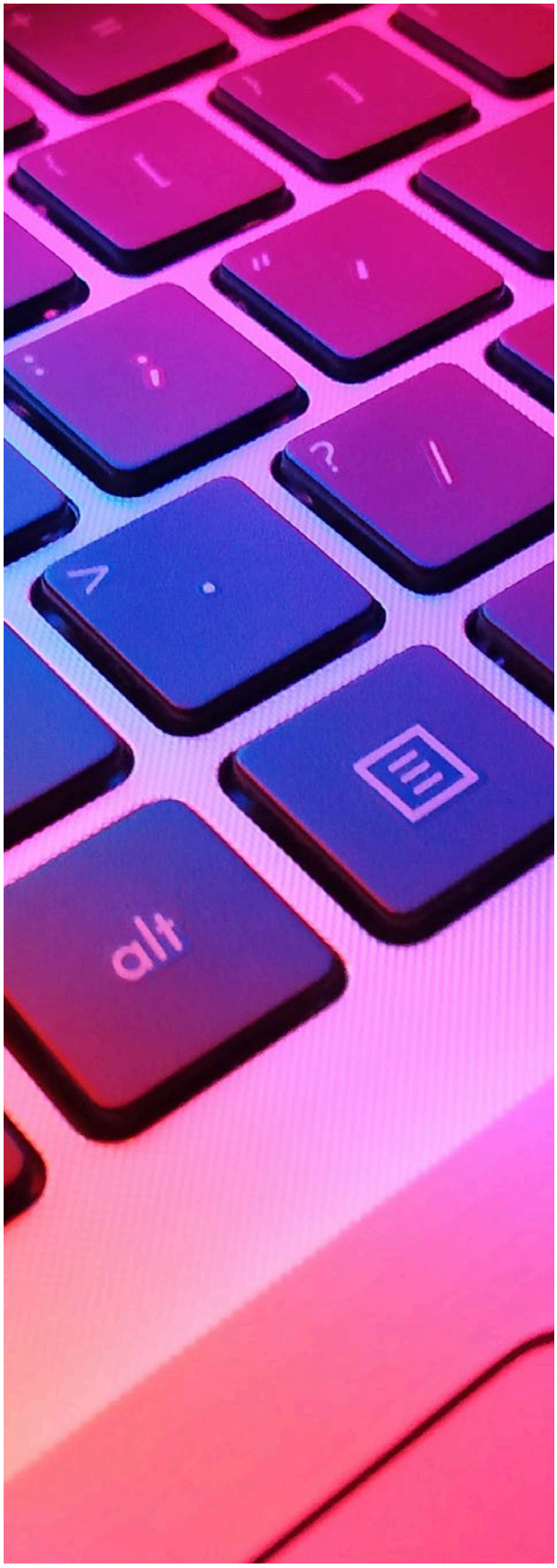
D Fase de Producción

En el análisis que estamos estudiando en este punto, el de la confirmación de una hipótesis, esta fase no tiene la importancia que en el procedimiento de eDiscovery, debido a que aquí lo importante no es la producción de unos documentos que van a representar la «evidencia digital» en cuando al objeto del proceso, sino que lo que se busca en este procedimiento es la confirmación o no de la hipótesis, siendo esa la conclusión.

Sin embargo, **la producción de todos los documentos considerados finalmente como relevantes también será particularmente importante en esta metodología**, especialmente si se acompañan con la expresión de su clasificación respecto a la hipótesis de trabajo: Confirmatorio, Matizador, Contradictorio o Neutro. Esto permitirá que las otras partes o el tribunal puedan comprender el procedimiento seguido y especialmente el soporte existente para la confirmación o negación de la hipótesis.

E Fase de Presentación

La fase de presentación en este caso será un ***informe*** en el que se valoren los elementos ***Confirmatorios, Matizadores, Contradictorios y Neutros***. Tanto en su número, como en su proporción, como en su **exactitud y fiabilidad**, obteniendo una conclusión razonada al respecto.



Anexo: terminología relevante

En esta temática existe un amplísimo elenco de términos (no siempre unívocos), algunos de los cuales proceden de traducciones de otros idiomas. Incorporamos aquellos términos ligados a la materia abordada:

- **Cadena de custodia:** Procedimiento de trazabilidad controlado que se aplica a las evidencias, desde su adquisición hasta su análisis y presentación final, el cual tiene como fin no alterar la integridad y autenticidad de las mismas, asegurando en todo este proceso que los datos originales no son alterados (AENOR, 2013)[47].
- **Clonado:** Proceso de copia, a bajo nivel y firmado digitalmente, de la información original por el cual se traslada ésta a un nuevo soporte de almacenamiento digital, preservando la inalterabilidad de la información en el sistema o soporte de origen y asegurando la identidad total entre aquella y la extraída (AENOR, 2013)[48].
- **Comunicación electrónica:** Entendemos por comunicación electrónica aquella transmisión de un mensaje de forma unidireccional o multidireccional, a través de medios electrónicos. Incluimos en este concepto todo tipo de mensajes en los que el emisor envía una comunicación a un receptor que a su vez puede contestar con otro mensaje similar. Por tanto, consideremos como tales el correo electrónico, las aplicaciones de mensajería instantánea (Whatsapp, Telegram, SMS, etc.), que, con distintos formatos, comparten la misma naturaleza.
- **Custodio:** en el campo de la investigación forense informática es la persona física que tiene asignado un determinado dispositivo electrónico en una organización, o bien el propietario de dicho dispositivo.
- **Datos informáticos:** se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función, de acuerdo con el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 (Instrumento de Ratificación por España en BOE de 17 de septiembre de 2010[49]).
- **Dispositivo o medio electrónicos:** mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras (Anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia).
- **Documento electrónico:** Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado (Anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia).
- **Evidencia:** cualquier dato o información que puede ser utilizado para determinar la existencia o no de un hecho (AENOR, 2013). Cada uno de los datos digitales recogidos en la escena de interés susceptibles de ser analizados con una metodología forense (HIDALGO CAJO, 2019)[50].
- **Evidencia electrónica o «evidencia digital»**, también denominada **prueba electrónica o prueba digital**, que es aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal (SANCHÍS CRESPO, 2012)[51].

47. UNE 71506. Tecnologías de la Información. Metodología para el análisis forense de las evidencias electrónicas. 2013.
48. *Ibid.*
49. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221
50. HIDALGO CAJO, I.M., YASACA PUCUNA, S., HIDALGO CAJO, G.G. 2019. "Evidencias Digitales en la Investigación Forense Informática". Riobamba : Editorial Politécnica ESPOCH, 2019.
51. SANCHÍS CRESPO, C. 2012. "La prueba en soporte electrónico". Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio. Navarra : Thomson Reuters Aranzadi, 2012.

También puede definirse como:
«aquella información con valor probatorio que se encuentra incluida en un medio electrónico o es transmitida por dicho medio y la forma en la que se manifiesta, expresa o contiene la prueba digital lo es: 1. bien dentro de un medio tecnológico o aparato informático,2. bien en un proceso de comunicación en el que pueda estar presente, o no, la parte que puede quedar afectada por un hecho que consta en el proceso de comunicación (…)» (MAGRO SERVET, 2020)[52].

En el modelo EDRM se denomina ESI que se corresponde con *Electronically Stored Information* (EDRM, 2020)[53], y que a los efectos de este texto tienen el mismo significado.

- **Función "hash":** Función unidireccional que aplicada a un documento electrónico cualquiera proporciona un resumen (huella digital o "hash") del mismo. El tamaño del resumen es fijo, según la función utilizada, y no depende del tamaño del documento electrónico (AENOR, 2013)[54].
- **Huella digital:** Secuencia de valores resultado de aplicación de una función hash a un fichero electrónico (AENOR, 2013)[55].
- **Imagen forense:** Es el producto de realizar un clonado de cualquier evidencia electrónica en un formato de fichero, sin tener en cuenta el soporte que la contiene (AENOR, 2013)[56].
- **Información original:** Conjunto organizado de datos que mantiene su integridad desde el inicio hasta el final del fichero o soporte informático que los contiene (AENOR, 2013)[57].
- **Metadato:** Información que describe el contenido de un dato (AENOR, 2013)[58] concreto asociado a un fichero _(i.e. fechas MAC – modificación, acceso, creación-, autor…). Existen metadatos generados por el sistema operativo y otros metadatos generados por la aplicación que crea o trata los ficheros.
- **Muestra:** Parte representativa o significativa de una evidencia (AENOR, 2013)[59].
- **Trazabilidad:** Propiedad de la información de ser rastreada o reconstruida hasta su origen (AENOR, 2013)[60].

Fernando Lacasa Cristina
Rafael Aguilera Gordillo
Codirectores del Compliance Advisory LAB
Septiembre 2022

52. MAGRO SERVET, VICENTE. 2020. "Casuística práctica de la prueba digital en el proceo civil y penal". *Actualidad Civil*. Wolters Kluwer, 2020.
53. EDRM. 2020. EDRM. 2020. https://edrm.net/.
54. UNE 71505-1. Tecnologías de la Información. Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. 2013.
55. *Ibid.*
56. UNE 71506. Tecnologías de la Información. Metodología para el análisis forense de las evidencias electrónicas. 2013.
57. *Ibid.*
58. UNE 71505-1. Tecnologías de la Información. Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. 2013.
59. UNE 71506. Tecnologías de la Información. Metodología para el análisis forense de las evidencias electrónicas. 2013.
60. *Ibid.*

Resumen

La «evidencia digital»: tipos de procedimientos de análisis y configuración

¿Cuál es el papel que juega la «evidencia digital» en el actual contexto empresarial?

¿Cómo se desarrolla el análisis de la «evidencia digital»?

¿En qué consiste el conocido como procedimiento eDiscovery?

¿De qué fases se componen los protocolos de extracción y análisis realizados por los departamentos especializados en Forensic?

La «evidencia digital» se ha convertido en un elemento primordial, tanto en el marco de las investigaciones internas corporativas como en los procesos judiciales.

A pesar de ello, muchos de sus aspectos clave siguen siendo muy poco conocidos para los profesionales ligados al ámbito del *Compliance* o al asesoramiento legal corporativo. Así, suele desconocerse la metodología de análisis aplicada a la «evidencia digital», cada fase que la conforma, numerosos de los conceptos utilizados o los sujetos expertos en Forensic que intervienen en esta tipología de procedimientos (analistas y técnicos informáticos).

Este octavo report del Compliance Advisory LAB se abordan los aspectos fundamentales del análisis de la «evidencia digital». El objetivo es ofrecer información relevante a aquellos profesionales que detentan responsabilidades ligadas a la ejecución de «sistemas de *compliance*» o «sistemas internos de información».

Se analizan y explican las fases que conforman **tres procedimientos de análisis de la «evidencia digital»**:

- **Procedimiento de análisis de «evidencia digital» eDiscovery.**
- **Procedimiento de análisis para la obtención de conclusiones.**
- **Procedimiento de confirmación de hipótesis.**

Además, se incorpora un anexo con terminología relevante asociada a la «evidencia digital» y referencias de interés.

Por tanto, se trata de un texto que resultará especialmente interesante para ***compliance officers*, asesores legales corporativos, analistas de riesgos, órganos colegiados con funciones vinculadas al *compliance*** o responsables del «sistema de información interna». Por supuesto, el contenido de este report concierne tanto a **directivos** como a miembros del **consejo de administración**.

Reports publicados

Consulta los reports publicados hasta la fecha por el **Compiance Advisory Lab** de Grant Thornton

REPORT 1

El «traslado» de responsabilidad penal entre empresas: Soporte socio-legal del artículo 130.2 C.P., identidad y due diligence penal.

REPORT 2

Refuerzo de la eficacia del *Compliance*: «Behavioral *Compliance*» y «Nudges».

REPORT 3

Incertidumbres en el *Compliance* Penal: fragilidades con implicaciones reales para la empresa. «Beneficio corporativo indirecto», «incumplimiento grave de los deberes de supervisión», «nulidad de prueba en investigaciones internas y confidencialidad».

REPORT 4

Consideraciones de profesionales expertos en *Compliance*: percepciones de especialistas del ámbito judicial, académico y empresarial sobre aspectos clave del *Compliance*.

REPORT 5

Tres Autos -cruciales- sobre *compliance* de la Audiencia Nacional: un análisis de los puntos clave de tres resoluciones judiciales dictadas en distintas investigaciones penales de relevancia que ilustran la especial trascendencia de los «sistemas de *compliance*».

REPORT 6

Probabilidad del riesgo, dolo eventual e imprudencia consciente: examen de una difusa frontera entre la condena y la absolución de la persona jurídica.

REPORT 7

«Sistema interno de información»: la próxima -gran- obligación para toda persona jurídica o física con más de 49 trabajadores. Análisis de las ventajas, aspectos jurídico-penales, efectos sobre el sistema de *compliance* y otros puntos relevantes del Anteproyecto de Ley de Protección al Informante.

REPORT 8

La «evidencia digital»: tipos de procedimientos de análisis y configuración.

Directores Compliance Advisory LAB

Fernando Lacasa

Socio de Forensic, Codirector del Compliance Advisory Lab

T +34 91 441 52 83

E Fernando.Lacasa@es.gt.com

Ver CV

Rafael Aguilera Gordillo

Codirector del Compliance Advisory LAB

T +34 91 576 39 99

E Rafael.Aguilera.ex@es.gt.com

Ver CV

https://www.grantthornton.es/servicios/financial-advisory/forensic/Compliance-advisory-lab/

www.grantthornton.es

Grant Thornton

grantthornton.es