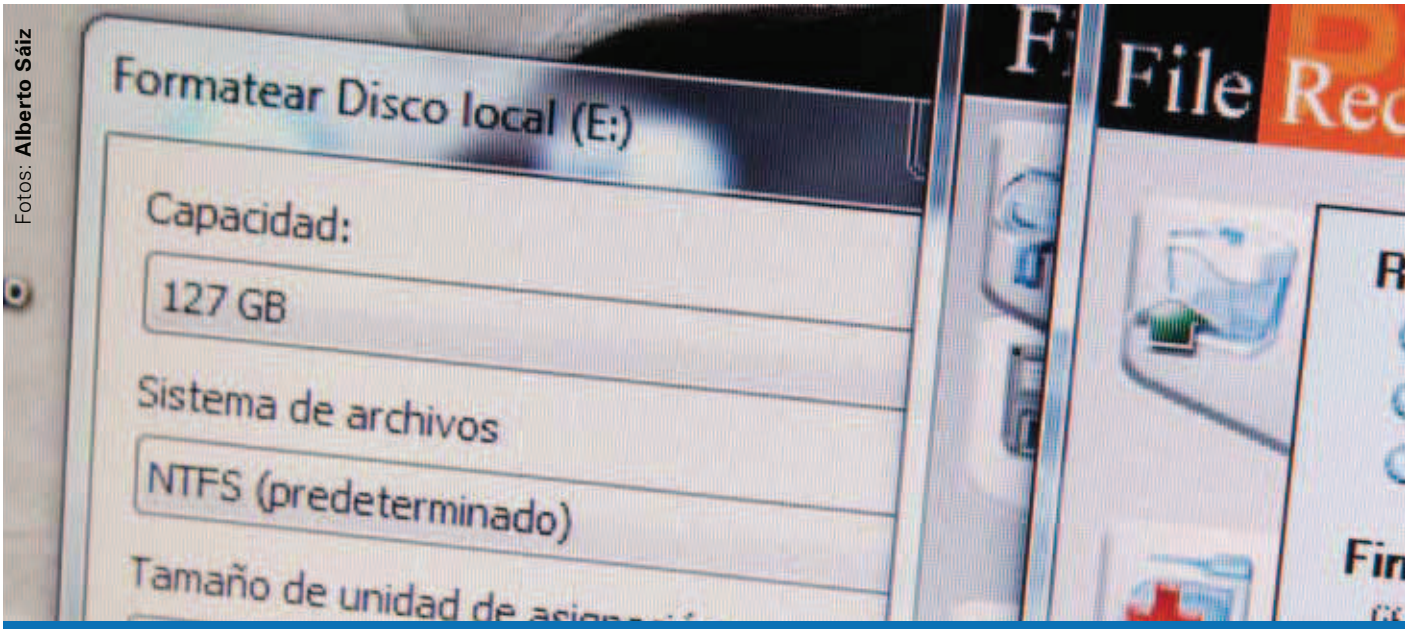


Fotos: **Alberto Sáiz**

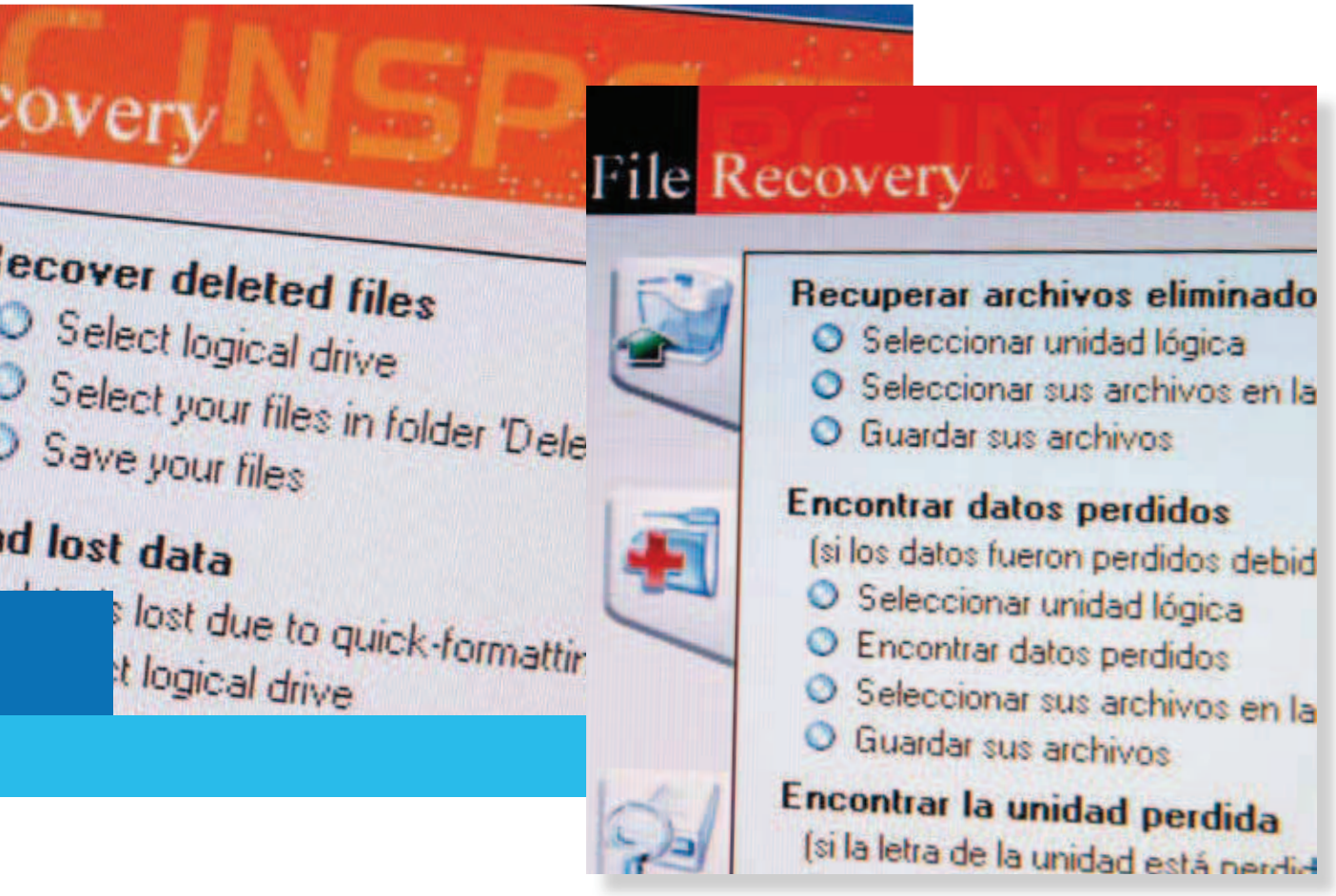
Evidencias electrónicas
en un dictamen pericial

Col. de Ingenieros en Informática de la CV. Comisión de Control del Turno de Actuaciones Profesionales

LAS EVIDENCIAS electrónicas o digitales 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 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.

En enero de 2012, 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 condujo a investigar el ordenador del director comercial, 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 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. El letrado no ha desestimado la conveniencia de una querella penal posterior.

Tradicionalmente, la evidencia auditora se clasifica en: evidencia física, documental, analítica y testimonial. A estas cuatro categorías se añade hoy la evidencia informática. Algunos autores consideran que esta última es una evi-



dencia 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: tras acceder 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 poseía y distribuyó material pedófilo; además se puede añadir la evidencia del registro del proveedor o servidor de correo y otras evidencias que apoyen las conclusiones.

Existe un amplio catálogo de incidentes de carácter informático y telemático. Los abogados han demostrado 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. A modo de ejemplo, alguno de estos incidentes son: descubrimiento y revelación de secretos, espionaje industrial, delitos económicos, societarios o contra el mercado o los consumidores, vulneración de la intimidad, interceptación de comunicaciones… (Penal), creación de empresa paralela, vulneración de la buena fe contractual, uso indebido de equipos… (Laboral), publicidad engañosa o sin consentimiento, competencia desleal, cumplimiento de obligaciones y contratos… (Mercantil-Civil).