Masterclass: ‘Informática Forense y Evidencia Digital para Abogados’

Departamento de Derecho de las Comunicaciones y Tecnologías de la Información.

Universidad Externado de Colombia

27 de noviembre de 2025

Bogotá D.C., Colombia

Compilado por
Jaider Jael Morales Torres
Universidad Externado de Colombia

Calle 12 No. 1-17 Este
Bogotá D.C., Colombia

Teléfono: 282 60 66 Ext.1105, 1106
esdercom@uexternado.edu.co

Introducción

En el contexto actual, la informática forense y la evidencia digital se han convertido en pilares fundamentales para garantizar la correcta administración de justicia. Su adecuada gestión permite preservar la cadena de custodia, asegurar la integridad de la prueba y fortalecer la confiabilidad del proceso judicial, especialmente en casos donde la tecnología juega un rol central en la comisión o investigación de delitos.

Por esto el Departamento de Derecho, Comunicaciones y Tecnologías de la Información de la Universidad Externado de Colombia realizó la Masterclass "Informática Forense y Evidencia Digital para Abogados", un espacio académico diseñado para abordar los desafíos jurídicos que plantea la recolección, análisis y uso de evidencia digital en el contexto legal contemporáneo.

La Masterclass estuvo a cargo del Dr. Juan Alejandro León, destacado abogado con amplia trayectoria en derecho digital, cibercriminología y auditoría forense. Formación que incluye estudios en Derecho Contractual, Derecho Internacional de la Empresa, Legaltech, Auditoría Antifraude y Pedagogía jurídica, con experiencia como investigador, perito y docente en procesos de ciberseguridad y gestión de evidencia digital.

Durante esta Masterclass, se abordaron temas como: Fundamentos de la informática forense aplicada al derecho, técnicas de recolección y preservación de evidencia digital, rol del abogado frente a la evidencia tecnológica, entre otros.

Agenda del Evento

Instalación
Andrés Sebastián Moreno Guevara – Asistente de investigación del Departamento de Derecho Comunicaciones y Tecnologías de la Información de la Universidad Externado de Colombia.
Desarrollo de la Masterclass
Juan Alejandro León - Director ejecutivo de Legal Heed. Secretario general y jurídico de UNISANGIL. Asesor externo de la Cámara de Comercio de Bucaramanga y docente

Instalación

Andrés Sebastián Moreno Guevara, presentó el enfoque general del encuentro y contextualizó los retos que había traído consigo la nueva era digital para el ámbito jurídico. Señaló que, en un escenario donde la tecnología permeaba cada aspecto de la vida cotidiana, los delitos informáticos crecían exponencialmente y la evidencia digital se había convertido en un pilar esencial para garantizar la correcta administración de justicia.

Explicó que, en la actualidad, no resultaba suficiente que los abogados conocieran únicamente el derecho sustancial y procesal; por el contrario, debían comprender cómo se recolectaba, preservaba y analizaba la información digital para asegurar su integridad, autenticidad y validez. Enfatizó que una adecuada gestión de la evidencia permitía mantener la cadena de custodia, prevenir manipulaciones y fortalecer la confiabilidad del sistema judicial.

En este contexto, indicó que la sesión buscaba brindar herramientas conceptuales y prácticas para enfrentar los desafíos que planteaba la era digital en los procesos judiciales y en el ejercicio profesional del derecho. Acto seguido, presentó al expositor invitado, el doctor Juan Alejandro León, destacando su amplia trayectoria en derecho digital, cibercriminología y auditoría forense.

Desarrollo de la Masterclass

Para iniciar su presentación, el Doctor Juan Alejandro León explicó que la sesión buscaba introducir los conceptos y elementos fundamentales que los abogados necesitaban dominar en el contexto actual, donde la mayoría de la información, tanto en el ámbito corporativo como personal, se generaba, almacenaba y transmitía por medios digitales. Indicó que, frente a incidentes como ataques externos, intromisiones o fraudes internos, resultaba evidente que la información crítica residía en dispositivos y entornos digitales, lo que hacía indispensable comprender cómo debía gestionarse adecuadamente la evidencia.

León señaló que el flujo de información en las organizaciones ya fuera por correo electrónico, servicios en la nube o servidores internos, reforzaba la necesidad de que los abogados tuvieran claridad sobre el tratamiento técnico y jurídico de la evidencia digital. Explicó que resultaba fundamental conocer el marco legal que permitía aportar mensajes de texto, logs de eventos, archivos o documentos electrónicos ante un proceso judicial, garantizando su autenticidad, integridad y valor probatorio. Precisó que la perspectiva de la sesión se orientaba a las necesidades del abogado litigante o corporativo, quien debía identificar los

elementos esenciales para asegurar que cualquier procedimiento de recolección y preservación cumpliera con la normativa interna y con los estándares internacionales en materia de evidencia digital.

El conferencista relató que, en los últimos años, había acompañado múltiples casos relacionados con ciber incidentes y fraudes corporativos. Explicó que, en la mayoría de los escenarios, cuando una organización se enfrentaba a una vulneración, existía un momento inicial de incertidumbre respecto de las medidas a adoptar. Señaló que era indispensable que las entidades contaran con conocimientos básicos en informática forense que permitieran iniciar investigaciones internas, asegurar equipos, aislar dispositivos comprometidos y estructurar un plan de acción para recuperar la operación.

Con el fin de ilustrar el abordaje jurídico y técnico de estos eventos, León presentó un caso reciente atendido por su equipo. Describió que se trataba de una empresa comercializadora y distribuidora de repuestos automotrices, que empezó a recibir quejas sobre la baja calidad de ciertos productos. La dirección inició una revisión comparativa del inventario físico y del registro digital en el ERP, identificando discrepancias significativas. Paralelamente, llegaron denuncias a la línea ética señalando a un jefe de inventarios, quien presuntamente mantenía un negocio paralelo con un proveedor y habría manipulado el inventario para sustituir productos originales por artículos de menor calidad, beneficiándose económicamente.

Frente a las alertas de auditoría y las denuncias internas, la gerencia activó un plan de acción que incluyó la contratación de una auditoría externa y la realización de un proceso de recolección de evidencia digital. En esta etapa participaron un abogado especializado en evidencia digital y un perito en informática forense, encargados de investigar el comportamiento del funcionario y asegurar los datos relevantes.

León explicó que la mayor parte del material probatorio se encontraba en correos electrónicos, computadores corporativos, logs de eventos, archivos del ERP y otros registros digitales que podían revelar modificaciones o manipulaciones del inventario. Señaló que el objetivo era recolectar la información de forma técnicamente adecuada, de modo que pudiera ser usada en procesos judiciales o en decisiones internas disciplinarias o laborales.

Destacó que la informática forense combinaba conocimientos tecnológicos, científicos y jurídicos para obtener elementos materiales de prueba con validez jurídica y valor probatorio. Recordó que compañías y procesos judiciales de alto perfil, tanto en Colombia como en el exterior, dependían de un adecuado tratamiento de la evidencia digital desde su recolección hasta su análisis.

El conferencista enumeró los distintos componentes que podían contener información relevante en un caso de este tipo: el computador corporativo del

funcionario, dispositivos de almacenamiento externo, el servidor institucional, el ERP, las grabaciones de circuito cerrado en las bodegas, y el móvil corporativo asignado. Resaltó la importancia de que las organizaciones incorporaran en sus contratos laborales y políticas de TI cláusulas claras sobre la titularidad corporativa de la información en los dispositivos asignados, la prohibición de compartirla y la facultad de la empresa para inspeccionar y asegurar dichos equipos cuando fuera necesario. Explicó que esta previsión contractual evitaba inconvenientes jurídicos durante los procesos de recolección y aseguramiento de evidencia.

Agregó que, con estos elementos identificados, la estación de trabajo, el dominio y *hostname* del usuario, los registros del ERP y demás recursos digitales, se podía avanzar hacia un proceso ordenado de análisis forense que permitiera establecer responsabilidades dentro del eventual fraude.

Continuó explicando que, frente a los diferentes dispositivos y fuentes de información previamente identificados, el perito en informática forense debía proceder a una recolección forense de la evidencia. Señaló que este procedimiento se realizaba mediante software especializado disponible en el mercado y que su punto de partida era la creación de una imagen forense, entendida como una copia bit a bit de la información contenida en cada dispositivo.

Indicó que esta imagen forense debía formarse siguiendo un procedimiento estricto, ajustado a los parámetros que exigía la normativa para garantizar la validez jurídica del material recolectado. Explicó que el perito obtenía las imágenes del computador, del celular corporativo, del servidor y de los mensajes de datos del ERP, entre otros, y que cada una de ellas debía dividirse en dos segmentos: un almacén de evidencia, destinado a conservar intacta la información para asegurar su integridad, y un entorno de análisis, que permitía al experto revisar correos electrónicos, logs de eventos, trazabilidades y cualquier rastro digital dejado por el funcionario investigado.

A partir de esta distinción, enfatizó el rol que correspondía al abogado. Aclaró que, aunque la ejecución técnica era responsabilidad del perito, el abogado debía verificar que el proceso cumpliera con todas las garantías legales desde su inicio. Esto incluía la adecuada recolección, preservación y tratamiento de los elementos materiales probatorios, con el fin de que pudieran usarse posteriormente en instancias judiciales sin cuestionamientos sobre su validez.

Desde allí se remontó a la base normativa. Explicó que, para atribuir responsabilidad penal, el sistema colombiano exigía demostrar los hechos más allá de toda duda razonable, conforme al artículo 381 del Código de Procedimiento Penal. Indicó que, si la investigación interna revelaba la existencia de un delito, el caso necesariamente tendría repercusiones penales, por ejemplo, abuso de confianza o acceso abusivo

a un sistema informático, por lo que el tratamiento inicial de la evidencia debía cumplir con los requisitos que permitieran que un juez la valorara válidamente.

Señaló que la legislación reconocía múltiples medios para generar conocimiento al juzgador, incluyendo documentos, pruebas periciales y otros elementos técnicos que no vulneraran el ordenamiento jurídico. En este punto, explicó que era necesario distinguir entre la evidencia física tradicional y los elementos materiales probatorios digitales, dentro de los cuales se encontraban los mensajes de datos: correos electrónicos, logs, chats y documentos electrónicos.

Enfatizó que la definición de mensaje de datos provenía de la Ley 527 de 1999, norma estructural del derecho digital en Colombia. Explicó que el mensaje de datos consistía en información generada, enviada, recibida o almacenada por medios electrónicos, sin importar su formato. Destacó que, aunque la ley mencionaba ejemplos propios de su época, como telegrama, telex o telefax, el concepto abarcaba hoy toda manifestación digital de información.

Indicó que el artículo 5 de la Ley 527 prohibía negar efectos jurídicos o validez a información solo por estar contenida en un mensaje de datos, y que el artículo 6 permitía que estos cumplieran el requisito de “escrito” siempre que fueran susceptibles de consulta posterior. Explicó que esto consolidaba plenamente la fuerza jurídica del mensaje de datos en el ordenamiento colombiano.

Luego analizó el artículo 10, que establecía expresamente la admisibilidad de los mensajes de datos como medios de prueba y aclaraba que no era indispensable presentarlos en su formato original, siempre que pudieran reproducirse de manera fiable. Agregó que el artículo 11 introducía los criterios específicos para valorar su fuerza probatoria y que estos se centraban en tres requisitos esenciales: autenticidad, integridad y conservación/disponibilidad.

A continuación, desarrolló cada uno de estos pilares:

> – La autenticidad exigía identificar el origen del mensaje, es decir, el perfil digital desde el cual había sido generado o enviado.
>
> – La integridad consistía en demostrar que la información no había sido alterada o modificada desde su creación o recolección.
>
> – La conservación y disponibilidad requería garantizar que el mensaje pudiera consultarse posteriormente, ya fuera en su formato original o en un formato que reprodujera con exactitud su contenido.

Señaló que el artículo 12 precisaba los criterios para acreditar la conservación adecuada: accesibilidad futura, formato reproducible de manera exacta y

preservación de los metadatos, que contenían información clave como fecha, hora, origen y destino. Además, el artículo 13 permitía que el manejo técnico de esta conservación se realizara a través de terceros, siempre que cumplieran con las condiciones legales.

A partir de esto, reiteró que estos elementos establecían la validez jurídica y valor probatorio del mensaje de datos. Subrayó que las normas procesales, como el Código General del Proceso (CGP), reforzaban esta estructura normativa. Destacó que el artículo 244 del CGP presumía la autenticidad de los documentos electrónicos, siempre que existiera certeza sobre la identidad del emisor. Señaló que el artículo 247 exigía que los mensajes de datos fueran aportados en su formato original o en uno que reprodujera con exactitud la información, en concordancia con los requisitos de la Ley 527.

Con estos fundamentos, concluyó que la evidencia digital podía efectivamente conducir al convencimiento judicial necesario para atribuir responsabilidad penal o civil, siempre y cuando su recolección y conservación cumplieran desde el inicio con los criterios de autenticidad, integridad, disponibilidad y conservación definidos por la ley. Destacó que por ello el tratamiento inicial de la evidencia, cuando surgía el incidente dentro de la organización, era determinante para el éxito probatorio posterior.

El conferencista explicó que el valor probatorio de la evidencia digital dependía estrictamente del cumplimiento de los elementos analizados previamente, autenticidad, integridad, disponibilidad y conservación. Precisó que, en la práctica, el perito en informática forense era quien debía garantizar estos requisitos durante la recolección de la evidencia, utilizando software especializado para generar la imagen forense e indexar posteriormente la información en herramientas de análisis digital, con el fin de rastrear logs, correos electrónicos y demás elementos relevantes que permitieran atribuir responsabilidad.

Desde allí detalló qué debía verificar el abogado cuando recibía el informe pericial. Señaló que, aunque no existía un formato único u obligatorio para estos dictámenes, el abogado tenía la obligación de comprobar que el procedimiento seguido se ajustara a los estándares que imponían las normas internacionales en materia de evidencia digital. Expuso que la Ley 527 constituía la base jurídica, pero que resultaba indispensable contrastar el informe con lineamientos técnicos propios de estándares como la ISO 27037 o las guías del NIST, entre otras.

Indicó que uno de los principios rectores de todas estas normas era la integridad: el procedimiento debía excluir cualquier duda sobre una posible alteración de la evidencia. Para ello, explicó que estándares como el NIST SP 800-86 exigían la

identificación, etiquetado y registro adecuado de la evidencia, así como la verificación de integridad mediante el cálculo y comparación de códigos hash entre el original y la copia. Destacó que el analista debía documentar exhaustivamente el proceso, incluyendo modelo y número de serie del disco, software utilizado, versión, licencias vigentes, cadena de custodia y todo elemento que permitiera auditar posteriormente la recolección.

Señaló que la ISO 27037 reforzaba estos criterios, al exigir confiabilidad, auditabilidad, trazabilidad, disponibilidad de la documentación y justificabilidad del método utilizado. Esta norma exigía que cualquier tercero pudiera reproducir y validar el procedimiento aplicado. León insistió en que, cuando el perito afirmaba haber aplicado una norma determinada, el abogado debía verificar punto por punto su cumplimiento; de no ser así, el dictamen carecería de la solidez técnica necesaria para sostenerse en juicio.

Explicó que esta verificación minuciosa hacía parte del trabajo del abogado cuando evaluaba contradictores periciales o cuando debía determinar la validez de un proceso de recolección de evidencia digital. Advirtió que, si el informe no se ajustaba estrictamente a la metodología declarada por el perito, ello afectaba la garantización de integridad, auditabilidad y justificabilidad del procedimiento.

Añadió que, además de las normas internacionales, podían existir lineamientos locales, como el manual de la Fiscalía General de la Nación, aunque este no fuera tan profundo en materia de evidencia digital. Reiteró que la estructura final del informe dependía del perito, pero debía reflejar con claridad el cumplimiento de la metodología anunciada.

Posteriormente retomó el caso práctico expuesto al inicio. Explicó que, tras el análisis forense, se comprobó que el jefe de inventarios había accedido al sistema con privilegios de administrador y había modificado registros del ERP gracias a fallas de control interno, como la ausencia de segmentación de funciones y la existencia de accesos amplios sin restricciones. Añadió que del computador del funcionario se recuperó un archivo Excel previamente eliminado, en el cual estaban registrados los pagos que recibía del proveedor involucrado. También se hallaron correos electrónicos y mensajes que evidenciaban la relación ilícita entre ambos.

Señaló que, contrario a lo que muchos imaginaban, en la práctica los responsables de fraudes digitales dejaban múltiples rastros. Señaló que cada clic quedaba registrado en sistemas y dispositivos, lo que permitía reconstruir la trazabilidad incluso de información eliminada. A partir de estos hallazgos, la organización pudo confirmar la materialización del fraude y adoptar decisiones estratégicas, tales como la terminación unilateral del contrato, el inicio del proceso disciplinario y la activación de acciones judiciales.

Explicó que el dictamen de informática forense, conformado por el informe técnico de recolección, el análisis pericial y la certificación correspondiente, constituyó un insumo probatorio robusto para iniciar un proceso penal por acceso abusivo a un sistema informático y abuso de confianza. Recordó que la Corte Suprema de Justicia había reiterado que este delito podía configurarse incluso cuando el acceso provenía de un funcionario autorizado, siempre que dicho acceso excediera las funciones para las cuales había sido otorgado.

El conferencista concluyó que un procedimiento adecuado de recolección de evidencia digital, ejecutado conforme a las normas técnicas y jurídicas aplicables, permitía a las organizaciones tomar decisiones internas con seguridad jurídica y garantizar la eficacia de los procesos judiciales posteriores. Reiteró que, para el abogado, resultaba esencial comprender tanto la estructura técnica del mensaje de datos como los elementos legales que garantizaban su validez probatoria.

Finalmente, indicó que la sesión había permitido abordar la premisa central: qué debía tener en cuenta el abogado frente a la evidencia digital, cómo debía entender los pilares del mensaje de datos y por qué la informática forense se había convertido en una herramienta indispensable para las investigaciones internas y los procesos judiciales. Con ello, cedió nuevamente la palabra al moderador.

De manera seguida, Andrés Moreno dio paso a algunas preguntas de los asistentes, iniciando por una inquietud relacionada con la dificultad de atribuir responsabilidad cuando el ataque provenía de un ciberdelincuente externo. La pregunta subrayaba que, a diferencia de los fraudes internos, los atacantes externos solían eliminar sistemáticamente sus rastros, lo que complicaba el proceso de investigación.

Para responder, el conferencista explicó que, efectivamente, los ciberataques externos planteaban mayores retos, y que el éxito de la trazabilidad dependía de la inmediatez de la reacción, del despliegue de un plan de contención, y de la capacidad de asegurar rápidamente la evidencia digital comprometida. Destacó que, ante un ciberataque, la organización debía activar de inmediato un equipo articulado entre comunicaciones, operaciones, tecnología y asesoría jurídica para aislar las áreas afectadas, mantener la continuidad operativa y, en paralelo, capturar los datos que permitieran reconstruir los eventos. Subrayó que era indispensable recolectar la evidencia antes de que la volatilidad propia de ciertos datos —como registros en memoria RAM o sesiones activas— los hiciera desaparecer.

Explicó que la investigación debía concentrarse en reconstruir el punto de entrada, la técnica empleada y los rastros que hubieran quedado, aunque estos fueran mínimos, e insistió en que la articulación inmediata con Policía, Interpol u otras autoridades podía ser determinante en ataques transnacionales, como los que involucraban *ransomware* o fraudes mediante suplantación del CEO.

Una segunda pregunta se orientó hacia las políticas internas organizacionales y la necesidad de que los programas de transparencia o los manuales de TI incluyeran pautas claras sobre el tratamiento de casos de fraude digital.

El conferencista señaló que esta previsión era esencial: todos los funcionarios, contratistas y miembros de la organización debían conocer que la información contenida en los dispositivos corporativos pertenecía a la compañía, que su uso tenía límites estrictos, que la confidencialidad era obligatoria y que la empresa podía realizar auditorías o recolecciones forenses cuando lo estimara necesario. Explicó que, en las organizaciones que habían incorporado estos lineamientos desde sus políticas internas, las investigaciones se habían desarrollado con mayor éxito, sin controversias sobre propiedad, acceso o manipulación de la información.

Posteriormente, un asistente planteó la tensión entre la mitigación de un incidente de seguridad y la preservación de la evidencia digital. El conferencista aclaró que, si la atención del incidente no se realizaba de forma técnica y adecuada, podía alterarse la integridad de los mensajes de datos, por ejemplo modificando metadatos al abrir archivos o al apagar indebidamente un equipo. Explicó que los peritos empleaban herramientas de bloqueo de lectura para evitar cualquier alteración durante la creación de la imagen forense y que, dependiendo del caso, el experto definía si debía apagarse inmediatamente el equipo o si, por el contrario, debía recolectarse la evidencia volátil antes de cualquier acción. Insistió en que la intervención de personas sin formación técnica podía comprometer seriamente el valor probatorio de la evidencia.

La última inquietud giró en torno a la formación y certificaciones que debía acreditar un perito informático para garantizar su idoneidad ante un proceso judicial. El expositor señaló que el Código General del Proceso exigía demostrar experticia, por lo que el perito debía acreditar formación en ingeniería de sistemas o áreas afines, estudios especializados en seguridad de la información o informática forense, certificaciones en las herramientas empleadas y experiencia verificable en otros casos similares. Indicó que la hoja de vida anexada al informe debía demostrar la trayectoria del experto, ya que la idoneidad del perito era uno de los principales puntos de debate en sede judicial.

Con estas intervenciones, Andrés agradeció nuevamente al expositor y a los asistentes por su participación, destacando la relevancia del tema para la práctica jurídica contemporánea y extendiendo la invitación para conocer la oferta académica de la Universidad Externado de Colombia en Derecho Informático y Nuevas Tecnologías. El evento concluyó con los agradecimientos del expositor, quien reiteró su disposición para atender consultas posteriores y subrayó la importancia de seguir fortaleciendo estos espacios académicos dado el impacto creciente de la evidencia digital en los procesos judiciales.