TyD CONSULTORES

# EVIDENCIAS ELECTRÓNICAS

En enero de 2002, el gerente de una mediana empresa Valenciana, dedicada a la importación y exportación de equipos industriales, tuvo que despedir al director comercial por prácticas desleales con la empresa. La sospecha del gerente condujo a investigar el ordenador del posteriormente despedido, lo que reveló que éste había creado su propia compañía, con la misma actividad que la empresa en la que trabajaba y, por lo tanto, competencia. Los documentos de texto, hojas de cálculo, correos electrónicos y otros encontrados en el ordenador demostraron que el director comercial había estado realizando actividades ilícitas empleando medios de la empresa, sustrayéndole clientes y negocio. Las evidencias aportadas por el perito informático supusieron el despido procedente para el empleado y la presentación de una demanda civil por la empresa.

**Las evidencias electrónicas** son rastros existentes en los equipos informáticos que, debidamente preservados, y puestos en relación con información existente en otros ordenadores o en el contexto de otras evidencias o de hechos probados, permiten demostrar que se ha llevado a cabo una acción por medios informáticos e, incluso, quién o quienes la han llevado a cabo.

El término "Evidencia Electrónica" es, en cierto modo, de cuño reciente y recoge aspectos para los que, según el contexto, se emplean otras denominaciones, como prueba o indicio informático, electrónico o digital. El término evidencia se prefiere cuando pensamos que las conclusiones son incontrovertibles y se espera que la apreciación del juez discurra en el mismo sentido que la de los expertos forenses, en este caso, peritos informáticos, y las acepte como pruebas.

Tradicionalmente la evidencia auditora se ha clasificado en: evidencia física, documental, analítica y evidencia testimonial. A estas cuatro categorías debe añadirse hoy la evidencia informática. Sin embargo, algunos autores consideran que la evidencia electrónica o informática es una evidencia física, aunque intangible (en definitiva son registros magnéticos u ópticos que pueden ser recogidos y analizados). Un ejemplo de evidencia informática es el envío de correos electrónicos con pornografía infantil: si tuviéramos acceso con orden judicial al ordenador del sospechoso, podríamos encontrar dichos correos en la carpeta de elementos enviados, las fotos en el ordenador y otros; esto sería el "rastro" en la escena del crimen y es una evidencia inequívoca de que el sospechoso los tenía y envió correos; además se puede añadir la evidencia del registro del proveedor o servidor de correo.

**Ámbitos de actuación:** Existen dos campos dentro de los cuales las evidencias electrónicas o informáticas adquieren su significado:

- En el ámbito procesal, como elemento probatorio: Es un medio utilizado para lograr la convicción del órgano jurisdiccional respecto a la existencia, o no, de un determinado hecho, verdad o falsedad de un dato concreto. Los abogados están iniciando un gran interés por la forma en la que pueden presentar en las diferentes instancias judiciales los resultados de investigaciones en torno a sistemas informáticos y en los que es preciso demostrar que se ha llevado a cabo alguna actividad ilícita con los mismos.

- En el ámbito de la empresa: Se trata de la actuación de expertos en la elaboración de planes de previsión de riesgos, dentro del plan empresarial de seguridad, que en el futuro garanticen la validez de la pruebas aportadas en eventuales procesos

judiciales. Es extremadamente conveniente en contrataciones electrónicas. Es realmente un servicio de consultoría para la prevención de incidentes, para el establecimiento de metodologías de gestión que permiten preservar las pruebas futuras en caso de tratamiento de ilícitos de algún tipo, y para la gestión y preservación de las evidencias informáticas, en el tratamiento de diversas situaciones.

**Incidentes:** Cualquiera que sea el orden jurisdiccional ante el cual nos encontremos, descubriremos un amplio catalogo de incidentes de carácter informático y telemático.

Todos los incidentes deberán de adaptarse a un procedimiento probatorio a la hora de la fase procesal, independientemente de la rama jurisdiccional de la que provenga el supuesto hecho concreto. Como todo peritaje, el informático, independientemente de que estemos ante el orden jurisdiccional civil, penal, social o contencioso-administrativo, se aportará en los momentos que señalan las leyes de enjuiciamiento.

A modo de ejemplo, alguno de estos incidentes son:

- **Derecho Penal**
  - Descubrimiento y revelación de secretos, espionaje industrial,
  - Delitos económicos, societarios o contra el mercado o los consumidores,
  - Delitos contra la propiedad intelectual e industrial,
  - Vulneración de la intimidad, lectura de correo, interceptación de comunicaciones, protección de datos personales,
  - Estafa, fraudes, conspiración para alterar el precio de las cosas,
  - Sabotaje, destrucción de cosa de valor, etc.

- **Derecho Laboral**
  - Faltar a la lealtad debida (creación de empresa paralela),
  - Uso indebido de equipos (daños/uso abusivo),
  - Vulneración buena fe contractual (información confidencial),
  - Trasgresión del deber de buena conducta,
  - Amenazas, calumnias o injurias (también Penal).

- **Derecho Mercantil – Civil**
  - Publicidad engañosa o sin consentimiento, por medios electrónicos,
  - Competencia desleal, abuso de confianza,
  - Cumplimiento de obligaciones y contratos y consentimiento contractual (por medios telemáticos),
  - Venta de cosa ajena vía Internet,
  - Valoraciones de bienes informáticos.

**Procedimiento de Custodia de la prueba:** Una cuestión fundamental es la adecuada preservación de la cadena de custodia de las evidencias informáticas o electrónicas. Debe preservarse su contenido usando medios que no invaliden la prueba, de forma que esté disponible posteriormente para revisiones o estudio de los peritos de las partes, sin que pueda cuestionarse su obtención o su custodia, es decir, asegurando que no han sido alteradas o modificadas. El perito debe determinar el sistema que utilizará para la custodia de los elementos.

El objetivo de un peritaje de este tipo es presentar el contenido de archivos que puedan tener relevancia jurídica, informando de su significado y características. Esos archivos deben haberse mantenido en una "cadena de custodia", por lo que el perito debe detallar

en su informe los pasos dados desde que se intervienen o reciben los equipos informáticos, hasta que se presentan los archivos relevantes. El peritaje ha de poder ser repetido, por lo que no se pueden alterar los elementos informáticos originales, trabajándose siempre sobre copias clónicas. En el caso de que el perito emplee herramientas de auditoría o de búsqueda de archivos en el ordenador del sospechoso, deberá asegurarse de que no se altera el contenido del disco.

**Actividades periciales:** Los pasos a realizar en este tipo de peritajes informáticos, una vez designado el perito, son básicamente cinco:

1. Intervención. Se aprehenden los elementos informáticos (en ocasiones con orden judicial).
2. Revisión preliminar. Se descartan los elementos informáticos irrelevantes y se preparan los demás (sólo interesan los soportes donde se puedan guardar datos, no las pantallas, teclados, impresoras y otros).
3. Exploración de archivos y registros. Se localizan, imprimen y describen los archivos o evidencias informáticas relevantes. En función del caso concreto, cada uno de los pasos que haya dado el Perito Ingeniero en Informática constará de manera detallada en su informe de actuación.
4. Informe pericial. Se confecciona el informe procurando que se explique por sí mismo, así el perito simplemente se remitirá a lo ya expuesto en su dictamen. Cuanto más claro e irrefutable sea el informe, menos presencia posterior del perito.
5. Ratificación del dictamen ante sede judicial: Explicación del dictamen, responder a preguntas y objeciones de las partes y a solicitudes de ampliación y recibir la crítica del dictamen por el perito de la otra parte.

**Tipos de periciales informáticas**: la tipología de los peritajes informáticos es muy variada, tanto como las aplicaciones de la informática en la sociedad y el uso de los ordenadores. Antes hemos expuesto sólo uno de los tipos posibles. La metodología de trabajo del perito será muy distinta a la expuesta en caso de, por ejemplo, propiedad intelectual de programas de ordenador, en los que se precise encontrar semejanzas entre dos programas; o de cumplimiento de contratos de desarrollo e implantación de programas a medida, o de adaptación de paquetes de software, en los que se deba conocer si el sistema funciona correctamente o los posibles defectos o incumplimientos de contratos; el método de trabajo será también distinto en valoración de máquinas o programas, así como en otros tipos de dictámenes.

Los Ingenieros en Informática de **TyD Consultores** acumulamos una larga experiencia en la emisión de dictámenes informáticos, tanto judiciales como extrajudiciales, y preparamos la orientación y método de trabajo más adecuado para cada cuestión concreta. Preséntenos su caso y le prepararemos el enfoque y presupuesto oportuno.

D. Antonio López-Silves
Socio-Director de Tecnología y Dirección, S.L.
Licenciado en Informática
Colegiado nº 16 del COIICV