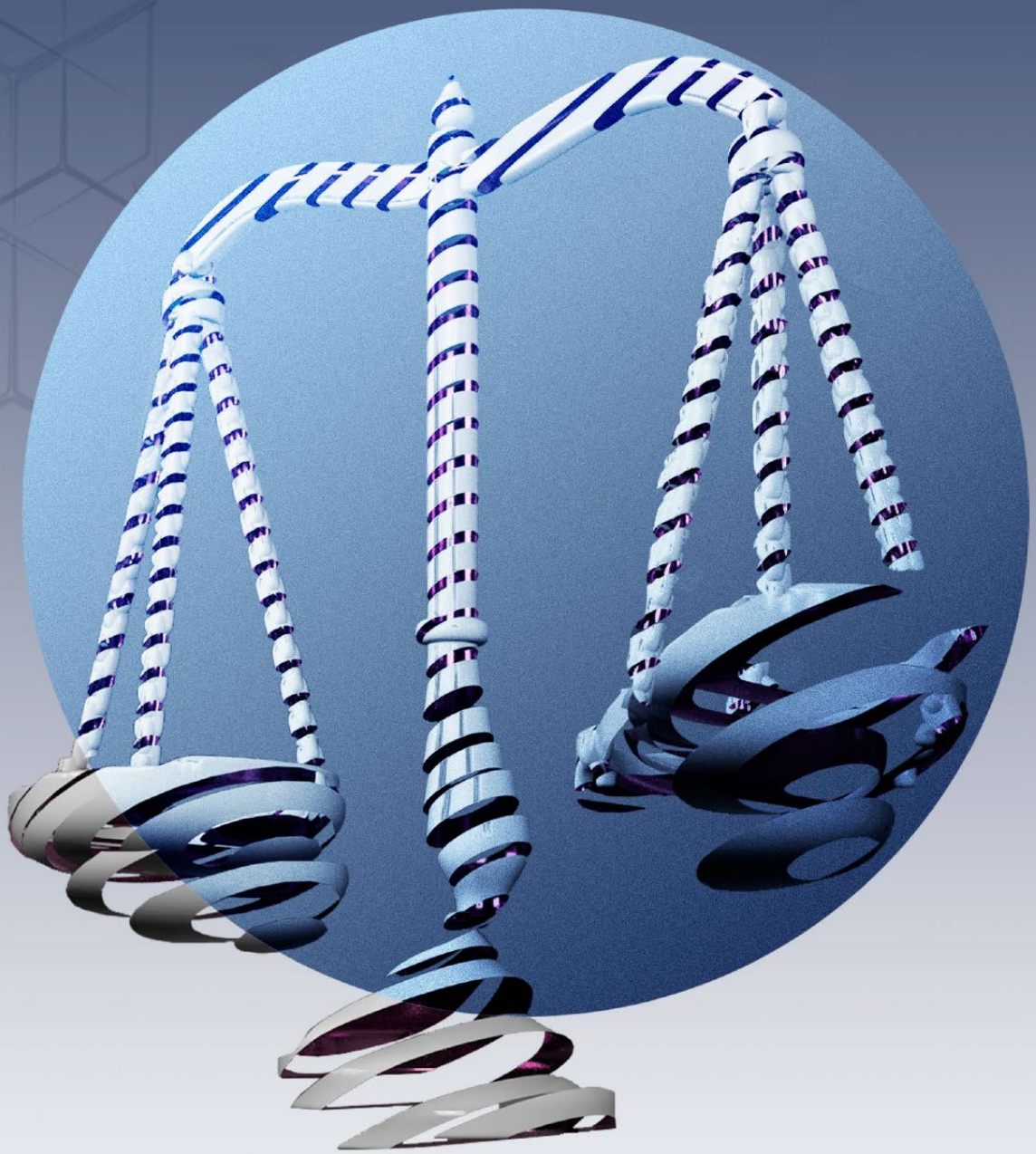
Evidencia Digital
Aspectos Generales



Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Escuela Judicial
"Rodrigo Lara Bonilla"

EVIDENCIA DIGITAL
Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia
Aspectos Generales

RAMA JUDICIAL DEL PODER PÚBLICO
CONSEJO SUPERIOR DE LA JUDICATURA

Presidenta
DIANA ALEXANDRA REMOLINA BOTÍA

Vicepresidenta
GLORIA STELLA LÓPEZ JARAMILLO

Magistradas y Magistrados
MAX ALEJANDRO FLÓREZ RODRÍGUEZ
MARTHA LUCÍA OLANO DE NOGUERA
AURELIO ENRIQUE RODRÍGUEZ GUZMÁN
JORGE LUIS TRUJILLO ALFARO

Directora Escuela Judicial
"Rodrigo Lara Bonilla"
MARY LUCERO NOVOA MORENO

Revisor - Metodólogo Escuela Judicial
"Rodrigo Lara Bonilla"
ALEXANDER RESTREPO RAMÍREZ

Autores Cartillas Evidencia Digital
y Prueba Electrónica
FREDY BAUTISTA GARCÍA
ÁLVARO JOSÉ MOSQUERA SUÁREZ
ANDRÉS MENESES OBANDO
DANIEL RÍOS SARMIENTO

Diseño e Ilustración de portada
CÉSAR MONROY

Diseño y diagramación
CAROLINA FRANCO

ISBN: En trámite

Podcast Evidencia Digital:
https://anchor.fm/evidenciadigital

Contenido

Índice de ilustraciones

Índice de tablas

1. CONVENCIONES, ABREVIATURAS, SIGLAS Y GLOSARIO

1.1. TABLA DE CONVENCIONES

Tabla 1. Convenciones

O	Objetivo general de la Guía
Og	Objetivo general
Oe	Objetivo específico
Co	Contenidos
Ap	Actividades pedagógicas
Ae	Autoevaluación
J	Jurisprudencia
B	Bibliografía

1.2. LISTA DE ABREVIATURAS

Tabla 2. Abreviaturas

Art.	Artículo
Cap.	Capítulo
CP	Constitución Política
EJRLB	Escuela Judicial Rodrigo Lara Bonilla
MP	Magistrado o Magistrada Ponente
Núm.	Numeral
Tit.	Título
Trad.	Traducción
EDiPE	Evidencia Digital y Prueba Electrónica
TIC	Tecnologías de la Información y de las Telecomunicaciones
IOCE	International Organization On Computer Evidence (Organización Internacional de Evidencia Digital)

1.3. LISTA DE SIGLAS

Tabla 3. Siglas

APB	Aprendizaje Basado en Problemas
CSJ	Consejo Superior de la Judicatura
ICONTEC	Instituto Colombiano de Normas Técnicas y Certificación
MEN	Ministerio de Educación Nacional
GAA	Guía de Aprendizaje Autodirigido
RIAEJ	Red Iberoamericana de Escuelas Judiciales
SEA	Sistema de Evaluación del Aprendizaje
SIGCMA	Sistema Integrado de Gestión de la Calidad y el Medio

1.4. GLOSARIO

1.4.1. Mensaje de Datos MD

"La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax" (Colombia, 1999)[1]

1.4.2. Intercambio Electrónico de Datos (EDI)

"La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto" [Colombia, 1999][2]

1.4.3. Evidencia Digital

Mensajes de datos electrónicos que tiene vocación a reconocerse como plena prueba de un hecho, acto o contrato que haya sido suscrito en entornos digitales.

A diferencia de la evidencia física, que está compuesta de átomos, la evidencia digital está compuesta de un lenguaje lógico binario que representa una unidad de información.

1.4.4. Prueba Electrónica

Término implementado por el Art 216 del Código Administrativo de Colombia, para referirse a la "evidencia digital" definida de la siguiente manera: *"Será admisible la utilización de los medios electrónicos para efectos probatorios de conformidad con lo dispuesto en las normas que regulan la materia y en concordancia con las disposiciones de este código y las del código de procedimiento civil" (Administrativo, 2011)*[3]

1.4.5. Legal Tech (Derecho y Tecnología)

Creación, diseño, desarrollo y aplicación de software y hardware que compone tecnología especializada en ofrecer soluciones en el estudio y ejercicio del Derecho.

1 Colombia. Ley 527 de 1999 Comercio Electrónico. Colombia: Colombia, 1999. 2. [1 pág. 2]
2 Ibidem [1 pág. 2]
3 Administrativo, Código de Procedimiento Administrativo y de lo Contencioso. Artículo 216. [aut. libro] Colombia. LEY 1437 DE 3 2011. Colombia: s.n., 2011. [2 pág. 1]

2. PRESENTACIÓN

En el año 2019, la Escuela Judicial Rodrigo Lara Bonilla (EJRLB) cumplió su vigésimo primer aniversario *"como parte de la Sala Administrativa del Consejo Superior de la Judicatura (CSJ), tiempo en el cual ha venido consolidando su Misión de liderar la formación judicial con los más altos estándares de calidad, objetivo que no sido pensado únicamente en cumplimiento de procesos técnicos, sino de una formación integral que incluye el desarrollo humano, las competencias, el respeto y garantía del multiculturalismo como expresión de la democracia colombiana, y la ética como pilar de toda expectativa social e institucional de justicia y transparencia."* [4]

En el marco del cumplimiento de estos fines institucionales, se presenta, a continuación, la Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia, Aspectos Generales conforme con los lineamientos de la NTC 1486, la NTC 1487, y la ISO 9001-2015.

3. SINOPSIS PROFESIONAL Y LABORAL DE AUTORES

3.1 FREDY BAUTISTA GARCÍA

Fundador y primer director del Centro Cibernético de la Policía Nacional de Colombia.

Experto en Ciberseguridad, Investigador de Cibercrimen y Perito en Informática Forense Digital, participó en la redacción de la Ley de Delito Informáticos en Colombia y fue gestor de la Política de Ciberseguridad y Ciberdefensa, actualmente participa en materia de Política de Seguridad Digital en Colombia.

Fue presidente en dos oportunidades del Grupo de Trabajo Jefes de Unidades de Cibercrimen de INTERPOL para las Américas desde donde lideró importantes investigaciones contra el Crimen Transnacional.

Es actualmente docente universitario en los programas de Maestría y Especialización en Derecho Informático y Nuevas Tecnologías de la Universidad Externado de Colombia y participa como docente invitado en el programa de Maestría de Seguridad Informática en la Universidad de los Andes.

Ha sido formador en el Centro de Capacitación Judicial para Centro América y el

4 RAMÍREZ, ALEXANDER RESTREPO. 2019. MANUAL DE AUTORES PARA EL DISEÑO Y REDACCIÓN DE MÓDULOS DE APRENDIZAJE AUTODIRIGIDO. Bogotá D.C.: CONSEJO SUPERIOR DE LA JUDICATURA, 2019. (3 pág. 5)

Caribe en el Taller sobre la Obtención de Evidencia Digital para National Center for State Courts e instructor en el programa de Formación Especializada en Informática Forense para la Oficina Regional para Centro América y el Caribe de la Naciones Unidas en ROPAN.

Es Criminalista y cuenta con posgrados en Derecho Procesal Penal, Auditoria Forense, Administración de Laboratorios de Informática Forense, Crimen Organizado, Corrupción y Terrorismo. Actualmente es consultor de la OEA, FELABAN (Federación Latinoamericana de Bancos) y UNODC para Colombia.

3.2 ÁLVARO JOSÉ MOSQUERA SUÁREZ

Ha sido director del VII Curso de Formación Judicial para Jueces y Magistrados de la República de le Escuela Judicial "Rodrigo Lara Bonilla", Gerente del Programa ReintegraTIC de la Agencia para la Reincorporación y normalización de la Presidencia de la República, Asesor Regional de Teletrabajo, Coordinador de Formación de la Subdirección de Comercio Electrónico del Ministerio TIC, Asesor Nacional de Pedagogía del Programa Computadores para Educar.

Es Magister en Comunicación, Educación y Cultura de la Universidad Autónoma de Barcelona, Especialista en Marketing Digital y Licenciado en Educación Básica con énfasis en Tecnología e Informática.

3.3. ANDRÉS MENESES OBANDO

Magíster en Derecho Informático y de las Nuevas Tecnologías, Universidad Externado de Colombia, especialista en Redes y Servicios Telemáticos, especialista en Gerencia Informática, profesional en Ingeniería de Sistemas.

Se ha desempeñado como docente de Informática jurídica, TIC asociadas al derecho, derecho informático, ingeniería de software II y III y Fundamentos de Derecho, desde la educación básica hasta la educación superior.

Durante su vida profesional ha desempeñado cargos en el Ministerio TIC, con los programas de Computadores para Educar, Revolución y En TIC Confío.

Actualmente se desempeña como perito informático, prestando sus servicios a personas naturales y jurídicas.
Ha realizado estudios de investigación en desarrollo de aplicaciones móviles, pedagogía y evidencia digital.

3.4. DANIEL RÍOS SARMIENTO

Abogado de la Universidad del Rosario y candidato a Magister de Derecho Informático y de las nuevas Tecnologías de la Universidad Externado de Colombia.

Miembro Investigador de postgrado del Centro de Investigación de Derecho Informático CIDI de la Universidad Externado de Colombia. Investigador de la Democracia

Colombiana en la sociedad del conocimiento #CyberDemocraciaCo

Programador y desarrollador certificado en el programa Full Stack y Tecnologías Hibridas por Fedesoft, MinTIC y Colciencias en el 2018. Finalista en Premios Ingenio Categoría educación FEDESOFT 2017.

Programador de Internet de las Cosas IoT, certificado por Cisco Networking Academy 2019 y certificado en Fundamentos de programación y frontend por Bogotá Institute of Tecnology Bictia.com.co 2019

Experto en Derecho de Autor, Propiedad intelectual, marcas, delitos informáticos y programas de informática forense digital trabaja actualmente como abogado externo en las firmas Ríos Sarmiento Abogados, AbogadoTIC y @CyberAbogado y profesor investigador de la Escuela Mayor de Derecho de la Universidad Sergio Arboleda.

4. JUSTIFICACIÓN

La siguiente guía de aprendizaje autodirigido trata los aspectos generales de la Evidencia Digital y Prueba Electrónica (EDiPE) y se propone como una herramienta de capacitación en los fundamentos teóricos y la normatividad relacionada suficiente para una apropiación de las Tecnologías de la Información y de las Telecomunicaciones (TIC) en el ejercicio de la administración de la justicia en Colombia.

El propósito de este guía de aprendizaje es capacitar sobre los conceptos generales que él/la discente debe tener en cuenta como en fundamentos técnicos y jurídicos necesarios para afrontar la pregunta jurídica de ¿Cuándo el posible medio de prueba presentado en formato de Mensaje de Datos (MD), puede ser valorado y validado como (EDiPE) en un proceso judicial en Colombia?

Así mismo, esta guía fomenta integralmente la apropiación social del conocimiento relacionado con la evidencia digital y prueba electrónica (EDiPE) como posibles herramientas tecnológicas capaces de mejorar el desempeño profesional de los discentes en el cotidiano oficio del tratamiento de grandes volúmenes de mensajes de datos en la administración de la justicia.

Por otro lado, esta guía aclara las directrices de buenas prácticas jurídicas locales y estándares internacionales que procuren evitar cometer errores respecto a la valoración de la evidencia digital y la prueba electrónica (EDiPE), repasando la evolución normativa y las disposiciones que al respecto el Consejo Superior de la Judicatura ha emitido.

5. RESUMEN DE LA GUÍA

A modo de introducción por el especializado mundo de la EDiPE, esta guía de aprendizaje autodirigido presentará los principales aspectos que se deben tener en cuenta desde la perspectiva de las funciones propias de él/la discente de la administración de la Justicia en Colombia.

La guía parte de una exposición sucinta de los principios rectores que enmarcan la EDiPE desde el ordenamiento jurídico aplicable.

Posteriormente, la guía desglosará la totalidad de fuentes de derecho colombiano que trata la EDiPE, con el objetivo de aportar una herramienta de consulta digital, la cual conduce a hipervínculos oficiales del ordenamiento jurídico.

Una vez esbozado el ámbito jurídico, se entrará a explicar: de qué está compuesto la EDiPE (respuesta anticipada: mensajes de datos MD) y se complementará con una serie de recomendaciones técnicas y jurídicas que se requiere para que dicho mensaje de datos se convierta en EDiPE, explicando las definiciones técnicas y jurídicas que dan claridad sobre el concepto de EDiPE.

Entendiendo las definiciones técnicas y jurídicas para convertir Mensajes de Datos a EDiPE, la guía continúa aterrizándolo al derecho colombiano propiamente dicho, identificando consecuentemente unos principios forenses digitales que debe tener en cuenta él/la discente.

La guía recopila, posteriormente, los Principios Forenses de la International Organization On Computer Evidence (IOCE) con el fin de dotar de competencias a él/la discente que requiere cumplir estándares internacionales al momento de aplicar la EDiPE.

Entre los estándares internacionales, se detallará sobre los atributos de recuperación estandarizada de EDiPE y la aplicación teórica de los principios y atributos de EDiPE en la informática forense, el objetivo es aplicar los estándares en el procedimiento jurídico colombiano.

Para un abordaje integral, la guía continuará con las diferentes clases de EDiPE acorde a sus características técnicas y características legales.

Por último, se repasará sobre buenas prácticas forenses digitales, desde el Ciclo de vida de administración de la EDiPE (cadena de custodia), la auditabilidad y trazabilidad de la EDiPE, la valoración y validez jurídica de la EDiPE y cuatro (4) ejercicios de Estudio y análisis de casos relacionados.

6. RECOMENDACIÓN DE IMPLEMENTACIÓN

Para que tenga en cuenta él/la discente de la Guía de aprendizaje autodirigida: esta tiene como finalidad una capacitación teórico-práctica de los aspectos generales de la EDiPE.

6.1. ¿QUÉ ES GUÍA DIDÁCTICA DE APRENDIZAJE AUTODIRIGIDO?

Constituye para la EJRLB y el Plan de Formación de la Rama Judicial, unas:

> *"herramientas con especificaciones para realizar acciones puntuales de estudio autónomo de acuerdo con los objetivos de aprendizaje, recursos y material disponible en una Unidad, Curso/MAA o Diplomado. La GDAA presenta un plan para el desarrollo del curso/módulo; un calendario que organiza sesiones de trabajo virtual (foros), presencial (talleres, conversatorios, mesas de trabajo grupal), y da pautas sobre la consulta de material primario (necesario) o secundario (complementario), es decir, representa una operacionalización del plan de formación."* [5]

En el caso concreto de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 1. Aspectos Generales se compone de la siguiente manera:

Tabla 4. Modelo guía de aprendizaje

ÍTEM	DESCRIPCIÓN		
Aspectos Generales	Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 1. Aspectos Generales		
Objetivos: ¿para qué?	Nivel de Formación	**SABER**	**Identificar** Estándares técnicos y fuentes legales pertinentes a la evidencia digital y prueba electrónica. **Reconocer** aplicaciones de la tecnología como un escenario de desarrollo profesional y de apoyo a las actividades judiciales y procedimentales.

5 Ibidem (3 pág. 47)

ÍTEM	DESCRIPCIÓN
Requisitos previos:	Lectura Unidad 9 de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 1. Aspectos Generales.
Contenidos:	Subtema 1.1: Principios Rectores de la Evidencia Digital y Prueba Electrónica Subtema 1.2. Definiciones doctrinales de la Evidencia Digital y Prueba Electrónica Subtema 1.3. Fuentes de derecho colombiano relacionado con la Evidencia Digital y Prueba Electrónica Subtema 1.4. Mensaje de Datos Subtema 1.5: Evidencia Digital y Prueba Electrónica en el derecho colombiano Subtema 1.6: Principios forense digital Subtema 1.7: Principios Forenses de la International Organization on Computer Evidence Subtema 1.8: Atributos de recuperación estandarizada de Evidencia Digital y Prueba Electrónica Subtema 1.9: Aplicación teórica de administración de la Evidencia Digital y Prueba Electrónica Subtema 1.10. Clases de Evidencia Digital y Prueba Electrónica Subtema 1.11. Características técnicas de la Evidencia Digital y Prueba Electrónica Subtema 1.12. Características legales de la Evidencia Digital y Prueba Electrónica Subtema 1.13. Ciclo de vida de la administración de la Evidencia Digital y Prueba Electrónica Subtema 1.14. Auditabilidad y trazabilidad de la Evidencia Digital y Prueba Electrónica Subtema 1.15. Valoración y validez de la prueba electrónica
Estrategias metodológicas: ¿Cómo?	• Análisis y estudio de casos
Actividades: ¿Qué hacer?	**Análisis de casos por Grupos** Acorde a número de participantes, se divide en grupos de cincuenta por ciento (50%) cada uno, para analizar los casos Lectura Unidad de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 1. Aspectos Generales. Cada grupo debe resolver el caso defendiendo una postura contraria, basados en la lectura de Unidad 9. de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 1. Aspectos Generales. Se espera que la división por grupos permita ampliar el conocimiento sobre la ruta hermenéutica utilizada para resolver el caso, incluso, no se descarta que haya de manera motivada una desviación de la ruta jurisprudencial propuesta.
Recursos: ¿Qué usar?	Esta información debe ser proporcionada por los facilitadores conforme con la disponibilidad y la logística de cada Plan de Formación.

Temporalización: ¿Cuándo?	**Curso de formación inicial (Curso Concurso de Méritos):** una (1) sesión de ocho (8) horas (Reunión Inicial y Conversatorio local).
Evaluación: ¿qué, cuándo, cómo, con quién y para qué?	Valoración cuantitativa y cualitativa de lo aprendido, destrezas implementadas, habilidades adquiridas, actitudes demostradas, en la resolución de los casos: Lectura Unidad 9 de la Guía Didáctica de Aprendizaje Autodirigido de Evidencia Digital y Prueba Electrónica en Colombia N° 1. Aspectos Generales Para que aplique integralmente los procedimientos técnicos de la Evidencia Digital y Prueba Electrónica en Colombia.

Fuente: Elaboración propia con base en el MANUAL DE AUTORES PARA EL DISEÑO Y REDACCIÓN DE MÓDULOS DE APRENDIZAJE AUTODIRIGIDO DE LA ESCUELA JUDICIAL RODRIGO LARA BONILLA 2019.

7. MISIÓN Y OBJETIVOS DE LA GUÍA

7.1. MISIÓN

Capacitar a él/la discente en la Investigación sobre Aspectos generales de la Evidencia Digital y Prueba Electrónica en Colombia:

7.2. OBJETIVO GENERAL DE LA GUÍA

Proporcionar a él/la discente de herramientas de aprendizaje orientadas a potenciar los conocimientos, habilidades y destrezas para desempeñar de forma eficiente y eficaz sus funciones, mediante la realización de procesos de formación y capacitación, promoviendo su desarrollo integral para el mejoramiento de la Administración de Justicia.

7.3. OBJETIVOS ESPECÍFICOS DE LA GUÍA

7.3.1. Identificar

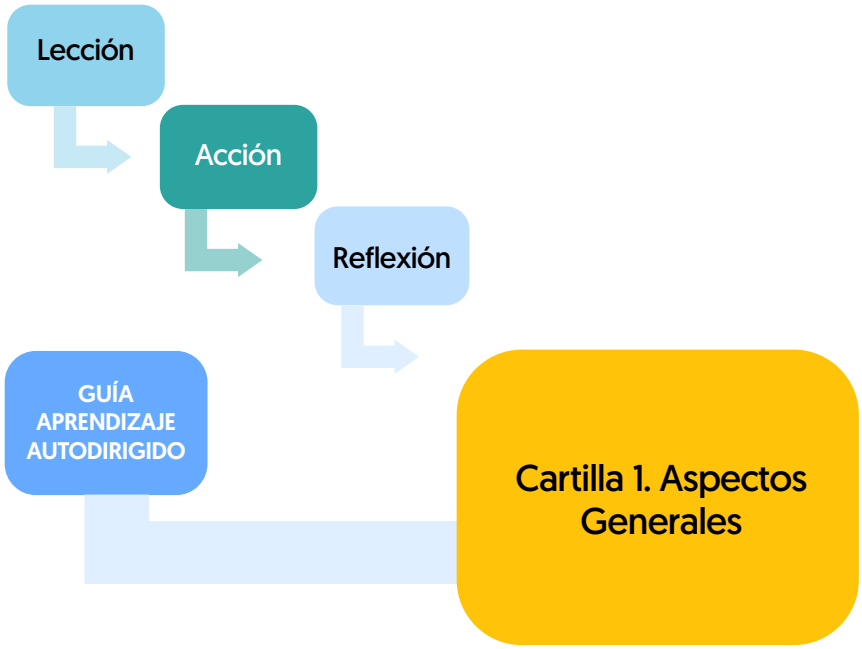
Estándares técnicos y fuentes legales pertinentes a la evidencia digital y prueba electrónica.

7.3.2. Reconocer

Aplicaciones de la tecnología como un escenario de desarrollo profesional y de apoyo a las actividades judiciales y procedimentales.

8. MAPA CONCEPTUAL DE LA GUÍA

Ilustración 1. Mapa conceptual Guía de Aspectos Generales de la EDiPE



Fuente: Elaboración propia.

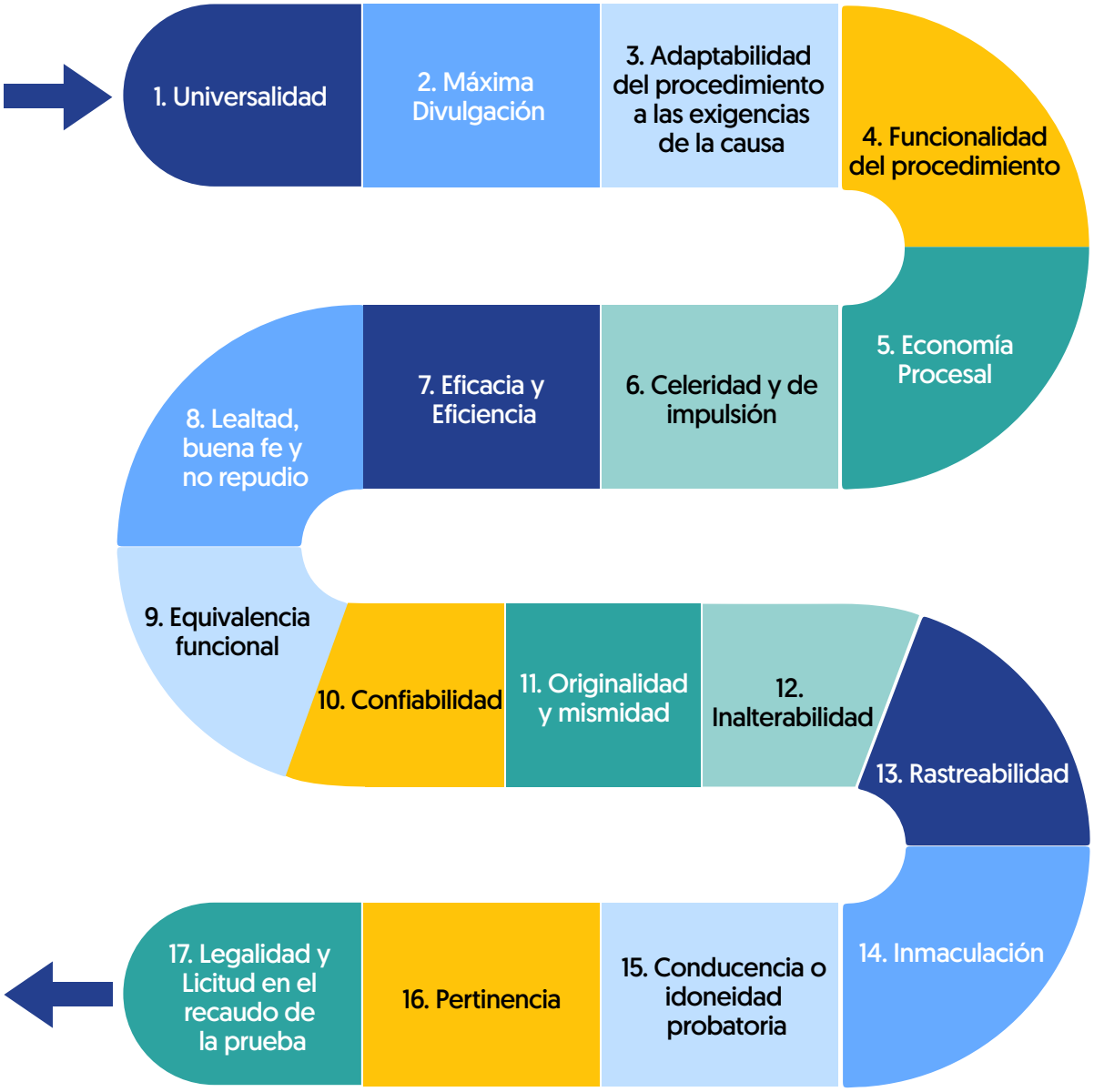
9. ASPECTOS GENERALES DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

9.1. PRINCIPIOS RECTORES DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

A continuación, se expone, gracias a una recopilación de doctrina especializada en evidencia digital, una serie de principios formulados que enmarcan y delimitan el alcance de la aplicación del derecho a través del entorno digital.

Estos principios proponen aportar una delimitación de aspectos esenciales para tener en cuenta para determinar y valorar idóneamente la prueba digital.

Ilustración 2. Principios Rectores de la EDiPE en Colombia



Fuente Elaboración propia fundamentados en Doctrina especializada del Dr. (Romelio, 2017)[6]

9.2. DEFINICIONES DOCTRINALES DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

Teniendo en cuenta que el uso de los términos depende de la jurisdicción, es decir que se habla generalmente de evidencia digital, pero en la competencia administrativa y contenciosa administrativa de prueba electrónica, a continuación, encontrará los temas relevantes para tener en cuenta al momento de afrontar este tipo de medios de prueba en un juicio particular.

6 Romelio, Daza Molina. 2017. Las TIC Ante el Derecho Colombiano y la Gestión Judicial. Bogotá D.C.: Librería Ediciones del Profesional L.T.D.A., 2017. (4)

Entiéndase por evidencia digital cualquier medio probatorio en formato de mensaje de datos (en adelante MD) que esté almacenado o transmitido en formato digital de tal manera que tenga vocación a probar un acto, contrato o hecho que sea relevante en un juicio o proceso judicial.

La doctrina especializada contextualiza el MD de la siguiente manera: *"la ley 270 de 1996 contempló en su artículo 95 la incorporación de la tecnología de avanzada al servicio de la administración de la justicia. Así mismo dispuso que dicha tecnología debiera enfocarse principalmente a mejorar la práctica de pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información"*[7]

El Dr. Daniel Peña Valenzuela define la prueba digital así: *"Es prueba digital cuando la información que corresponda al hecho, acto o contrato que se quiera probar es creada, generada, transmitida o almacenada como mensaje de datos mediante un sistema electrónico de información. La información digital, objeto de prueba, no es material ni corpórea, sino que es un código binario que representa una imagen y un contenido, aunque el medio en el que encuentra almacenada sí lo sea"*[8]

9.3 FUENTES DE DERECHO COLOMBIANO RELACIONADO CON LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

A continuación, encontrará una lista de fuentes jurídicas ordenadas cronológicamente y el contenido normativo que regulan la relación entre la gestión judicial y la tecnología en Colombia.

Tabla 5. Fuentes de Derecho Colombiano aplicado a la EDiPE

FUENTE	DESCRIPCIÓN	ENLACE
Documento CONPES 2790 de 1995 <Gestión Pública orientada a resultados	El Estado evidencio la importancia de mejorar la relación con los ciudadanos desde la perspectiva de los trámites, por lo anterior, se creó la Unidad de Eficiencia de la Consejería Presidencial para el Desarrollo Institucional para regular trámites innecesarios que permitiera una atención pública más eficiente.	https://www.armada.mil.co/es/content/documento-conpes-2790-de-1995-gesti%C3%B3n-p%C3%BAblica-orientada-resultados
Artículo 26, Decreto Ley 2150 de 1995 <Decreto Anti-tramites >	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.	http://www.secretariasenado.gov.co/senado/basedoc/decreto_2150_1995.html

7 Ibidem (4 pág. 225)
8 Peña, Daniel. De la Firma Manuscrita a las Firmas Electrónicas y Digital. Bogotá D.C.: Universidad Externado de Colombia, 2015 (5 pág. 72)

FUENTE	DESCRIPCIÓN	ENLACE
Ley Modelo sobre Comercio Electrónico	Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional	http://campus.usal.es/~derinfo/derinfo/CE/LMCNUDMI.HTM
Ley 270 de 1996 ESTATUTARIA DE LA ADMINISTRACIÓN DE JUSTICIA	ARTÍCULO 95. TECNOLOGÍA AL SERVICIO DE LA ADMINISTRACIÓN DE JUSTICIA. El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información. Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones. Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales. Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad, y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0270_1996.html
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html
Documento CONPES 3072 de 2000 <Agenda de Conectividad >	Busca masificar el uso de las Tecnologías de la Información y con ello aumentar la competitividad del sector productivo, modernizar las instituciones públicas y de gobierno, y socializar el acceso a la información, siguiendo los lineamientos establecidos en el Plan Nacional de Desarrollo 1998 – 2002 "Cambio para Construir la Paz"	https://www.mintic.gov.co/portal/604/articles-3498_documento.pdf

FUENTE	DESCRIPCIÓN	ENLACE
Ley 594 de 2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.	https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4275
Directiva presidencial 02 de 2000	Diseño de la Agenda de Conectividad, como política de Estado, que busca masificar el uso de las TIC en Colombia y aumentar la competitividad del sector productivo, modernizar las instituciones públicas y socializar el acceso a la información.	https://www.mintic.gov.co/portal/604/articles-3646_documento.pdf
Decreto 127 de 2001	Por el cual se crean las Consejerías y Programas Presidenciales en el Departamento Administrativo de la Presidencia de la República. Creó el Programa Presidencial para el Desarrollo de las Tecnologías de la Información y de las Comunicaciones.	https://www.mintic.gov.co/portal/604/articles-3551_documento.pdf
Art. 102. Código Disciplinario Único LEY 734 DE 2002	Art. 102. NOTIFICACIÓN POR MEDIOS DE COMUNICACIÓN ELECTRÓNICOS. <Artículo derogado a partir del 1 de julio de 2021, por el artículo 265 de la Ley 1952 de 2019> Las decisiones que deban notificarse personalmente podrán ser enviadas al número de fax o a la dirección de correo electrónico del investigado o de su defensor, si previamente y por escrito, hubieren aceptado ser notificados de esta manera. La notificación se entenderá surtida en la fecha que aparezca en el reporte del fax o en que el correo electrónico sea enviado. La respectiva constancia será anexada al expediente.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0734_2002.html
Directiva Presidencial 10 de 2002	Programa de renovación de la Administración Pública: hacia un Estado Comunitario y crea el Programa de Renovación de la Administración Pública.	https://www.mintic.gov.co/portal/604/w3-article-3652.html?_noredirect=1
Decreto 3107 de 2003	Suprímase en el Departamento Administrativo de la Presidencia de la República el Programa Presidencial para el Desarrollo de las Tecnologías de la Información y de las Comunicaciones.	https://www.mintic.gov.co/portal/604/articles-3599_documento.pdf
Decreto 3816 de 2003	Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública y Crea la Comisión Intersectorial de Políticas y Gestión de la Información para la Administración Pública.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=11233

FUENTE	DESCRIPCIÓN	ENLACE
CONPES 3292 de 2004	Creó el Proyecto de Racionalización y Automatización de Trámites, que regula toda la cadena de pasos que se tienen que seguir para la consecución de los trámites sectoriales mediante tres pilares: Coordinación Interinstitucional y adecuación normativa, Análisis funcional para la racionalización y Fortalecimiento tecnológico.	https://www.mintic.gov.co/portal/inicio/3501:Conpes-3292-de-2004
Artículo 170. Ley 906 de 2004 Código de Procedimiento Penal	Artículo 170, REGISTRO DE LA NOTIFICACIÓN. El secretario deberá llevar un registro de las notificaciones realizadas tanto en audiencia como fuera de ella, para lo cual podrá utilizar los medios técnicos idóneos.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html
Artículo 172. Ley 906 de 2004 Código de Procedimiento Penal	Artículo 172. FORMA. Las citaciones se harán por orden del juez en la providencia que así lo disponga, y serán tramitadas por secretaría. A este efecto podrán utilizarse los medios técnicos más expeditos posibles y se guardará especial cuidado de que los intervinientes sean oportuna y verazmente informados de la existencia de la citación. El juez podrá disponer el empleo de servidores de la administración de justicia y, de ser necesario, de miembros de la fuerza pública o de la policía judicial para el cumplimiento de las citaciones.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html
Artículo 275. Ley 906 de 2004 Código de Procedimiento Penal	ARTÍCULO 275. ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA. Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes: g) El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html
LEY 962 DE 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.	http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.html
Acuerdo No. PSAA06-3334 de 2006	Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia (aplica para civil, contencioso administrativo, laboral, penal y disciplinario).	https://normograma.info/crc/docs/pdf/acuerdo_csjudicatura_3334_2006.pdf
Ley 1151 de 2007 Plan Nacional de Desarrollo	Formulación de una política de Gobierno electrónico que comprende: modernización de esquemas de rendición de cuentas, difusión de la información, automatización de trámites través de sistemas de información.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1151_2007.html

FUENTE	DESCRIPCIÓN	ENLACE
Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de 2007	La presente Convención será aplicable al empleo de las comunicaciones electrónicas en relación con la formación o el cumplimiento de un contrato entre partes cuyos establecimientos estén en distintos Estados.	https://www.uncitral.org/pdf/spanish/texts/electcom/06-57455_Ebook.pdf
Decreto 1151 de 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.	https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.	https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009
Circular 58 de 2009 Procuraduría General de la Nación	Por medio de la cual la Procuraduría General de la Nación cumple con Decreto 1151 de 14 de abril de 2008, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.	https://www.mintic.gov.co/portal/604/articles-3518_documento.pdf
Corte Suprema de Justicia (Sala de Casación Civil) RAD. 11001 3110 005 2004 01074 01. del 16 de diciembre de 2010	En este caso la Corte Suprema de Justicia evalúa la admisibilidad y valoración probatoria de un correo electrónico, aportado en un proceso de familia.	https://arkhaios.com/wp-content/uploads/2011/07/DOCUMENTO-ELECTRNICO-autenticidad-y-veracidad.pdf
Artículo 186. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 186. ACTUACIONES A TRAVÉS DE MEDIOS ELECTRÓNICOS. Todas las actuaciones judiciales susceptibles de surtirse en forma escrita se podrán realizar a través de medios electrónicos, siempre y cuando en su envío y recepción se garantice su autenticidad, integridad, conservación y posterior consulta, de conformidad con la ley. La autoridad judicial deberá contar con mecanismos que permitan acusar recibo de la información recibida, a través de este medio.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html

FUENTE	DESCRIPCIÓN	ENLACE
	PARÁGRAFO. La Sala Administrativa del Consejo Superior de la Judicatura adoptará las medidas necesarias para que en un plazo no mayor de cinco (5) años, contados a partir de la vigencia del presente Código, sea implementado con todas las condiciones técnicas necesarias el expediente judicial electrónico, que consistirá en un conjunto de documentos electrónicos correspondientes a las actuaciones judiciales que puedan adelantarse en forma escrita dentro de un proceso.	
Artículo 197. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 197. DIRECCIÓN ELECTRÓNICA PARA EFECTOS DE NOTIFICACIONES. Las entidades públicas de todos los niveles, las privadas que cumplan funciones públicas y el Ministerio Público que actúe ante esta jurisdicción, deben tener un buzón de correo electrónico exclusivamente para recibir notificaciones judiciales. Para los efectos de este Código se entenderán como personales las notificaciones surtidas a través del buzón de correo electrónico.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html
Artículo 198. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 198. NOTIFICACIÓN PERSONAL DEL AUTO ADMISORIO Y DEL MANDAMIENTO DE PAGO A ENTIDADES PÚBLICAS, AL MINISTERIO PÚBLICO, A PERSONAS PRIVADAS QUE EJERZAN FUNCIONES PÚBLICAS Y A PARTICULARES QUE DEBAN ESTAR INSCRITOS EN EL REGISTRO MERCANTIL.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html
Artículo 200. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 200. FORMA DE PRACTICAR LA NOTIFICACIÓN PERSONAL DEL AUTO ADMISORIO DE LA DEMANDA A OTRAS PERSONAS DE DERECHO PRIVADO. Para la práctica de la notificación personal que deba hacerse a personas de derecho privado que no tengan dirección electrónica para notificaciones judiciales por no estar inscritas en el registro mercantil, se procederá de acuerdo con lo previsto en los artículos 315 y 318 del Código de Procedimiento Civil.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html
Artículo 201. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 201. NOTIFICACIONES POR ESTADO. Los autos no sujetos al requisito de la notificación personal se notificarán por medio de anotación en estados electrónicos para consulta en línea bajo la responsabilidad del secretario. La inserción en el estado se hará el día siguiente al de la fecha del auto y en ella ha de constar: 1. La identificación del proceso. 2. Los nombres del demandante y el demandado. 3. La fecha del auto y el cuaderno en que se halla.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html

FUENTE	DESCRIPCIÓN	ENLACE
	4. La fecha del estado y la firma del secretario. El estado se insertará en los medios informáticos de la Rama Judicial y permanecerá allí en calidad de medio notificador durante el respectivo día. De las notificaciones hechas por estado el secretario dejará certificación con su firma al pie de la providencia notificada y se enviará un mensaje de datos a quienes hayan suministrado su dirección electrónica. De los estados que hayan sido fijados electrónicamente se conservará un archivo disponible para la consulta permanente en línea por cualquier interesado, por el término mínimo de diez (10) años. Cada juzgado dispondrá del número suficiente de equipos electrónicos al acceso del público para la consulta de los estados.	
Artículo 203. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 203. NOTIFICACIÓN DE LAS SENTENCIAS. Las sentencias se notificarán, dentro de los tres (3) días siguientes a su fecha, mediante envío de su texto a través de mensaje al buzón electrónico para notificaciones judiciales. En este caso, al expediente se anexará la constancia de recibo generada por el sistema de información, y se entenderá surtida la notificación en tal fecha.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html
Artículo 205. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 205. NOTIFICACIÓN POR MEDIOS ELECTRÓNICOS. Además de los casos contemplados en los artículos anteriores, se podrán notificar las providencias a través de medios electrónicos, a quien haya aceptado expresamente este medio de notificación. En este caso, la providencia a ser notificada se remitirá por el secretario a la dirección electrónica registrada y para su envío se deberán utilizar los mecanismos que garanticen la autenticidad e integridad del mensaje. Se presumirá que el destinatario ha recibido la notificación cuando el iniciador recepcione acuse de recibo o se pueda por otro medio constatar el acceso del destinatario al mensaje. El secretario hará constar este hecho en el expediente. De las notificaciones realizadas electrónicamente se conservarán los registros para consulta permanente en línea por cualquier interesado.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html
Artículo 206. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Artículo 206. DEBER DE COLABORACIÓN. Los empleados de cada despacho judicial deberán asistir y auxiliar a los usuarios en la debida utilización de las herramientas tecnológicas que se dispongan en cada oficina para la consulta de información sobre las actuaciones judiciales.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1437_2011.html

FUENTE	DESCRIPCIÓN	ENLACE
Artículo 216. Ley 1437 de 2011 Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014. Creó y reglamentó el expediente judicial electrónico el cual establece parámetros legales en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y el Código General del Proceso.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1450_2011.html
Ley 1450 de 2011 DECRETO <LEY> 19 DE 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.	http://www.secretariasenado.gov.co/senado/basedoc/decreto_0019_2012.html
Acuerdo N° PSAA12-9269 del 27 de febrero de 2012	Por el que se expide el Plan Estratégico Tecnológico de la Rama Judicial que busca la actualización, eficacia y eficiencia del sistema de administración de la justicia.	http://actosadministrativos.ramajudicial.gov.co/GetFile.ashx?url=%7E%2FApp_Data%2FUpload%2FPSAA12-9269.pdf
Numeral 14 Artículo 78. Ley 1564 de 2012 Código General del Proceso	Numeral 14 Artículo 78. DEBERES DE LAS PARTES Y SUS APODERADOS. Son deberes de las partes y sus apoderados: 14. Enviar a las demás partes del proceso después de notificadas, cuando hubieren suministrado una dirección de correo electrónico o un medio equivalente para la transmisión de datos, un ejemplar de los memoriales presentados en el proceso. Se exceptúa la petición de medidas cautelares. Este deber se cumplirá a más tardar el día siguiente a la presentación del memorial. El incumplimiento de este deber no afecta la validez de la actuación, pero la parte afectada podrá solicitar al juez la imposición de una multa hasta por un salario mínimo legal mensual vigente (1 smlmv) por cada infracción.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html
Numeral 10 Artículo 82. Ley 1564 de 2012 Código General del Proceso	Numeral 10 Artículo 82. REQUISITOS DE LA DEMANDA. Salvo disposición en contrario, la demanda con que se promueva todo proceso deberá reunir los siguientes requisitos: 10. El lugar, la dirección física y electrónica que tengan o estén obligados a llevar, donde las partes, sus representantes y el apoderado del demandante recibirán notificaciones personales.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html
Numeral 5 Artículo 96. Ley 1564 de 2012 Código General del Proceso	Numeral 5. El lugar, la dirección física y de correo electrónico que tengan o estén obligados a llevar, donde el demandado, su representante o apoderado recibirán notificaciones personales.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html

FUENTE	DESCRIPCIÓN	ENLACE
Artículo 103. Ley 1564 de 2012 Código General del Proceso	USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES. En todas las actuaciones judiciales deberá procurarse el uso de las tecnologías de la información y las comunicaciones en la gestión y trámite de los procesos judiciales, con el fin de facilitar y agilizar el acceso a la justicia, así como ampliar su cobertura. Las actuaciones judiciales se podrán realizar a través de mensajes de datos. La autoridad judicial deberá contar con mecanismos que permitan generar, archivar y comunicar mensajes de datos. En cuanto sean compatibles con las disposiciones de este código se aplicará lo dispuesto en la Ley 527 de 1999, las que lo sustituyan o modifiquen, y sus reglamentos.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html
Artículo 105. Ley 1564 de 2012 Código General del Proceso	FIRMAS. Los funcionarios y empleados judiciales deberán usar, en todos sus actos escritos, firma acompañada de antefirma. Podrán usar firma electrónica, de conformidad con el reglamento que expida el Consejo Superior de la Judicatura.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html
Numeral 4. Y sig. Artículo 107. Ley 1564 de 2012 Código General del Proceso	AUDIENCIAS Y DILIGENCIAS. Las audiencias y diligencias se sujetarán a las siguientes reglas: (...) 4. Grabación. La actuación adelantada en una audiencia o diligencia se grabará en medios de audio, audiovisuales o en cualquiera otro que ofrezca seguridad para el registro de lo actuado. 5. Publicidad. Las audiencias y diligencias serán públicas, salvo que el juez, por motivos justificados, considere necesario limitar la asistencia de terceros. El Consejo Superior de la Judicatura deberá proveer los recursos técnicos necesarios para la grabación de las audiencias y diligencias. 6. Prohibiciones. Las intervenciones orales no podrán ser sustituidas por escritos. El acta se limitará a consignar el nombre de las personas que intervinieron como partes, apoderados, testigos y auxiliares de la justicia, la relación de los documentos que se hayan presentado y, en su caso, la parte resolutiva de la sentencia. Solo cuando se trate de audiencias o diligencias que deban practicarse por fuera del despacho judicial o cuando se presenten fallas en los medios de grabación, el juez podrá ordenar que las diligencias consten en actas que sustituyan el sistema de registro a que se refiere el numeral 4 anterior o que la complementen.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html

FUENTE	DESCRIPCIÓN	ENLACE
	El acta será firmada por el juez y de ella hará parte el formato de control de asistencia de quienes intervinieron. Cualquier interesado podrá solicitar una copia de las grabaciones o del acta, proporcionando los medios necesarios para ello. En ningún caso el juzgado hará la reproducción escrita de las grabaciones. De las grabaciones se dejará duplicado que hará parte del archivo del juzgado, bajo custodia directa del secretario, hasta la terminación del proceso.	
Artículo 111. Ley 1564 de 2012 Código General del Proceso	COMUNICACIONES. Los tribunales y jueces deberán entenderse entre sí, con las autoridades y con los particulares, por medio de despachos y oficios que se enviarán por el medio más rápido y con las debidas seguridades. Los oficios y despachos serán firmados únicamente por el secretario. Las comunicaciones de que trata este artículo podrán remitirse a través de mensajes de datos. El juez también podrá comunicarse con las autoridades o con los particulares por cualquier medio técnico de comunicación que tenga a su disposición, de lo cual deberá dejar constancia.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html
Artículo 247. Ley 1564 de 2012 Código General del Proceso	ARTÍCULO 247. VALORACIÓN DE MENSAJES DE DATOS. Serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud. La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1564_2012.html
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.	https://www.mintic.gov.co/portal/604/articles-3528_documento.pdf
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, Y se dictan otras disposiciones.	https://www.mintic.gov.co/portal/604/articles-3586_documento.pdf

FUENTE	DESCRIPCIÓN	ENLACE
Artículo 2. Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html
ACUERDO 002 DE 2014 Archivo General de la Nación	Por medio del cual se establecen los criterios básicos para creación, conformación, organización, control y consulta de los expedientes de archivo y se dictan otras disposiciones.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=61730
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.	https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596
ACUERDO 003 DE 2015 Archivo General de la Nación	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=61731
Decreto 1078 de 2015 Decreto Único Sectorial	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf
Ley 1753 de 2015	POR LA CUAL SE EXPIDE EL PLAN NACIONAL DE DESARROLLO 2014-2018 "TODOS POR UN NUEVO PAÍS"	https://www.mintic.gov.co/portal/604/articles-15015_documento.pdf
Decreto 415 de 2016	Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones."	http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf
Sentencia C 604 de 2016	Demanda de inconstitucionalidad contra el artículo 247 (parcial) de la Ley 1564 de 2012, “por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones”	https://www.corteconstitucional.gov.co/RELATORIA/2016/C-604-16.htm
Resolución 2405 de 25 de noviembre 2016	Por el cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité.	https://www.mintic.gov.co/portal/604/w3-article-47528.html?_noredirect=1

Fuente: Elaboración propia.

9.4. MENSAJE DE DATOS MD

Teniendo en cuenta la posibilidad didáctica de identificar la unidad de medida de la evidencia digital, sin duda alguna esta sería el mensaje de datos (MD). El concepto de MD abarca, desde lo particular a lo general, aquellos aspectos esenciales que se deben tener en cuenta, al momento de darle una connotación probatoria procesal.

Acorde a lo anterior, a continuación, se expone los principales supuestos relacionados con el MD cuando se propone darle una relevancia jurídica, partiendo de una definición sucinta, pasando por una visión comparativa entre el ejercicio judicial cotidiano, contrastado con los lineamientos expertos que capacitan buenas prácticas que se deben cumplir y la fuente jurídica especial que sustentan los lineamientos para tener en cuenta, a saber:

Tabla 6. Mensajes de datos

TEMA: Mensajes de Datos		
DEFINICIÓN: Información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplicar para identificar que es un MD?
El "pantallazo" no prueba el intercambio de MD, eje: https://play.google.com/store/apps/details?id=com.tiawy.fakechat	Se debe aplicar todos los requisitos de equivalencia funcional si se quiere convertir el MD en EDiPE	ACUERDO No. PSAA06-3334 DE 2006

Fuente: Elaboración propia.

Tabla 7. Reconocimiento jurídico de los MD

TEMA: Reconocimiento jurídico de los MD		
DEFINICIÓN: Refiere a la capacidad legal que tiene una MD para demostrar cierto hecho de tal manera que ostente carácter probatorio dentro de un trámite o proceso.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Se le da importancia al papel que reproduce el MD, como si fuera el único medio para aportar procesalmente.	Que se cumpla con el requisito de validez del MD: Que haya sido aportado en el mismo formato en que fue generado, enviado o recibido, o de algún otro formato que lo reproduzca. La impresión en papel del MD también aplica.	ARTÍCULO 5o. Ley 527 de 1999. RECONOCIMIENTO JURÍDICO DE LOS MENSAJES DE DATOS. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

Fuente: Elaboración propia.

Tabla 8. Requisitos jurídicos de los MD

TEMA: Requisitos Jurídicos de los MD		
DEFINICIÓN: Características con las que debe contar un MD acorde a la aplicación de normas, nacionales e internacionales, que regulan la materia que concluya en el reconocimiento como EDiPE dentro de un proceso judicial.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Existe un desconocimiento a acatar las normas que establecen requisitos para valorar el MD.	i) Escrito, la información contenida este accesible para posterior consulta.	Artículo 6, Ley 527 de 1999.
	ii) Firma, se utilizó método para identificar al iniciador de la información y que sea aprobada por él.	Artículo 7, Ley 527 de 1999.
	iii) Original, existe garantía confiable de integridad y que pueda ser mostrado el MD al suscriptor.	Artículo 8, Ley 527 de 1999.
	iv) Integridad, si el MD ha permanecido completo e inalterado acorde al fin del MD.	Artículo 9, Ley 527 de 1999.

Fuente: Elaboración propia.

Tabla 9. Criterio para valorar probatoriamente un MD

TEMA: Criterio para valorar probatoriamente un MD		
DEFINICIÓN: Para la valoración del MD que determine si tiene vocación probatoria, se delimita a través de criterios la interpretación consecuente.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Cuando se presenta un MD no se repara en establecer una delimitación en cuanto a su interpretación para determinar si debe considerarse o no como prueba.	Que *"Debe tenerse en cuenta la confiabilidad en la forma en la que se haya generado, archivado y comunicado el mensaje, la confiabilidad en la forma en que se identifique su iniciador y cualquier otro factor pertinente".*[9]	Artículo 11, Ley 527 de 1999. Corte Suprema de Justicia (Sala de Casación Civil) RAD. 11001 3110 005 2004 01074 01. del 16 de diciembre de 2010

Fuente: Elaboración propia.

9 Romelio, Daza Molina. Las TIC Ante el Derecho Colombiano y la Gestión Judicial. Bogotá D.C. : Libreria Ediciones del Profesional L.T.D.A. , 2017. (4 pág. 225)

Tabla 10. Conservación de los MD

TEMA: Conservación de los Mensajes de Datos MD		
DEFINICIÓN: Aplica en aquellos casos en que la norma expresa la necesidad de conservación de los MD por sí mismo o a través de terceros.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? Si toca conservar se deben cumplir estos requisitos	¿Qué norma aplica?
Cuando se presenta un MD no se repara en establecer una delimitación en cuanto a su interpretación para determinar si debe considerarse o no como prueba.	i) Disponibilidad del MD para posterior consulta.	¿Qué norma aplica? Artículo 12, Ley 527 de 1999. Artículo 13, Ley 527 de 1999.
	ii) Conservación del MD en el formato original y que permita demostrar reproducción exacta.	
	iii) Se acompañe y conserve información que permita determinar del MD: origen, destino, fecha y hora en que fue enviado.	

Fuente: Elaboración propia.

Tabla 11. Formación y validez de contratos suscritos a través de MD

TEMA: Formación y validez de contratos suscritos a través de MD		
DEFINICIÓN: Aplica en aquellos casos en que partes interesadas desean crear y validar un contrato específico.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Se cree que la única manera en que se puede suscribir y validar un contrato es por la forma tradicional de uso de papel y firma y presencia física de las partes, lo cual no es viable en un modelo de globalización.	Salvo pacto en contrario, las partes pueden acordar que la formación, oferta y aceptación podrán ser expresadas a través de MD.	Artículo 14, Ley 527 de 1999.

Fuente: Elaboración propia.

Tabla 12. Reconocimiento de los MD por las partes

TEMA: Reconocimiento de los MD por las partes		
DEFINICIÓN: Refiere a una aceptación entre el iniciador y el destinatario de un MD.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? Se entenderá que MD proviene de iniciador cuando:	¿Qué norma aplica?
El imaginario colectivo considera que sólo a través de medios físicos se tendrá certeza jurídica para obligarse y obligar con base en los acuerdos particulares de voluntades.	i) Haya sido enviado por el propio iniciador.	Artículo 15, Ley 527 de 1999.
	ii) Haya sido enviado por una persona facultada por el iniciador.	
	iii) Un sistema de información programado por el iniciador o en su nombre opera automáticamente.	

Fuente: Elaboración propia.

Tabla 13. Presunción del origen de MD

TEMA: Presunción del origen de un MD		
DEFINICIÓN: Origen se refiere al dato preciso que demuestra que el MD fue enviado por el iniciador.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? Se aplica la presunción siempre y cuando:	¿Qué norma aplica?
La carga de la prueba para tachar de falso le corresponde al demandado, lo cual implica una oportunidad procesal de contradicción ante la administración de la justicia para el destinatario y una economía procesal para el Estado.	i) El iniciador haya aplicado el procedimiento acordado con la otra parte para establecer que el MD proviene de él.	Artículo 17, Ley 527 de 1999.
	ii) El MD tenga relación con los actos entre las partes y le hayan dado acceso para identificar el MD como propio.	

Fuente: Elaboración propia.

Tabla 14. Concordancia del MD enviado con el MD recibido

TEMA: Concordancia del MD enviado con el MD recibido		
DEFINICIÓN: En principio el destinatario tiene el derecho a recibir de buena fe el MD por parte del iniciador, pero para eximirse de responsabilidad si actúa con debida diligencia.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
No existe una presunción de concordancia o no existe una voluntad para esclarecer si en verdad hay concordancia con el MD.	*"El destinatario "tendrá derecho a considerar que el MD recibido corresponde al que quería enviar el iniciador y podrá proceder en consecuencia"* [10]	Artículo 18, Ley 527 de 1999.

Fuente: Elaboración propia.

Tabla 15. Duplicados MD

TEMA: MD duplicados		
DEFINICIÓN: Presunción de valora cada MD recibido como diferente de los demás MD, lo cual implica que los duplicados se consideren una excepción.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Las copias son entendidas como el propio MD	Téngase en cuenta que: *"Salvo en la medida en que duplique otro MD, y que el destinatario sepa, o debiera saber, de haber actuado con la debida diligencia o de haber aplicado un método convenido, que el nuevo MD era un duplicado"* [11]	Artículo 19, Ley 527 de 1999.

Fuente: Elaboración propia.

10 Ibidem [4 pág. 225]
11 Ibidem [4 pág. 225]

Tabla 16. Acuse recibido de un MD

TEMA: Acuse recibido de un MD		
DEFINICIÓN: Ante la solicitud del iniciador de acusar recibido por parte del destinatario, sin que se haya acordado contractualmente un método.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? Se puede acusar recibido mediante:	¿Qué norma aplica?
Que se presume erróneamente que al enviar un MD este llegará sin problema alguno al destinatario. Pero no se sabe la importancia de términos y pruebas que implica el demostrar que sí recibió el MD.	i) Toda comunicación del destinatario, automatizada o no.	Artículo 20, Ley 527 de 1999.
	ii) Todo acto del destinatario que baste para indicar que recibió MD.	

Fuente: Elaboración propia.

Tabla 17. Presunción de recepción de un MD

TEMA: Presunción de recepción de un MD		
DEFINICIÓN: En principio, aplica esta presunción en el momento en que el iniciador recepcione y acuse recibo del destinatario.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Que, mediante el acuse recibido sin detallar el contenido del MD, se cree que hay aceptación de dicha información contenida en el MD.	Que *"la recepción de acuse recibido no implica certeza de que MD corresponda al MD recibido"* [12]	Artículo 21, Ley 527 de 1999.

Fuente: Elaboración propia.

12 Ibidem (4 pág. 225)

Tabla 18. Efectos Jurídicos del MD

TEMA: Efectos jurídicos del MD		
DEFINICIÓN: La fuente de derecho que aplica al caso en concreto de un MD será determinado por el tema de información contenida en el MD.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Mediante el acuse recibido sin detallar el contenido del MD, se cree que hay aceptación de dicha información contenida en el MD	*"Las consecuencias jurídicas del MD se regirá conforme a las normas aplicables al acto o negocio contenido en dicho MD"* [13]	Artículo 22, Ley 527 de 1999.

Fuente: Elaboración propia.

Tabla 19. Tiempo de envío de un MD

TEMA: Tiempo de envío de un MD		
DEFINICIÓN: Se refiere al criterio de interpretación que permite identificar la fecha en la que se expidió el MD para efectos jurídicos.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
La importancia de determinar el dato preciso sobre la fecha de expedición del MD radica en los términos que corren para traslado.	*"Se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el MD en nombre de este"* [14]	Artículo 23, Ley 527 de 1999.

Fuente: Elaboración propia.

13 Ibidem [4 pág. 225]
14 Ibidem [4 pág. 225]

Tabla 20. Tiempo de Recepción de un MD

TEMA: Tiempo de la recepción de un MD		
DEFINICIÓN: Se refiere al criterio de interpretación que permite identificar la fecha en la que se recibió el MD para efectos jurídicos.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? el momento de recepción de MD se determina:	¿Qué norma aplica?
La importancia de establecer un momento preciso de acuse de recibo del MD radica en la aplicación de las reglas de notificaciones que establece el artículo 291 y 292 del C.G.P.	i) *"Si es a través de un sistema de información:- en el momento en que ingrese el MD en el sistema de información,-si se envió a un sistema de información no designado por las partes, cuando recupere el MD."*[15]	Artículo 24, Ley 527 de 1999.
	ii) No a través de sistema de información, cuando el MD ingrese a un sistema de información del destinatario.	

Fuente: Elaboración propia.

Tabla 21. Lugar de envío y recepción de MD

TEMA: Lugar de envío y recepción del MD		
DEFINICIÓN: Se refiere al criterio de interpretación que permite identificar el lugar de envío y lugar de recepción del MD para efectos jurídicos.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
Que la importancia de tener certeza en cuanto al lugar de envío y recepción del MD radica en que, en algunos casos concretos, es determinante para establecer, jurisdicción, competencia, certeza probatoria de notificación efectiva de las partes intervinientes y debido proceso.	REGLA GENERAL: El lugar de envío: es el domicilio del iniciador, y lugar de recibido: es el domicilio del destinatario. Si una parte o ambas, tiene más de un establecimiento será el lugar más cercano. Si una parte o ambas no tiene establecimiento el lugar será la residencia donde habita.	Artículo 25, Ley 527 de 1999.

Fuente: Elaboración propia.

15 Ibidem (4 pág. 225)

Tabla 22. Recepción de los actos de comunicación procesal y de los MD

TEMA: Recepción de los actos de comunicación procesal y de los mensajes de datos		
DEFINICIÓN: Aplica para usuarios y autoridad judicial y refiere a los actos de comunicación procesal y cuando se entiende recibidos los MD.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto?	¿Qué norma aplica?
El acuse recibido se hacía manualmente con una descripción de la firma de quien recibe, la fecha y en número de folios que contiene el recibido.	Que se tenga en cuenta el momento en que se genera en el sistema de información de la autoridad judicial el acuse de recibo junto con la radicación consecutiva propia de cada despacho.	Artículo 10, ACUERDO No. PSAA06-3334 de 2006

Fuente: Elaboración propia.

Tabla 23. Recepción de los actos de comunicación procesal y de los MD por parte de autoridades procesales

TEMA: Recepción de los actos de comunicación procesal y de los mensajes de datos por parte de autoridades judiciales		
DEFINICIÓN: Aplica para autoridad judicial y refiere a las reglas de la recepción de MD.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? Siga estas reglas para recepción de MD	¿Qué norma aplica?
La autoridad judicial escoge, acorde a su propia experiencia en la materia, su propio medio y protocolo de recepción de MD	i) Si el originador del MD remitido a autoridad judicial advierte en la transmisión un error deberá avisar inmediatamente a autoridad judicial.	Artículo 11, ACUERDO No. PSAA06-3334 de 2006
	ii) La autoridad judicial deberá llevar estricto control y relación de MD recibidos a través de su sistema de información. So pena de reconocerse falta disciplinaria.	
	iii) La autoridad judicial deberá procurar mantener la casilla de correo electrónico de tal manera que no se llene o bloquee su uso y proteger información contenida.	

Fuente: Elaboración propia.

Tabla 24. Prueba de la Recepción de los actos de comunicación procesal emitidos por autoridad judicial

TEMA: Prueba de la recepción de los actos de comunicación procesal emitidos por autoridad judicial		
DEFINICIÓN: Aplica para efectos de demostrar la recepción de los actos de comunicación procesal.		
¿Qué sucede en la práctica?	¿Qué sugiere el experto? tenga loen cuenta:	¿Qué norma aplica?
El usuario debía tener presente y disponer del medio de acuse recibido escogido por la autoridad judicial como protocolo de recepción de MD	i) Será prueba de recepción del MD, el acuse recibido junto con la radicación consecutiva generadas por el sistema de información.	Artículo 12, ACUERDO No. PSAA06-3334 de 2006
	ii) Frente a la diferencia entre el contenido del acuse de recibo aportado por el destinatario del MD y los datos generados por el sistema de información de autoridad judicial, prevalece el segundo.	
	iii) Si el sistema de información de autoridad judicial rechaza el MD, el originador deberá comunicar mediante documento físico e informar del rechazo digital dentro del día hábil siguiente de ocurrido el rechazo.	
	iv) La autoridad judicial que reciba un MD, deberá hacer una impresión en papel de este para incorporarlo al expediente judicial.	

Fuente: Elaboración propia.

9.5. EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA EN EL DERECHO COLOMBIANO

Ante la inminente y disruptiva transformación digital mundial, Colombia expide en el año de 1999 la Ley 527 que propone regular el comercio electrónico y reconoce el posible valor probatorio de un mensaje de datos en cualquier proceso judicial, dada la vocación que tiene de probar un hecho, acto o contrato relevante judicialmente.

Desde la entrada en vigencia de la norma precitada, se dispuso en su artículo 95 la incorporación de recursos tecnológicos avanzados para la administración de justicia en lo relativo a mejorar la práctica de pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información; lo anterior demuestra la importancia que le concede el Consejo Superior de la Judicatura a la tecnología dado que permite en su implementación, facilitar a los jueces el ejercicio de las facultades otorgadas por la citada norma en el nuevo contexto de la sociedad del conocimiento, a saber:

"ARTÍCULO 95. TECNOLOGÍA AL SERVICIO DE LA ADMINISTRACIÓN DE JUSTICIA. El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información.

Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones. Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad, y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley." [16]

Asimismo, la norma precitada estableció criterios de reconocimiento y validez probatoria a los mensajes de datos a través de remisiones a normas especiales (en esa época el derogado Código de Procedimiento Civil), a saber:

"ARTÍCULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil.
En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o debido a no haber sido presentado en su forma original.

ARTÍCULO 11. CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente." [17]

16 Colombia. Ley 527 de 1999 Comercio Electrónico. Colombia : Colombia, 1999. 2. (5 pág. 2)
17 Colombia. Ley 527 de 1999 Comercio Electrónico. Colombia: Colombia, 1999. 2. (5 pág. 2)

En el DERECHO PENAL Ley 906 de 2004 incorporó en el marco procesal penal una categoría específica para la denominada evidencia digital, al momento de establecer una serie de elementos materiales probatorios que son válidos en el proceso penal, específicamente define en el literal g del artículo 275 como una de las formas de evidencia, el mensaje de datos, en esta competencia, entendida como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen.

Así mismo, la doctrina especializada establece un marco específico para la implementación de medios tecnológicos en el caso concreto de las interceptaciones penales, de la siguiente manera:

"la legalidad de la prueba en el caso de mensajes de datos está asociada a la interceptación de las comunicaciones el cumplimiento de las competencias reguladas de la Fiscalía General de la Nación.

La interceptación, cualquiera que sea su origen o tecnología, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la ley.

Los proveedores de redes y servicios de telecomunicaciones que desarrollen su actividad comercial en Colombia deben:

a) Implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que corren por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación o su delegado, con todas aquellas labores tendentes a la interceptación de las comunicaciones requeridas;

b) Atender oportunamente los requerimientos de interceptación de comunicaciones que efectúe el fiscal general de la nación, para facilitar la labor de interceptación de los organismos permanentes de policía judicial;

c) Suministrar a la fiscalía general de la nación o demás autoridades competentes, a través del grupo de policía judicial designado para la investigación del caso, los datos del suscriptor, tales como identidad, dirección de facturación y tipo de conexión, y

d) Suministrar a la fiscalía general de la nación, a través de los organismos con funciones permanentes de policía judicial, la información específica contenida en sus bases de datos, tal como sectores, coordenadas geográficas y potencia, entre otras, que contribuye a determinar la ubicación geográfica de los equipos terminales o dispositivos que intervienen en la comunicación" [18]

18 Peña, Daniel. De la Firma Manuscrita a las Firmas Electrónicas y Digital. Bogotá D.C.: Universidad Externado de Colombia, 2015 (4 pág. 80)

9.6. PRINCIPIOS FORENSE DIGITAL

Todos los procesos asociados a la evidencia digital en la medida en que busque promover un elevado índice de confiabilidad probatoria deben ostentar los siguientes principios, a saber:

9.6.1. Confidencialidad

Este principio responde a la necesidad de que ningún tercero, que no esté autorizado, tenga acceso a la evidencia o al material probatorio de carácter informático. En otras palabras, se debe impedir que personas no autorizadas accedan y/o manipulen y/o divulguen la información que se quiere proteger y reconocer como evidencia digital a presentar en el ámbito judicial.

9.6.2. Disponibilidad

Este principio se refiere precisamente a que el material probatorio deberá estar siempre a disposición de cada una de las partes cuando requieran adquirir o acceder a él en las etapas procesales relacionadas.

9.6.3. Integridad

Este principio hace alusión a la condición que debe tener la evidencia digital respecto a que no se puede alterar de ninguna manera la información o los datos contenidos por el material probatorio; por lo anterior se concluye que se debe garantizar que los documentos electrónicos con vocación probatoria no sean alterados, modificados, falsificados o manipulados.

9.6.4. No Repudio

Este principio propone una certeza jurídica de que la evidencia digital es un medio válido para demostrar plena voluntad de los intervinientes en las tareas relacionadas, por ende, tiene un alcance en cuanto a: la identificación, preservación, recolección, análisis y la presentación de resultados.

9.7. PRINCIPIOS FORENSES DE LA INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE

Este instrumento internacional define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

Tabla 25. Pasos forenses de la International Organization on computer evidence

PASO	ACTIVIDAD	RECOMENDACIÓN
1	Sobre recolectar	Las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2	Sobre el acceso	Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
3	Sobre recolección, el acceso, almacenamiento o a la transferencia	Toda la actividad debe ser documentada completamente, preservada y disponible para la revisión.
4	Sobre la responsabilidad	Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
5	Sobre responsabilidad Estatal	Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Fuente: Elaboración propia.

9.8. ATRIBUTOS DE RECUPERACIÓN ESTANDARIZADA DE EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

Además de los principios anteriormente señalados, existe una serie de definiciones detalladas de los principios desarrollados para la recuperación estandarizada de evidencia computarizada se deben gobernar por los siguientes:

Tabla 26. Atributos de Recuperación Estandarizada de EDiPE

PASO	PRINCIPIO
1	Consistencia con todos los sistemas legales. Refiere a que la evidencia debe ser obtenida conforme a las leyes vigentes que regulan la materia.
2	Permitir el uso de un lenguaje común. Refiere a una exposición clara y sucinta que sea fácil entendimiento para las partes intervinientes en un proceso, independientemente de la técnica o complejidad del tema que se aborda.
3	Durabilidad. Refiere a la disponibilidad y acceso para las partes procesales interesadas en todo momento que se requiera. En algunos países se han definido los tiempos límites por los cuales se debe preservar dicho material con miras a garantizar el derecho fundamental a la contradicción y defensa.

PASO	PRINCIPIO
4	Capacidad de cruzar límites internacionales. Hace referencia al principio de universalidad que determina un adecuado procesamiento de la evidencia digital a tal punto que pueda ser reconocida en cualquier ordenamiento jurídico internacional.
5	Capacidad de ofrecer confianza en la integridad de la evidencia. Hace referencia a la garantía de inalterabilidad que debe ostentar la evidencia en aras de evitar una alteración, modificación o cambio del material.
6	Aplicabilidad a toda la evidencia forense. Refiere a que los parámetros de manejo debido de la Evidencia Digital.

Fuente: Elaboración propia.

9.9. APLICACIÓN TEÓRICA DE ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

Acorde a la necesidad de cumplir a cabalidad los principios y atributos que gobiernan la evidencia digital, se establece unos lineamientos que dan alcance a la actividad de informática forense para alcanzar este noble propósito.

Cuando hablamos de confidencialidad claramente la cadena de custodia garantiza la identificación de quienes tienen contacto con la evidencia, ello supone que quien no esté autorizado no pueda tener acceso a los datos almacenados o a la información; en el caso de las bodegas de evidencia y el control que se haga por el custodio del material probatorio vienen posteriormente a facilitar la condición de confidencialidad que demanda la informática forense.

Respecto a la disponibilidad el procedimiento de imagen forense facilita que en el momento en que no se pueda retener o incautar un elemento probatorio digital en su estado original, por ejemplo, un servidor de una entidad bancaria, la imagen forense de los logs de las transacciones sujeto de investigación, siempre estarán disponibles sin que haya sido alterados porque la imagen forense resulta ser la copia exacta bit a bit de la información objeto de la investigación o sujeta de evidencia.

La disponibilidad entonces es el principio en informática forense que garantiza que el elemento material probatorio va a estar al alcance de las partes intervinientes, para cuando se requiera una posterior consulta.

Finalmente, la integridad se basa también en la aplicación del valor hash, que es un algoritmo matemático que arroja un valor en letras y números único irrepetible vinculados directamente a un archivo a un dispositivo o a los datos en general, con el fin de dotarlo de un metadato de originalidad.

9.10. CLASES DE EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

La guía para la administración de evidencia TI, conocida como el HB:171 2003, o Guidelines for the management of IT Evidence. En este sentido el documento mencionado, establece que la evidencia digital puede ser dividida en tres categorías:

9.10.1. Registros almacenados en el equipo de tecnología informática

Refiere a mensajes de datos almacenados en dispositivos tecnológicos y lógicos.

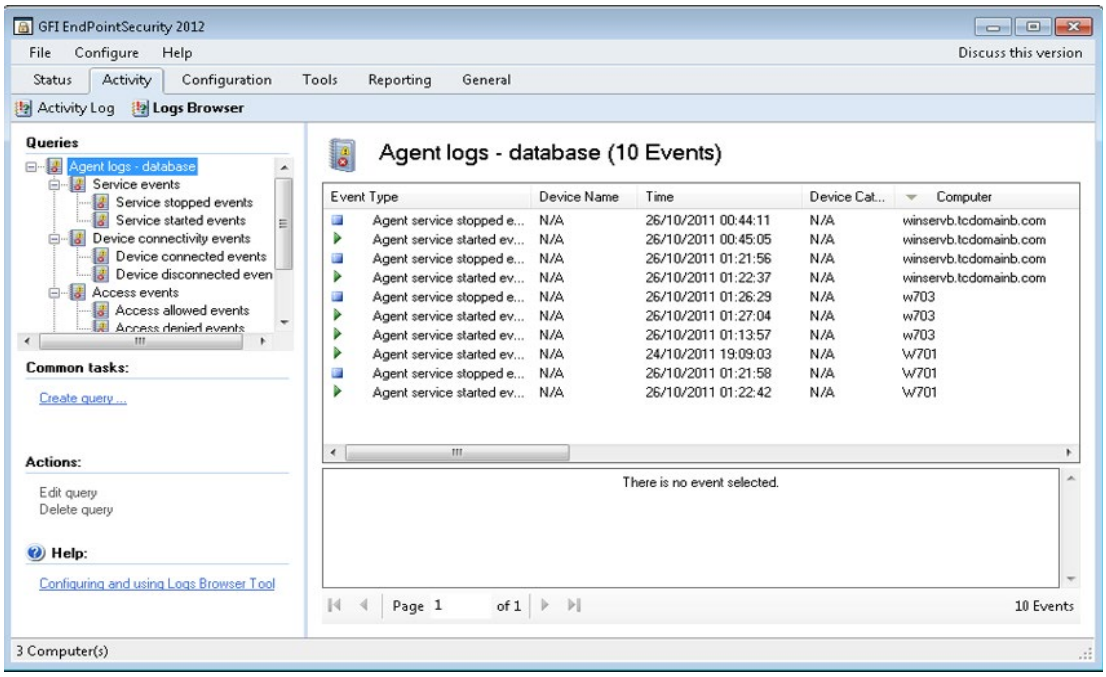
Ilustración 3. Logos registros almacenados en equipos de tecnología informática

Fuente: Microsoft 2019

9.10.2. Registros generados por los equipos de tecnología informática

Refiere a registros de auditoría, registros de transacciones, registros de eventos, etc.

Ilustración 4. Ejemplo registro generado GFI END POINT SECURITY 2012



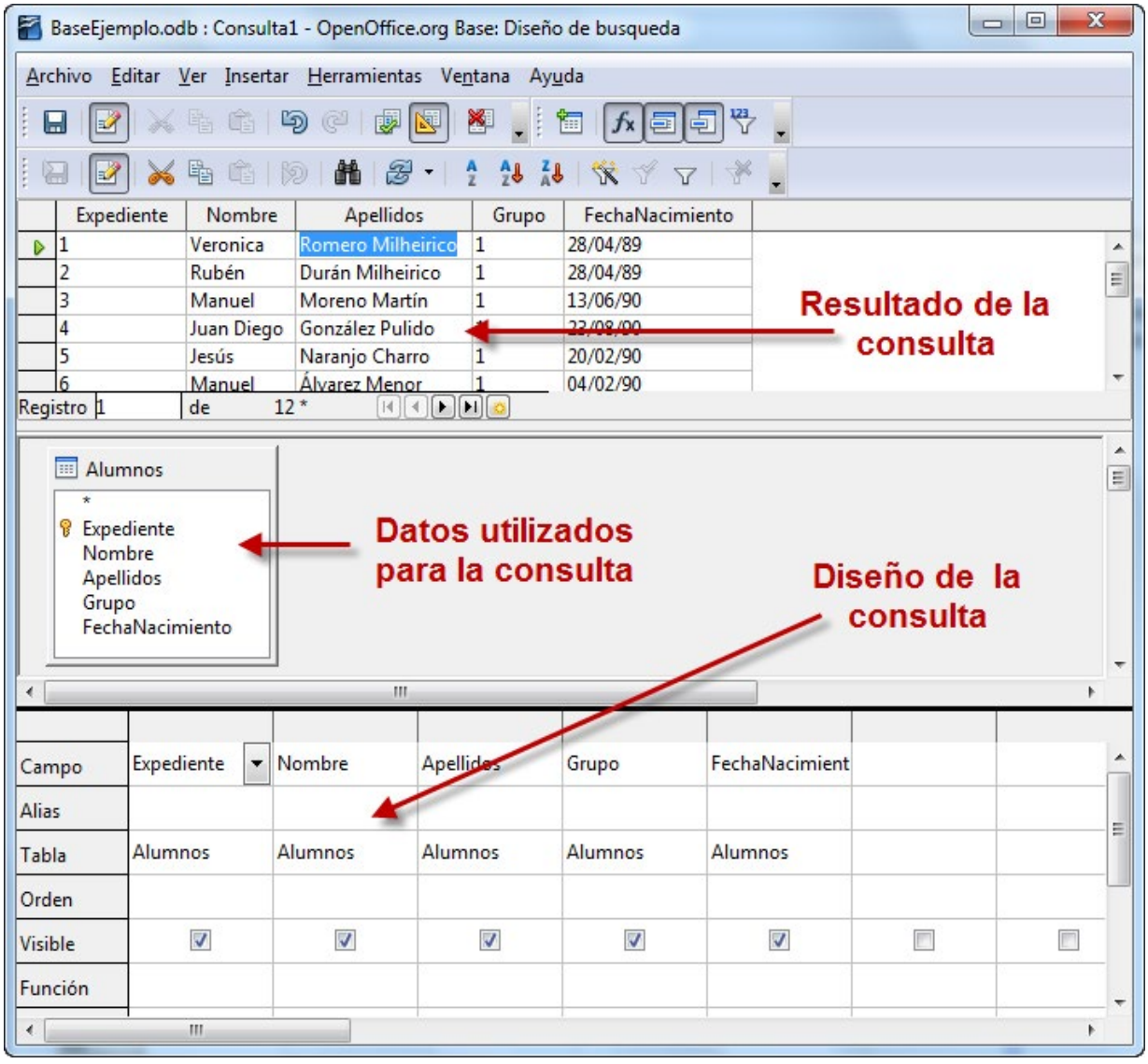
Fuente: software GFI END POINT SECURITY 2012 [19]

19 GFI. END POINT SECURITY. 2012. (6)

9.10.3. Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática

Refiere a hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc.

Ilustración 5. base ejemplo openoffice.org



9.11. CARACTERÍSTICAS TÉCNICAS DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

La evidencia digital tiene unas características especiales que la diferencian de la evidencia tradicional, la comunidad técnica ha identificado al menos cinco características que deben ser tenidas en cuenta para su adecuado tratamiento, estas son:

9.11.1. Volátil

La volatilidad se refiere a la posibilidad de que la evidencia desaparezca o se pierda si no se recolecta de manera oportuna, el RFC 3227 establece al respecto un orden de volatilidad situando en primer lugar la evidencia digital contenida en la memoria RAM de los equipos de cómputo y la cual almacena información relacionada con los procesos que se ejecutan en un sistema cuando este está encendido, de tal manera que si el sistema se apaga se puede perder valiosa información útil para el esclarecimiento o claridad de los hechos objeto de controversia. (Procesos, documentos, contraseñas, sitios web visitados, entre otros).

9.11.2. Eliminable

Esta condición muy vinculada a la anterior característica técnica y señala que la evidencia digital puede ser eliminada por una acción voluntaria o involuntaria de quien la accede, manipula o custodia.

La evidencia digital al estar almacenada en un soporte digital y ser generada a través de pulsos electromagnéticos puede eliminarse por una acción deliberada de descargas no deseadas de energía o acción de ondas producidas por un elemento altamente conductor o transmisor de ondas, señales o pulsos que tienen la capacidad de eliminar la originalidad de la evidencia.

Igualmente, un transporte inadecuado puede generar daños físicos a los dispositivos de almacenamiento, lo que sin duda puede ocasionar que la evidencia se elimine o se pierda definitivamente.

9.11.3. Duplicable

A través de procedimientos forenses el especialista puede generar duplicados de la evidencia digital, los cuales mediante un riguroso registro de cadena de custodia pueden garantizar la continuidad del debido cuidado de esta, su integridad, confidencialidad y disponibilidad. Los duplicados de imagen forense, por ejemplo, ayudan al especialista forense a dividir objetivos específicos con miras a determinar un hecho o acto particular jurídicamente relevante.

Sin el duplicado la labor forense podría ser dispendiosa y afectar los tiempos de respuesta que requiere para su cabal cumplimiento de objetivos trazados. Otra perspectiva de la duplicidad de la evidencia digital la encontramos en la posibilidad de que la interacción de una o más personas a través de un medio informático se almacene de manera simultánea en diferentes repositorios susceptibles en todo caso de ser recolectados y aportados como evidencia digital, como ejemplo, existe la posibilidad de disponer de evidencia almacenada localmente en un dispositivo y paralelamente tener un duplicado en la nube disponible para consulta.

9.11.4. Anónima

La condición de anonimato de la evidencia es una de las características más exigentes en la labor de un especialista forense y por tanto del operador judicial al momento de validar la autenticidad, debido a la difícil tarea de vincular mediante un nexo causal directo a la evidencia digital con el sujeto relacionado con miras a adjudicar una responsabilidad objetiva.

Ejemplo de lo anterior, podemos encontrarlo en suplantaciones de perfiles de redes sociales, sin que necesariamente el autor de esta suplantación sea el titular de la red, por ello se hace necesario vincular el actuar de suplantación a una persona determinada.

9.11.5. Alterable y modificable

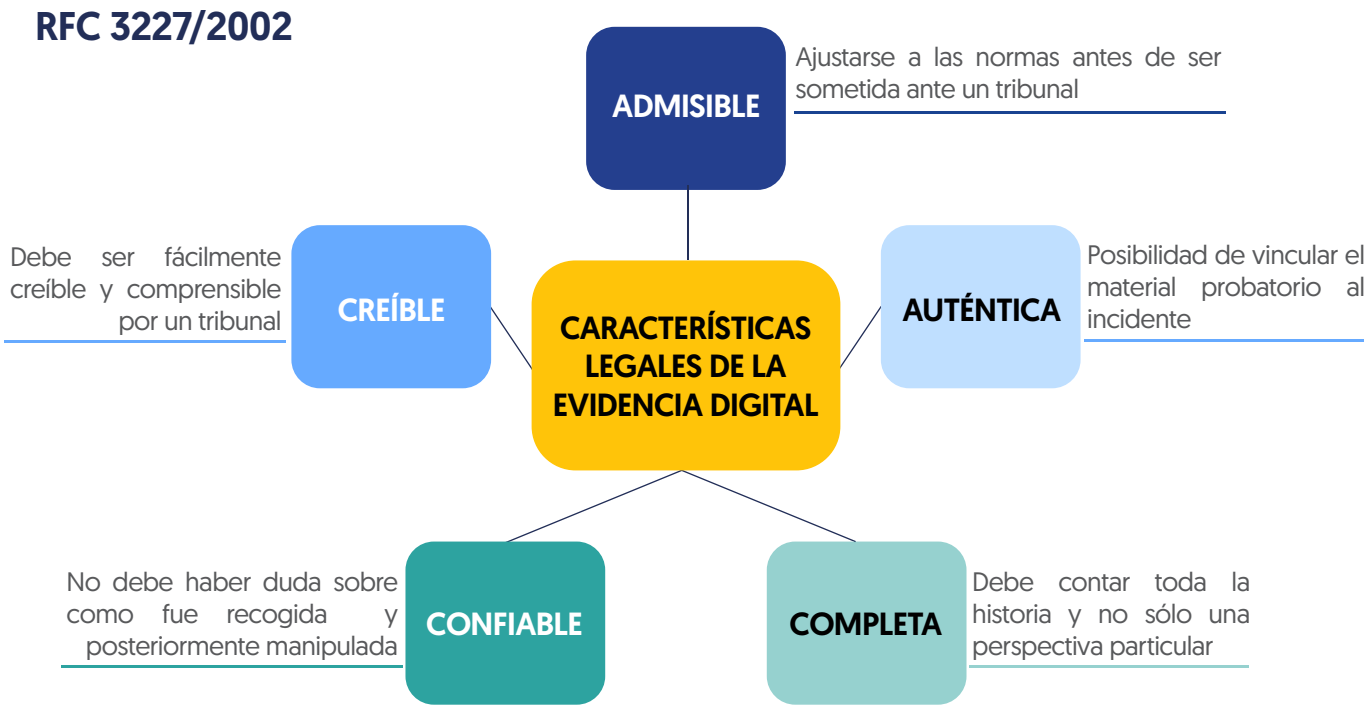
Dadas sus características técnicas, la evidencia digital puede ser objeto de manipulaciones por parte de terceros si no se respeta el debido cuidado expuesto en el principio de confidencialidad, no obstante, la comunidad técnico científica ha desarrollado procedimientos para validar la integridad e inmodificabilidad de la evidencia al asignarle un valor único alfanumérico que garantiza una identificación que debe permanecer durante el transcurso de la actuación procesal como certeza de que se ha cumplido a cabalidad este propósito.

Más adelante trataremos en el capítulo de técnicas antiforenses algunos aspectos externos para tener en cuenta para evitar que se afecte esta característica técnica.

9.12. CARACTERÍSTICAS LEGALES DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

Teniendo en cuenta que la relevancia del estudio detallado de la evidencia digital está encaminada en la obtención de un reconocimiento pleno de este material como prueba válida dentro de un ordenamiento jurídico específico, se hace necesario identificar una serie de consideraciones de tipo legal que permite identificar una serie de requisitos para tener en cuenta. Acorde a lo anterior la Admisibilidad de la Evidencia está supeditada a las siguientes características, a saber:

Ilustración 6. RFC 3227/ 2002



FUENTE: Coronel (Reserva Activa) Fredy Bautista. 2019. Editada por @CyberAbogado

9.12.1. Autenticidad

La evidencia digital requiere confirmar, para obtener un grado elevado de certeza, que contiene lo que la realidad propone que sea, para efectos de vocación probatoria.

Al respecto, la autenticidad está llamada a fortalecer la admisibilidad y la relevancia de la prueba en la medida en que quede registrado, en este caso electrónicamente, los elementos que permiten validar la confirmación de que lo contenido es lo verdadero reflejado de la realidad.

9.12.2. Confiabilidad

Refiere al grado de certeza que tienen las partes para constatar el cabal cumplimiento de los requisitos necesarios para considerar y presentar ante el sistema información. La confidencialidad se refiere igualmente a esa característica legal que disminuye el temor o incertidumbre sobre la manipulación no autorizada de la evidencia que se aporta. Algunos ejemplos claros de procedimientos asociados a la confiabilidad son los siguientes:

9.12.2.1. El dispositivo de almacenamiento de destino debe estar debidamente sanitizado para evitar contaminaciones de la evidencia.

9.12.2.2. Es sistema operativo del equipo utilizado para la recolección, así como las herramientas utilizadas para este procedimiento deben estar legalmente registradas, autorizadas o reconocidas por la comunidad científica internacional.

9.12.3. Completitud o Suficiencia

La evidencia debe tener como atributo que la misma se refiere a la presencia de toda la información necesaria para adelantar el caso.

El desarrollo de esta característica implica tener una visión Para asegurar esto es necesario "contar con mecanismos que proporcionen integridad, sincronización y centralización" para lograr tener una vista completa de la situación. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos, la cual puede ser manual o sistematizada.

9.12.4. Conformidad con las leyes y regulaciones de la administración de justicia

Esta característica se refiere a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien es cierto que el ordenamiento jurídico de Colombia dispone diversas directrices que establecen la manera de aportar una prueba a un proceso, en el campo internacional existen iniciativas como las de la IOCE, el Digital Forensic Research Workshop, donde se formulan marcos de acción y lineamientos que cobijan la evidencia en medios electrónicos. Por lo anterior es dable concluir que la Evidencia Digital debe ser recolectada de acuerdo con el marco normativo vigente.

9.12.5. Licitud e ilicitud de la evidencia digital

Al respecto, se hace propicio señalar, el instrumento internacional denominado Guidelines for Evidence Collection and Archiving, en virtud del cual se establece las siguientes condiciones que debe cumplir la evidencia digital:

- Relevante Que la evidencia digital está relacionada con el crimen bajo investigación

- Permitida Legalmente: Que la evidencia digital fue obtenida de manera legal.

- Confiable: Que la evidencia digital no ha sido alterada o modificada.

• Identificada: Que la evidencia digital ha sido claramente etiquetada.

• Preservada: Que la evidencia digital no ha sido dañada o destruida.

9.13. CICLO DE VIDA DE LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

Hace referencia a la serie de pasos que se deben surtir para abordar integralmente una evidencia digital de tal suerte que se cumpla a cabalidad los presupuestos técnicos formulados por los mejores estándares internacionales, especialmente HB 171 Handbook guidelines for the management of IT evidencie 2003, a saber:

9.13.1. Diseño de la evidencia

Teniendo en cuenta que la admisibilidad y relevancia de la prueba digital radica en buenas prácticas relacionadas con su proyección de la evidencia y su objetivo central de tener validez jurídica, la guía internacional de Standards Australia International 2003 establece cinco objetivos para tener en cuenta para el diseño, a saber:

"11.1.1. Asegurarse que se ha determinado la relevancia de los registros electrónicos, que estos se han identificado, están disponibles y son utilizables,
11.1.2. Los registros electrónicos tienen un autor claramente identificado,
11.3. Los registros electrónicos cuentan con una fecha y hora de la creación o alteración,
11.4. Los registros electrónicos cuentan con elementos que permiten validar su autenticidad.
11.5. Se debe verificar la confiabilidad de la producción o la generación de los registros electrónicos por parte del sistema de información."
Acorde a estos objetivos existen algunas prácticas asociadas que permiten dar certeza de cabal cumplimiento, entre estas tenemos:
i) "Clasificar la información de la organización con un criterio de relevancia en el orden (mayor prioridad a mayor relevancia)
ii) Determinar los tiempos de retención de documentos electrónicos, la transformación de estos y la disposición final
iii) Diseñar los registros de auditoría de las aplicaciones, como parte fundamental de la fase de diseño de la aplicación
iv) Utilización de modelos tecnológicos de seguridad informática para validar la autenticidad y la integridad de los registros electrónicos." [20]

9.13.2. Producción de la evidencia

"En cuanto a la conformación de la evidencia que se propone hacer valer judicialmente, se establece una serie de pasos que permite guiar hacia el cabal cumplimiento de este objetivo, entre otros:

20 M., Jeimy J. Cano. Computación Forense Descubriendo los rastros informáticos. Bogotá D.C. : Alfaomega, 2015. (7 pág. ED)

11.2.1. Que el sistema o la tecnología de información produzca los registros electrónicos,
11.2.1. Identificar el autor de los registros electrónicos almacenados,
11.2.3. Identificar la fecha y hora de creación,
11.2.4. Verificar que la aplicación está operando correctamente en el momento de generación de los registros, bien sea en su creación o modificación,
11.2.5. Verificar la completitud de los registros generados"

Para aterrizar estos objetivos al ejercicio práctico forense digital, se evidencia, gracias a la doctrina especializada, tenemos:

"i) Desarrollar y documentar un plan de pruebas formal para validar la correcta generación de los registros de la aplicación
ii) diseñar mecanismos de seguridad basados en certificados digitales para las aplicaciones, de tal forma que se pueda validar que es la aplicación la que genera los registros electrónicos
iii) En la medida de lo posible, establecer un servidor de tiempo contra el cual se pueda verificar la fecha y la hora de la creación de los archivos,
iv) Contar con pruebas y auditorías frecuentes alrededor de la confiabilidad de los registros y su completitud, frente al diseño previo de los registros electrónicos.
v) Diseñar y mantener un control de integridad de los registros electrónicos, que permita identificar los cambios que se hayan presentado en ellos"[21]

9.13.3. Recolección de la evidencia

Este objetivo propone localizar toda evidencia digital de tal manera que se pueda garantizar una certeza en cuanto a la ubicación dado que lo ideal es demostrar que no ha habido ningún tipo de alteración en su aprehensión con miras a cumplir este objetivo.

9.13.4. Análisis de la evidencia

El análisis de la evidencia se refiere al ejercicio juicioso del especialista o perito en informática, quien observando todos los protocolos establecidos para tal fin, accede al repositorio de la evidencia digital y la ausculta con herramientas forenses que le permiten según el objeto del análisis, entre otros aspectos; recuperar información eliminada, encontrar archivos de interés para la investigación, determinar usuario(s) que ha(n) tenido acceso a la evidencia, enumerar los archivos disponibles susceptibles de exportar y plasmar en el informe final, identificar los metadatos de la información entre otros aspectos.

21 Ibidem (7 pág. ED)

9.13.5. Reporte y Presentación

Los informes y reportes del perito deben contener la información que resulte relevante para la investigación y ajustarse a los requisitos legales establecidos para la presentación de un informe de peritaje. En todo caso debe conservar características de sencillez y fácil entendimiento para el operador judicial.

9.14. AUDITABILIDAD Y TRAZABILIDAD DE LA EVIDENCIA DIGITAL Y PRUEBA ELECTRÓNICA

9.14.1. Auditabilidad

Aquella propiedad de todo sistema o tecnología de información utilizada para conservar el registro detallado de todas las actividades y eventos sucedidos en torno a al sistema que genera la evidencia o a la evidencia en sí misma, pese a que se trata de un registro con fines de mantener el historial de interacciones con el sistema, cuando hablamos de evidencia digital un log de eventos se constituye en una importante fuente de información para posteriores cotejos o auditorías.

La auditabilidad permite por ejemplo conocer si una alteración de un dato pudo ser ocasionada por un agente externo y no por el autor conocido, usuario del dato, o responsable del sistema a auditar. Igualmente permite conocer el estado de cumplimiento del principio de confidencialidad pues ayuda a determinar si un externo ha manipulado, accedido o consultado el mensaje de datos sin estar autorizado. (Cano 2003)

En términos generales podríamos decir que los logs se convierten en herramienta fundamental para determinar posibles eventos externos que puedan afectar la integridad de la evidencia.

9.14.2. Trazabilidad

Evidencia digital está muy vinculada al registro de cadena de custodia que trataremos más adelante en detalle, pero se refiere a aquella condición técnica que permite rastrear, construir o establecer qué ha sucedido con la evidencia digital desde el momento de su identificación y preservación hasta su análisis y presentación.

La trazabilidad permite reconocer igualmente el contacto, manipulación, transporte, de la evidencia digital, y determinar que la misma pese a su condición de intangibilidad ha estado debidamente custodiada o resguardada de cambios que afecten su integridad.

9.15. VALORACIÓN Y VALIDEZ DE LA PRUEBA ELECTRÓNICA

El Código General del Proceso por su parte en su artículo 243 por su parte mantiene la misma línea del C de P.C. (Art. 251 y SS) en lo que refiere a considerar la prueba electrónica como una especie del género documental, bien reseñado en el Artículo 243 del precitado código cuando menciona las Distintas clases de documentos.

> *"Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares".*[22]

9.16. ANÁLISIS JURISPRUDENCIAL

A continuación, un análisis de un precedente jurisprudencial que permite identificar las principales disposiciones que sobre EDiPE han surgido de las Altas Cortes, con el fin de unificación de criterios e interpretación de las normas que regulan la materia.

Tabla 27. Resumen sentencia C 604 de 2016

1. Sentencia C-604/16 Corte Constitucional	
ENLACE DE ACCESO A SENTENCIA COMPLETA https://www.corteconstitucional.gov.co/RELATORIA/2016/C-604-16.htm#_ftnref3	
1.1. ANTECEDENTES	1.1. Demanda de inconstitucionalidad contra el artículo 247 (parcial) de la Ley 1564 de 2012, "[p]or medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones".
	1.2. NORMA DEMANDADA LEY 1564 DE 2012 (Julio 12) Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones. Artículo 247. Valoración de mensajes de datos. Serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud. La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.
	1.3. Los demandantes acusan de inconstitucional el inciso subrayado. Consideran que, según a esta disposición, los mensajes de datos deben ser valorados a partir de su impresión en papel y conforme a las reglas generales sobre los documentos, no a la luz de sus características técnicas.

22 Colombia, República de. Código General del Proceso, Artículo 243. Colombia: Colombia. ed. (8)

	Siendo esto así, en tanto la integridad de la información contenida en dichas impresiones no resultaría confiable, la obligación de apreciar los mensajes de datos con base en ellas haría imposible controvertirlos y, como consecuencia, la norma desconocería el derecho a la contradicción probatoria.
PROBLEMA JURÍDICO	¿Es o no es, inconstitucional el apartado subrayado de la norma demandada? La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.
TESIS	Declararse INHIBIDA para emitir pronunciamiento de fondo sobre el inciso 2º del artículo 247 de la Ley 1564 de 2012, "Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones, por ineptitud sustancial de la demanda, en relación con el cargo formulado.
TIPO DE PROBLEMA JURÍDICO	De Derecho - Conflicto de método de interpretación
FUENTES JURÍDICAS	Artículo 247 de la Ley 1564 de 2012
EXTRACTOS RELEVANTES	La Ley 527, así como el modelo de la CNUDMI, pretenden crear, en relación con el uso masivo del documento tradicional en papel, una nueva plataforma documental homóloga, a partir de una reconceptualización de nociones como "escrito", "firma" y "original", con el propósito de dar entrada al empleo de técnicas basadas en la informática [5]. En este sentido, el fin de dichas regulaciones es la creación de los denominados "equivalentes funcionales", es decir, de técnicas y mecanismos telemáticos orientados a cumplir la misma función que desempeñan los tradicionales documentos en papel, con idénticas garantías de seguridad y confianza en la información consignada. De esta manera, si el papel hace que el documento sea legible para todos, asegura su inalterabilidad a lo largo del tiempo, permite su reproducción y autenticación y proporciona una manera aceptable de presentación ante las autoridades y los tribunales, el propósito de una legislación sobre el documento electrónico es establecer los requisitos técnicos y jurídicos, a partir de las cuales, todas esas funciones puedan ser realizadas por la documentación basada en mensajes de datos. En la mayoría de los casos, según la Ley Modelo, dicho tipo de documento podría de hecho realizar con mucha mayor fiabilidad y rapidez las mencionadas funciones, por la facilidad para determinar el origen y del contenido de los datos.
	A raíz de los avances tecnológicos en el campo de los computadores, las telecomunicaciones y la informática surgió el "documento electrónico", concebido por la doctrina jurídica como "cualquier representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser

asimilados en forma humanamente comprensible", y reconocido por la legislación patria, concretamente, por la Ley 527 de 1999, declarada exequible mediante las sentencias C-662 de 8 de junio de 2000 y C-831 de 8 de agosto de 2001, estatuto inspirado en la Ley Modelo sobre Comercio Electrónico elaborada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), uno de cuyos principios vertebrales es el de "la equivalencia funcional" de los documentos de esa especie y que se funda en un análisis de los objetivos y funciones que cumple el documento sobre papel con miras a determinar la manera de satisfacerlos en el contexto tecnológico.

Conforme a lo anterior, el artículo 6 de Ley 527 de 1999 estableció que en todos aquellos casos en los cuales una norma jurídica requiera que la información conste por escrito, el requisito quedará satisfecho con un mensaje de datos, si la respectiva información es accesible para su posterior consulta. Por su parte, el artículo 7 previó que cuando se exija la firma del correspondiente documento, la exigencia se entenderá cumplida si se utiliza un método que permita identificar al iniciador del mensaje y determinar que el contenido cuenta con su aprobación, y si es confiable y apropiado para el propósito en virtud del cual el mensaje fue generado o comunicado.

Y, a la luz del artículo 8 ídem, en todos los supuestos en los cuales la ley imponga que la información sea presentada y conservada en su forma original, esta exigencia quedará llevada cabo con un mensaje de datos, siempre que obre alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma, y además, si de requerirse su presentación, puede ser efectivamente exhibida.

Para efectos del artículo anterior, además, la Ley 527 considera que la información contenida en un mensaje de datos es íntegra, siempre que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. Señala, así mismo, que el grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso (art. 9).

6.2.4.5. En relación con la aptitud demostrativa de los documentos en cuestión, la Ley 527 establece como mandato general que en toda actuación judicial o administrativa no podrán negarse efectos jurídicos, validez o fuerza obligatoria y probatoria a todo tipo de información contenida en mensajes de datos (arts. 5 y 20). Pero, además, señala que los mensajes de datos son admitidos como medios de prueba y su fuerza

	probatoria corresponde a la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil (art. 10). En el artículo 11, prescribió que, a efectos de valoración de la fuerza probatoria de los mensajes de datos, deben ser tenidas en cuenta las reglas de la sana crítica y los demás criterios reconocidos legalmente para la apreciación de las pruebas. En particular, señaló como relevantes la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje y en la modalidad de conservación de la integridad de la información, la manera en la que se identifique a su iniciador y cualquier otro factor pertinente. Del mismo modo, la ley establece que en todos los casos en que las normas exijan que documentos, registros o informaciones sean conservados, el requisito quedará satisfecho: i) si la información respectiva es accesible para su posterior consulta; ii) si el mensaje de datos o el documento es conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y iii) si se conserva, de existir, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento (art. 12).
	La confiabilidad en el contenido de los mensajes de datos, como lo puso de presente la Corte Suprema de Justicia en sentencia citada por los demandantes, depende de mecanismos técnicos que garanticen su integralidad, inalterabilidad, rastreabilidad, recuperabilidad y conservación. La integralidad asegura que el contenido transmitido electrónicamente sea recibido en su totalidad; la inalterabilidad garantiza la permanencia del mensaje en su forma original, mediante sistemas de protección de la información; la rastreabilidad permite al acceso a la fuente original de la información; la recuperabilidad posibilita su posterior consulta y de la conservación depende su perdurabilidad en el tiempo, contra deterioros o destrucción por virus informativos.

FUENTE: Sentencia C-604/16 Corte Constitucional

10. AUTOEVALUACIÓN

Ahora que ha terminado de estudiar esta temática, conviene reforzar una serie de conceptos generales que debieron ser aprendidos en esta sección. Lea con atención las siguientes preguntas y formule la respuesta que consideraría que mejor se ajusta a lo estudiado en la sección. Una vez considere que su respuesta es la ideal, revise la respuesta propuesta por los autores y contraste las dos respuestas, reflexionando sobre las similitudes y diferencias obtenidas.

¿Qué es MENSAJE DE DATOS MD?

> *"La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax" (Colombia, 1999)* [23]

¿Cómo está regulado el MD en la legislación colombiana?

La Ley 527, así como el modelo de la CNUDMI, pretenden crear, en relación con el uso masivo del documento tradicional en papel, una nueva plataforma documental homóloga, a partir de una reconceptualización de nociones como "escrito", "firma" y "original", con el propósito de dar entrada al empleo de técnicas basadas en la informática [5]. En este sentido, el fin de dichas regulaciones es la creación de los denominados "equivalentes funcionales", es decir, de técnicas y mecanismos telemáticos orientados a cumplir la misma función que desempeñan los tradicionales documentos en papel, con idénticas garantías de seguridad y confianza en la información consignada.

¿Qué diferencias hay entre MD y Evidencia Digital y Prueba Electrónica?

El Mensaje de Datos contiene información, la EDiPE es un mensaje de datos que contiene información jurídicamente relevante en un proceso judicial y que, al ser valorada y validada como medio de prueba por parte de un Juez competente, hace parte del acervo probatorio que motive una decisión jurisprudencial en un caso particular.

23 Colombia, Republica de. 1999. Ley 527 de 1999 Ley de Comercio Electrónico. Colombia: s.n., 1999. (5 pág. 1)

11. TALLER DE ESTUDIO DE ANÁLISIS DE CASOS

11.1. INSTRUCCIONES DE IMPLEMENTACIÓN

Lea con atención cada ficha técnica del caso que se le presenta, identifique cual es el problema jurídico central y con base a lo repasado en la guía de aspectos generales de la EDiPE, responda la pregunta de cada caso particular.

11.2. LECTURA PREVIA

En la parte inferior del título de cada caso encontrará unos antecedentes que debe leer como contexto de cada caso particular. Debe ser abordada esta lectura antes de responder lo requerido.

11.3. ESTRATEGIA DE EVALUACIÓN

Usualmente un caso de estudio implica una situación, un diagnóstico y una propuesta de solución.

En derecho, eso se traduce en: Hechos del Caso, Definición de Problema Jurídico, y propuesta de Teoría del Caso/Estrategia del Litigio.

La evaluación usualmente es proponerle al discente que defina el problema jurídico y presente una teoría/estrategia y que luego la contraste con la solución presentada por el docente.

Se especifican los criterios a evaluar, a través de una tabla que dependerá de lo que responda él/la discente.

1	Presentación de tesis
2	Identificación del problema jurídico
3	Fuentes jurídicas aplicadas
4	Estándares técnicos implementados
5	Procedimiento forense propuesto

11.3.1. CASO "GIMNASIO"

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos

ANTECEDENTES	El 24 de mayo de 2018, Ana María Ramírez, mayor de edad, madre de dos menores de edad y esposa de Juan Angarita, trabajó como entrenadora personal de un gimnasio ubicado en Bogotá
	El 31 de octubre de 2018, Ana María Ramírez comenzó a sostener una relación extramatrimonial con un cliente del gimnasio llamado Juan Francisco Palomeque, mayor de edad, padre de un menor de edad y esposo de Mónica Leguizamo.
	El 15 de noviembre de 2018 Ana María Ramírez recopila indicios que la llevan a sospechar de una posible infidelidad de su pareja sentimental con otra persona. Dichos indicios eran: varias llamadas de números desconocidos y nerviosismo al contestar en su presencia, también por un testimonio de oídas de una amiga de la señora que trabaja con su compañero sentimental.
	El día 20 de noviembre de 2018, Ana María Ramírez compró, a través de la darknet, un software adquirido en la página web https://www.spymyfone.com/es/ Ana María decidió pagar con cargo a su tarjeta de crédito la suma de $600.000 colombianos pesos los cuales pidió diferir en 10 cuotas. Este software ofrecía entre otras las siguientes capacidades: • Acceder a Chats de Mensajería Instantánea y Archivos de Multimedia • Monitorear Llamadas Telefónicas & Mensajes de Texto • Rastrear de Ubicación & Geo-Cerca • Monitorear todas las Actividades En Línea & Desconectado • Para acceder a estos servicios, la compañía Spymyfone le entregó un usuario y una clave a Ana María, con la cual pudo acceder a la plataforma provista por esa compañía a sus clientes y configurar o personalizar las peticiones que requería del teléfono a monitorear. • Según las instrucciones así recibiría un enlace que debía compartir a través de un correo o chat (mensajería de WhatsApp), al teléfono a monitorear.
	El día 16 de diciembre de 2018, Ana María Ramírez aprovechó: i) el acceso a las claves de los casilleros de ropa de los clientes del Gimnasio y logró acceder al celular de Juan Francisco Palomeque, quien guardó su equipo sin bloqueo de seguridad. Producto de lo anterior, Ana María logró instalar el software malicioso previamente comprado.

	El mismo 16 de diciembre de 2018, el software le reportó, a María Ramírez, remotamente una serie de mensajes de datos que relacionaban a Juan Francisco Palomeque con Helena Montoya y cuyo contenido era material explícito en formatos foto, video y chat.
	El 31 de diciembre de 2018, Ana María Ramírez envía, en estado de alicoramiento, a Mónica Leguizamo (esposa de Juan Francisco Palomeque) los mensajes de datos que obtuvo con el software malicioso que instaló en el celular de Juan Francisco Palomeque.
	El día 8 de febrero de 2019 Mónica Leguizamo decide interponer una demanda de divorcio y separación de sociedad conyugal aduciendo como causal principal infidelidad y allegando material para demostrarlo los mensajes de datos que le fueron entregados por parte de María Ramírez.
PROPÓSITO DEL ESTUDIO DE CASO	Identificar las fuentes de derecho que regulan aspectos tratados en el caso en concreto.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto.
	Aplicar los conocimientos prácticos obtenidos en la Guía de Evidencia Digital y Prueba electrónica para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Es o no es, el material digital presentado en la demanda de divorcio, válido como material probatorio en un proceso jurídicamente relevante? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.
	Uso de instrumento de entrevista semiestructurada dirigido a funcionario judicial participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

11.3.2. CASO "CLÍNICA"

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos

ANTECEDENTES	El día 29 de diciembre de 2017, Ricardo Portela, ingeniero de soporte TI de la Clínica Infinity, fue notificado personalmente por su empleador, sobre la no continuidad y cancelación y liquidación de su contrato de prestación de servicios profesionales a partir del 1 de enero de 2018.
	El día 30 de diciembre de 2017, Ricardo Portela entregó su puesto de trabajo a su jefe inmediato, incluyendo las credenciales del acceso de administración y gestión del software clínicaaldía Versión 3.0. de la Clínica Infinity.
	El software clínicaaldía Versión 3.0. de la Clínica Infinity trataba mensajes de datos entre otros datos personales de los pacientes.
	El día 2 de enero de 2018, apareció en un portal web desconocido, una galería de fotos, datos, y videos de los pacientes de la Clínica Infinity.
	El día 09 de enero, Patricia Alcalá, paciente de la clínica, empezó a recibir mensajes en su teléfono celular desde un número incógnito, en los cuales le exigían el pago de 12 millones de pesos, a cambio de la no divulgación de unas fotografías desnuda de ella.
	El 10 de enero Paula Enciso, paciente de la clínica igualmente recibió mensajes de carácter extorsivo en la misma tónica, en su caso ya habían sido subidas algunas fotografías a un portal de pornografía gratuita como medio de presión.
	El día 12 de enero, las tablas de las bases de datos de las historias clínicas, fueron afectadas y la información no era posible de acceder por cuanto los registros de edad, sexo, medidas, talla, peso, y otros datos relevantes del tratamiento habían sido desligados del gestor que traía la información al sistema que permite visualizarlos en pantalla.
	El día 13 de enero la Clínica fue demandada por parte de seis pacientes por la fuga de las fotografías y las extorsiones consecuentes que se presentaron.
PROPÓSITO DEL ESTUDIO DE CASO	Identificar las fuentes de derecho que regulan aspectos tratados en el caso en concreto.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto y sus implicaciones en razón a la afectación de derechos fundamentales.

	Aplicar los conocimientos prácticos obtenidos en la Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia - Aspectos generales para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Qué procedimientos forenses se podrían realizar para ayudar al Juez a determinar el responsable por el criminal uso de los datos personales sensibles de los pacientes de la Clínica Infinity? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.
	Uso de instrumento de entrevista semiestructurada dirigido a funcionario judicial participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

11.3.3. CASO PRUEBAS CONCURSO PARA ADMISIÓN

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos

ANTECEDENTES	El día 10 de agosto de 2019, Rene Quintero participó en el Concurso de admisión de nuevos profesionales en el recientemente creado Ministerio de Ciencia y Tecnología en adelante MCT.
	El 20 de septiembre de 2019, fueron publicados los resultados siendo admitidos 35 nuevos profesionales para ocupar las plazas vacantes en concurso. Rene Quintero no apareció en los admitidos.
	El día 21 de septiembre de 2019, Rene Quintero instauro una demanda contenciosa administrativa por la falla en el servicio" al no haber cumplido con los requisitos de selección del concurse establecido en la ley. La demanda aduce que las preguntas del examen fueron filtradas abusivamente y se encontraban disponibles para consulta en diversos foros de internet accesibles solo mediante pago.
	La demanda adjunta en formato electrónico un archivo con el nombre "Cuestionario concurso admisión al MCT". Las propiedades de este archivo señalan su fecha de creación el día 19 de julio de 2019. Autor: Oficina Admisiones MCT.

	El demandante RENE QUINTERO, informa en el escrito que este archivo se encuentra disponible en el enlace pruebasaccesos.onion y que se enteró de ello el mismo día del examen.
	Admitida la demanda el delegado del MCT responde en la contestación de la demanda, que el examen siempre estuvo en custodia de la entidad y no se conocía su contenido hasta una hora antes del examen. Así mismo aduce que las características del archivo aportado en la demanda no corresponden en fechas ni usuarios a las que reposan en el MCT. Para ello aporta un archivo denominado "Examen admisión pruebas Concurso Agosto"
	Al comparar el contenido de los cuestionarios, se evidencia que trata las mismas preguntas, en otras palabras, contienen la misma información.
PROPÓSITO DEL ESTUDIO DE CASO	Identificar las fuentes de derecho que regulan aspectos tratados en el caso en concreto.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto y sus implicaciones en razón a la afectación de derechos fundamentales.
	Aplicar los conocimientos prácticos obtenidos en la Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia - Aspectos generales para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Cuál de los dos medios presentados en juicio, el presentado por el demandante o el de la entidad demandad, tiene mayor validez y vocación probatoria? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.
	Uso de instrumento de entrevista semiestructurada dirigido a funcionario judicial participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

11.3.4. CASO CyberCelos

NOTA: Caso de la vida real, se cambiaron los nombres y situaciones reales con fines académicos

ANTECEDENTES	El día Nueve (9) de febrero del 2007 el señor Jaime Ceballos contrajo matrimonio con la señora Margarita Castro.
	El día treinta (30) de enero de 2015 la señora Margarita Castro entró a trabajar en Banco Macondo en el área de servicio al cliente.
	El día diez (10) de julio de 2016, la señora Margarita Castro accede abusivamente a las bases de datos financieros de tarjetas de crédito del Banco Macondo; en dicha base de datos encontró un reporte de pago a nombre del señor Jaime Ceballos en un Motel. Dicha base de datos le arrojo el día exacto, el lugar exacto y el monto pagado. A dicho reporte revisado desde un computador del Banco Macondo, la señora Margarita Castro le tomo una foto con su celular.
	El día doce (12) de agosto de 2016, la señora Margarita, demanda de divorcio, por medio de apoderada, al señor Jaime Ceballos, adjuntando como prueba la fotografía tomada al computador del Banco Macondo.
PROPÓSITO DEL ESTUDIO DE CASO	Identificar las fuentes de derecho que regulan aspectos tratados en el caso en concreto.
	Analizar las características técnicas relacionadas con los mensajes de datos objeto de debate en el caso en concreto y sus implicaciones en razón a la afectación de derechos fundamentales.
	Aplicar los conocimientos prácticos obtenidos en la Guía de Aprendizaje Autodirigido en Evidencia Digital y Prueba Electrónica en Colombia – Aspectos Generales para dirimir el caso en concreto.
PREGUNTA DE REFLEXIÓN	¿Cumplió o no, el mensaje de datos del caso con los requisitos jurídicos y técnicos internacionales para valorarlo y validarlo como evidencia digital? justifique su respuesta.
UNIDAD DE ANÁLISIS	Guía de aprendizaje autodirigido de Evidencia Digital y Prueba Electrónica: Aspectos Generales.
MÉTODO E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN	Uso de método cualitativo con énfasis en comprender las perspectivas de las personas involucradas en el caso en concreto.

	Uso de instrumento de entrevista semiestructurada dirigido a él/la discente participante en el caso que expone hechos de la vida real.
MÉTODO DE ANÁLISIS DE LA INFORMACIÓN	La información recolectada se analizó acorde a las preguntas del caso en concreto.

12. JURISPRUDENCIA

A continuación, se presenta a él/la discente, una lista de precedentes jurisprudenciales ordenados cronológicamente para conocer los principales conceptos definidos y relacionados con la Evidencia Digital y Prueba Electrónica en Colombia.

El objetivo de esta lista es proveer a él/la discente de un instrumento de consulta directa y detallada de los conceptos unificados resultantes del ejercicio continuo de fallos jurisprudenciales, que son fuente directa de derecho aplicable a casos concretos.

AÑO	MAGISTRADO PONENTE	FUENTE DE DERECHO	RELEVANCIA	TEMA	CATEGORIA	LINK
2007	M.P. DR. JAIME CÓRDOBA TRIVIÑO	Sentencia 405/2007	Autodeterminación sobre la propia imagen.	Prevalencia del bloque de constitucionalidad.	El derecho a: la imagen, intimidad, honra y al buen nombre del ser humano.	https://www.corteconstitucional.gov.co/relatoria/2007/T-405-07.htm
2012	M.P. D.R. HUMBERTO ANTONIO SIERRA PORTO	Sentencia T-260/ 2012	Principio del interés superior del menor-consagración constitucional e internacional/derechos de los niños, niñas y adolescentes-obligación del estado de brindar una protección especial	Intimidad y habeas data en página web o sitio de internet-	Acceso a redes sociales de niños, niñas y adolescentes-debe darse con acompañamiento de los padres o personas responsables de su cuidado.	https://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM
2013	M. P. DRA. MARÍA VICTORIA CALLE CORREA	Sentencia T-634/2013	Régimen de Protección de Datos Personales	Derecho a la imagen, Autorización para el uso de la propia imagen	Uso de Imagen como Dato Sensible	https://www.corteconstitucional.gov.co/relatoria/2013/t-634-13.htm
2016	M.P. DR. LUIS GUILLERMO GUERRERO PÉREZ	Sentencia T-145/2016	UNIFICACIÓN DE CONCEPTOS JURISPRUDENCIALES EN TORNO A LOS CONFLICTOS OCASIONADOS EN EL	libertad de expresión stricto sensu y libertad de información	Caso en que a través de la red social Facebook, se publicó foto del rostro de accionante en	https://www.corteconstitucional.gov.co/relatoria/2016/t-145-16.htm

AÑO	MAGISTRADO PONENTE	FUENTE DE DERECHO	RELEVANCIA	TEMA	CATEGORIA	LINK
			ÁMBITO DE LAS REDES SOCIALES [24]		primer plano, acompañada de un comentario injurioso y contrario a su buen nombre	
2016	M.P. DR. GABRIEL EDUARDO MENDOZA MARTELO	Sentencia T-050/2016	ESTADO DE INDEFENSION-Configuración cuando se da la circulación de información u otro tipo de expresiones a través de medios que producen un alto impacto social que trascienden la esfera privada de quienes se ven involucrados.	Libertad de expresión en internet y redes sociales	Estado de Indefensión	https://www.corteconstitucional.gov.co/Relatoria/2016/T-050-16.htm
2017	M.P. DR. CARLOS BERNAL PULIDO	Sentencia T-593/17	Exoneración de carga de la prueba cuando se trata de afirmaciones y negaciones indefinidas	Derechos al buen nombre y honra frente a libertad de expresión y opinión	mensaje fue difundido mediante la aplicación "WhatsApp y Facebook.	https://www.corteconstitucional.gov.co/relatoria/2017/T-593-17.htm

24 (i) Las redes sociales pueden convertirse en centros de amenaza, en particular para los derechos fundamentales a la intimidad, a la imagen, al honor y a la honra.

(ii) Cuando se presentan amenazas o violaciones a derechos fundamentales en una red social, el problema de índole jurídico debe resolverse a la luz de las disposiciones constitucionales y no a partir de la regulación establecida por la red social específica de que se trate.

(iii) Las tecnologías de la información y las comunicaciones (redes sociales y otras) potencializan el daño causado a las víctimas de acoso y maltrato.

(iv) El derecho a la intimidad se trasgrede cuando se divulgan datos personales de alguien que no corresponden a la realidad.

(v) El derecho a la imagen emana del derecho al libre desarrollo de la personalidad y del derecho al reconocimiento de la personalidad jurídica. Se trasgrede cuándo la imagen personal es usada sin autorización de quien es expuesto o si se altera de manera falsa o injusta la caracterización que aquél ha logrado en la sociedad.

(vi) Los derechos al buen nombre y a la honra se lesionan cuando se utilizan expresiones ofensivas, falsas, erróneas o injuriosas en contra de alguien.

(vio) El derecho a la libertad de expresión, materializado a través de cualquier medio, tiene límites. Así, no ampara la posibilidad de exteriorizar los pensamientos que se tienen sobre alguien de manera ostensiblemente descomedida, irrespetuosa o injusta. (viii) El derecho a la libertad de expresión en principio tiene prevalencia sobre los derechos al buen nombre y a la honra, salvo que se demuestre que en su ejercicio hubo una intención dañina o una negligencia al presentar hechos falsos, parciales, incompletos o inexactos que violan o amenazan los derechos fundamentales de otros, en tanto los derechos de los demás en todo caso constituyen uno de sus límites.

(ix) En el ejercicio de la libertad de opinión no puede denigrarse al semejante ni publicar información falseada de éste, so pena de que quien lo haga esté en el deber de rectificar sus juicios de valor. (x) Ante casos de maltrato en redes sociales el juez constitucional debe propender porque se tomen medidas para que este cese y, además, para que se restauren los derechos de los afectados, siempre que así lo acepten éstos últimos, condición que se exige en aras de evitar una nueva exposición al público de situaciones que hacen parte de su esfera privada.

AÑO	MAGISTRADO PONENTE	FUENTE DE DERECHO	RELEVANCIA	TEMA	CATEGORIA	LINK
2018	M.P. DR. JOSÉ FERNANDO REYES CUARTAS	Sentencia T-454/18	en las redes sociales –Facebook, Twitter, Instagram, etc.- pueden generar un estado de indefensión entre particulares, debido al amplio margen de control que tiene quien la realiza	Derecho a la honra y al buen nombre frente a libertad de expresión e información, Derecho de rectificación de información, Derecho a la imagen Redes sociales	Derecho a la información y a la honra, buen nombre en sociales	https://www.corteconstitucional.gov.co/relatoria/2018/T-454-18.htm
2018	M.P. DR. CRISTINA PARDO SCHLESINGER	Sentencia T-277/18	Caso en que se realizaron publicaciones en Facebook sobre la gestión como alcalde del accionante	Derechos a la intimidad, buen nombre y honra frente a libertad de expresión y opinión-	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2018/T-277-18.htm
2018	M.P. DR. CARLOS BERNAL PULIDO	Sentencia T-121/18	Casos en que se solicita rectificación de información difundida y eliminación de video de la plataforma YouTube	Derecho a la honra y al buen nombre en redes sociales-	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2018/t-121-18.htm
2018	M.P. DRA. DIANA FAJARDO RIVERA	Sentencia T-243/18	Vulneración en red social por una publicación donde se acusaba de hurto sin haber sentencia judicial que así lo soportara	Derecho a la honra y al buen nombre de empleada doméstica en redes sociales-	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2018/T-243-18.htm
2019	M.P. DR. ALEJANDRO LINARES CANTILLO	Sentencia T-179/19	No se reconoce protección constitucional a los derechos fundamentales a la honra, intimidad y buen nombre	Libertad de expresión en redes sociales	Derechos Fundamentales	https://www.corteconstitucional.gov.co/relatoria/2019/T-179-19.htm#_ftn15

13. BIBLIOGRAFÍA

1. Administrativo, Código de Procedimiento Administrativo y de lo Contencioso. Artículo 216. [aut. libro] Colombia. *LEY 1437 DE 2011.* Colombia: s.n., 2011.

2. Restrepo, Alexander. *Manual de Autores para el diseño y redacción de módulos de Aprendizaje Autodirigido.* Bogotá D.C.: Consejo Superior de la Judicatura, 2019.

3. Romelio, Daza Molina. *Las TIC Ante el Derecho Colombiano y la Gestión Judicial*. Bogotá D.C.: Librería Ediciones del Profesional L.T.D.A., 2017.

4. Peña, Daniel. *De la Firma Manuscrita a las Firmas Electrónicas y Digital.* Bogotá D.C.: Universidad Externado de Colombia, 2015. 72.

5. Colombia. *Ley 527 de 1999 Comercio Electrónico.* Colombia: Colombia, 1999. 2.

6. GFI. *END POINT SECURITY.* 2012.

7. M., Jeimy J. Cano. *Computación Forense Descubriendo los rastros informáticos.* Bogotá D.C.: Alfaomega, 2015.

8. Colombia, República de. *Código General del Proceso, Artículo 243*. Colombia: Colombia. ed.

Podcast Evidencia Digital:
https://anchor.fm/evidenciadigital

CONSEJO SUPERIOR DE LA JUDICATURA
ESCUELA JUDICIAL "RODRIGO LARA BONILLA"

escuelajudicial.ramajudicial.gov.co
CALLE 11 # 9 A – 24, PISO 4
PBX (+57) 355 06 66
BOGOTÁ D.C., COLOMBIA
2020