COMUNICACIÓN INTERINSTITUCIONAL

Para: Entidades Públicas Nacionales y Territoriales

De: Agencia Nacional de Defensa Jurídica del Estado

Asunto: Lineamiento sobre uso adecuado y eficiente de los mensajes de datos como medio de prueba

Bogotá, D.C, 10 de junio de 2022

En desarrollo de lo dispuesto en la Ley 1444 de 2011, el Decreto Ley 4085 de 2011 otorgó competencias en materia de defensa judicial y prevención de las conductas y del daño antijurídico a la Agencia Nacional de Defensa Jurídica del Estado (ANDJE). De conformidad con este marco normativo, a la entidad le corresponde recomendar, en aquellos casos que considere pertinente, las acciones y gestiones que deban adelantar las entidades públicas para una adecuada prevención y defensa de los intereses de la Nación.

Esta Agencia, a través de la Dirección de Políticas y Estrategias, presenta el siguiente lineamiento que pretende promover el uso adecuado y eficiente de los mensajes de datos por parte de las entidades públicas[1].

El documento consta de tres capítulos. El primero aborda las generalidades de los mensajes de datos. El segundo describe el proceso de identificación, recolección, aseguramiento, almacenamiento y entrega de mensajes de datos. El tercero explica aspectos prácticos de la utilización de los mensajes de datos como medio de prueba en los procesos judiciales.

I. Generalidades sobre los mensajes de datos[2]

1. Un mensaje de datos es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares[3], por ejemplo: archivos de texto en

[1] El presente lineamiento es una guía que contiene los elementos básicos para la utilización de mensajes de datos. Para una mayor profundización en todo lo relacionado con este asunto, se recomienda realizar el curso sobre mensajes de datos disponible en la Comunidad Jurídica del Conocimiento.

[2] Sobre las generalidades de la evidencia digital, pueden consultarse las diferentes "Cartillas sobre Evidencia Digital" elaborada por la Escuela Judicial Rodrigo Lara Bonilla para los funcionarios de la rama judicial. Las Cartillas pueden descargarse en el siguiente enlace: CARTILLAS DIGITALES Y PODCAST SOBRE EVIDENCIA DIGITAL PRIMER CICLO DE CAPACITACIÓN GENERAL Y ESPECIALIZADA EN EL USO DE LAS TIC | Escuela Judicial Rodrigo Lara Bonilla (ramajudicial.gov.co).

[3] Cfr. Literal a, artículo 2 de la Ley 527 de 1999. La Corte Constitucional ha manifestado al respecto: "La noción de "mensaje" comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación modernas, bajo la configuración de los progresos técnicos que tengan contenido jurídico. Cuando en la definición de mensaje de datos, se menciona los "medios similares", se busca establecer el hecho de que la norma no está exclusivamente destinada a conducir las prácticas modernas de comunicación, sino que pretenden ser útil para involucrar todos los adelantos tecnológicos que se generen en un futuro." Corte Constitucional. Sentencia C-662 de 2000. M.P. Fabio Morón Díaz. Así mismo, sobre las características esenciales de los mensajes de datos ha indicado: (i) es una prueba de la

formato Word almacenados en un computador, mensajes de chat, fotografías o imágenes digitales, sitios web, archivos de audio, entre otros. Las normas procesales usan también la denominación de "documentos electrónicos"[4].

2. En relación con los mensajes de datos, las entidades públicas deben tener en cuenta que:

2.1. La información contenida en un mensaje de datos produce plenos efectos jurídicos y es vinculante[5] (p.e. la oferta que se acepta por correo electrónico).

2.2. Los mensajes de datos consideran equivalentes a los documentos en papel, es decir, cumplen la misma función y tienen la misma validez jurídica y eficacia probatoria[6]. Para el efecto, deben reunirse ciertas exigencias legales:

a) La información debe poderse consultar con posterioridad a su creación[7].

b) Para la consulta, las entidades públicas deben contar con:

existencia y naturaleza de la voluntad de las partes de comprometerse; (ii) es un documento legible que puede ser presentado ante autoridades administrativas y judiciales; (iii) admite su almacenamiento e inalterabilidad en el tiempo; (iv) facilita la revisión y posterior auditoría para los fines contables, impositivos y reglamentarios; (v) afirma derechos y obligaciones jurídicas entre los intervinientes; y (vi) es accesible para su ulterior consulta, en tanto la información en forma de datos computarizados es susceptible de leerse e interpretarse. (Corte Constitucional. Sentencia C-662 de 2000. M.P. Fabio Morón Díaz).

[4] Cfr. Artículo 2.8.2.7.2. del Decreto 1080 de 2015 "un documento generado y gestionado a través de sistemas o medios electrónicos". Son documentos electrónicos, por ejemplo, un contrato, un título valor, un texto electrónico en Word, entre otros mensajes de datos que tengan forma documental.

[5] Artículo 5 de la 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." La vinculatoriedad de la información contenida en mensajes de datos se ratifica en los artículos 14 y 15, que se refieren a la formación del contrato mediante la oferta y aceptación expresadas por medio de un mensaje de datos y a las manifestaciones de voluntad o declaraciones de las partes a través de mensajes de datos, respectivamente.

[6] Esta característica se conoce como el principio de "equivalencia funcional" de los mensajes de datos y es el eje fundamental de su validez jurídica y probatoria. La Corte Constitucional, al estudiar una norma procesal sobre el valor probatorio de los mensajes de datos, explicó sobre el origen y alcance de la equivalencia funcional: "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. 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 públicas 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." Corte Constitucional. Sentencia C-604 de 2016. M.P. Luis Ernesto Vargas Silva.

[7] Cfr. Artículo 6 de la Ley 527 de 1999 "ESCRITO. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. | Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito."

- El dispositivo o aparato electrónico que permita acceder al archivo digital (hardware).

- El programa o sistema operativo que permita traducir la información contenida en el mensaje de datos a un lenguaje comprensible para el usuario (software) [8].

2.3. El mensaje de datos puede estar en cualquier formato y utilizar cualquier tecnología[9].

2.4. La información que contiene se reputa original siempre que se cumplen dos requisitos[10]:

a) Que haya garantía de que la información se ha conservado completa e inalterada desde el momento en que se generó por primera vez (integridad de un mensaje de datos) [11].

b) Que la información pueda ser consultada con posterioridad.

2.5. La integridad de un mensaje de datos se garantiza con tecnologías como la firma electrónica[12] y la firma digital[13].

---

[8] El archivo digital es el canal que permite tener acceso a la información, pero no es el mensaje de datos en sí mismo. Si no se logra el acceso a la información, por más que exista un archivo digital, no puede considerarse -jurídicamente- que exista un mensaje de datos.

[9] Se conoce como el principio de "neutralidad tecnológica", según el cual el Estado garantiza la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen TIC y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible. No se debe excluir, restringir o privar de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología empleado (Decreto 2364 de 2012 -compilado en el D.U.R. 1074/2015- y Decreto 2609 de 2012 -compilado en el D.U.R. 1080/2015-).

[10] Cfr. Artículo 8 de la Ley 527 de 1999 "ORIGINAL. Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si: a) Existe 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; | b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar. | Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original".

[11] El artículo 9 de la Ley 527 de 1999 consagró el alcance de la noción de "integridad" de un mensaje de datos en los siguientes términos: "Integridad de un mensaje de datos. Para efectos del artículo anterior, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. 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".

[12] En los términos del artículo 1 del Decreto 2364 de 2012 la firma electrónica es aquella que se basa en "[m]étodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente."

[13] De acuerdo con el artículo 2 de la Ley 527 de 1999 la firma digital corresponde a un "valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación". Será equivalente a la firma manuscrita siempre que cumpla las siguientes características: (i) es única a la persona que la usa; (ii) es susceptible de ser verificada; (iii) está

a) Estos dos tipos de firma serán equivalente a una firma manuscrita si permiten acreditar con certeza quién es el firmante[14] ("autenticidad"[15]).

b) Ambas producen los mismos efectos jurídicos como mecanismos de autenticación. El contraste es exclusivamente probatorio y radica en las diferencias en la carga de probar los atributos de seguridad jurídica y la tecnología que utilicen.

c) La firma electrónica en un mensaje de datos hará que éste se considere "confiable" y "apropiado" si: (i) los datos de creación de la firma corresponden exclusivamente al firmante ("autenticidad") y (ii) es posible detectar cualquier alteración no autorizada del mensaje de datos hecha después del momento de la firma ("integridad"). En este caso, a diferencia de lo que ocurre con la firma digital, es necesario acreditar los atributos para demostrar su seguridad jurídica[16].

d) La firma digital en un mensaje de datos permite garantizar (i) la autenticidad (quién es el iniciador del mensaje[17]); (ii) la integridad (no alteración) y (iii) el no repudio de un mensaje de datos (imposibilidad de retractarse o de refutar). Estos atributos se entienden incorporados de manera automática en la firma digital, por lo que la ley presume que esta firma es "confiable" y "apropiada" (seguridad jurídica).

e) La validez de las firmas digitales es avalada por una "Entidad de Certificación"[18].

2.6. Los mensajes de datos permiten la conservación de documentos, registros o informaciones[19].

---

bajo el control exclusivo de la persona que la usa; (iv) está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada; y (v) está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

[14] Cfr. Artículo 7 de la Ley 527 de 1999: "FIRMA. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si: a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación; | b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado. | Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma."

[15] Propiedad de que una persona o entidad es la que afirma ser. Es esencial en el entorno digital, en tanto es el elemento que permite mitigar los riesgos de suplantación de identidad. (Cartilla evidencia digital Escuela Rodrigo Lara Bonilla)

[16] Cfr. Artículos 3 y 4 del Decreto 2364 de 2012.

[17] Persona que, actuando por su cuenta, o en cuyo nombre se haya actuado, envíe o genere un mensaje de datos (Cfr. Artículo 3 del Decreto 333 de 2014, Compilado en el D.U.R. 1074/2015).

[18] De acuerdo con el artículo 2 de la Ley 527 de 1999, se refiere a "aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales". Ver: Corte Constitucional. Sentencia C-662 de 2000. M.P. Fabio Morón Díaz.

[19] Al respecto, el artículo 12 de la Ley 527 de 1999 señala: "Conservación de los mensajes de datos y documentos. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:
1. Que la información que contengan sea accesible para su posterior consulta.

2.7. De acuerdo con la legislación colombiana, los mensajes de datos pueden ser considerados evidencia digital, es decir, medio de prueba válido y eficaz para ser aportado en actuaciones administrativas y en procesos judiciales y arbitrales.

2.8. Las entidades públicas que pretendan utilizar mensajes de datos como evidencia digital deben cumplir con los requerimientos y estándares establecidos en la normativa vigente y aplicable.

II. Identificación, recolección, aseguramiento, almacenamiento y entrega de mensajes de datos

1. Para utilizar adecuadamente un mensaje de datos en cualquier actuación y que tenga plena validez jurídica, ya sea en sede administrativa o judicial, es indispensable que las entidades realicen una adecuada identificación, recolección, aseguramiento, almacenamiento y entrega de la información.

2. Durante estas etapas, las entidades deben seguir unos rigurosos procedimientos en la manipulación de los mensajes de los datos para garantizar su eficacia probatoria y la seguridad de la información[20].

2.1. **Etapa de identificación.** Consiste en delimitar todos los dispositivos electrónicos de los que potencialmente se pueden extraer los mensajes de datos[21]. Se recomienda un trabajo conjunto con el profesional experto en recursos tecnológicos o ingeniero de soporte de la entidad, para:

a) Identificar todos los aparatos o dispositivos electrónicos de los que se puede extraer evidencia digital (hardware), tales como: computador (de escritorio y portátil), hardware de red, servidor[22], teléfono móvil inteligente, localizador, GPS, cámara digital, videocámara, asistente personal PDA, tarjeta inteligente, tableta, televisión, memoria "flash", impresora, fotocopiadora, grabadora, dron, USB, Firewire, CD/DVD, PCMCIA, disco óptico y magnético, disco duro (extraíble o no), memoria SD, MicroSD, router, registro de dispositivos de seguridad informática[23], plataforma antispam, etc.

---

2. Que el mensaje de datos o el documento sea 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
3. Que se conserve, de haber alguna, 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.
No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos". En el mismo sentido, ver el artículo 13 de la misma ley.

[20] El conjunto de acciones para un adecuado manejo de los mensajes de datos se denomina "debido procedimiento de informática forense" y consiste en la aplicación de la ciencia para la identificación, recolección, examen y análisis de los datos, preservando correctamente su integridad, llevando a cabo a su vez una estricta cadena de custodia de la información.

[21] En conjunto estos aparatos y dispositivos constituyen las "fuentes de evidencia digital".

[22] Puede ser web, DHCP, email, mensajería instantánea, VoIP Servers, FTP o cualquier servicio de filesharing.

[23] Por ejemplo, IDS y Firewalls.

b) Revisar los programas y mensajes de datos que se han generado, enviado, recibido, almacenado o comunicado a través de los aparatos o dispositivos electrónicos y precisar aquella información que pretenda utilizarse como evidencia digital.

c) Utilizar las herramientas y programas informáticos que determine el experto en recursos tecnológicos, con el fin de detectar cualquier incidente que pueda poner en riesgo la seguridad de la información[24], tales como: acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento o falla en la operación normal de las redes, sistemas o recursos informáticos; violación a una política de seguridad de la información; entre otros[25].

d) Ante la posible ocurrencia de incidentes de seguridad de información, el experto informático y/o el ingeniero de soporte, debe:

- Implementar el plan de acción previamente definido por la entidad que instruya al personal del área de sistemas y tecnologías de la información sobre cómo reaccionar y qué procedimientos a efectuar.

- Identificar información que pueda ayudar a reconstruir y analizar el origen del incidente (ej. ataque informático a la red), o que permita rastrear algún tipo de acceso o movimientos específicos que puedan estar relacionados con el incidente (ej. uso indebido de la información por parte de un funcionario).

- Evaluar la necesidad de aislar la escena del incidente para disminuir el impacto y/o preservar la información. De estimarse necesario, un profesional especializado de la entidad (preferiblemente un ingeniero informático forense o de seguridad de la información) debe proceder al aislamiento, para lo cual se recomienda:

  ✓ Registrar en un acta el procedimiento y metodología utilizados.

  ✓ Describir cada una de las actividades desarrolladas en el proceso de aislamiento por parte del experto informático.

  ✓ Prohibir cualquier tipo de contacto con el equipo y/o acceso a la red en la que reside la información. Debe establecerse un “perímetro de seguridad” para que ninguna persona no autorizada interfiera en el procedimiento.

  ✓ Evitar que se altere la escena o se borre información relevante. Para el efecto, si el dispositivo está encendido, no se debe apagar. Si está apagado, no se debe encender.

[24] Se denomina comúnmente “incidente de seguridad de información”.
[25] Ministerio de las Tecnologías de la Información y las Comunicaciones. *Seguridad y Privacidad de la Información.* Guía No. 13, “Evidencia Digital”, 2016.

- ✓ Asegurar el equipo. Por ejemplo, si el equipo es un portátil, mantenerlo encendido y conectado al cargador.

- ✓ Sellar los puertos del dispositivo (ej. USB, firewire, HDMI, unidades CD/DVD, etc).

- ✓ Tomar fotografías o videos para registrar lo que se observa en la pantalla durante cada uno de los procedimientos efectuados (documentos abiertos, notificación, fecha y hora, etc.).

- ✓ Almacenar la información original en un sitio con acceso restringido y con la debida seguridad informática (ej. carpeta en la nube encriptada).

- ✓ Evaluar si otros dispositivos tuvieron contacto o interacción con el equipo en cuestión, con el fin de determinar si otra información se vio afectada con el incidente de seguridad.

- Elaborar un reporte detallado sobre todas las actuaciones realizadas en el marco del incidente de seguridad. El reporte debe incluir:

  - ✓ El análisis final de los expertos sobre el incidente, indicando si hubo pérdida o alteración de información.

  - ✓ Explicación de cómo y por qué fueron utilizadas las diferentes herramientas y procedimientos en el incidente.

  - ✓ Acciones de mejora y recomendaciones para implementar las herramientas necesarias y evitar futuros incidentes (ej. mejoras a controles de seguridad, reducción de puntos vulnerables en la red, fortalecimiento de mecanismos de identificación para acceder a la información, etc.).

2.2. **Etapa de recolección.** Consiste en la extracción de los datos del aparato o dispositivo en los que reposan (ej. sustraer un mensaje de WhatsApp del celular del cual fue enviado o la información acerca de la entrega de un correo electrónico del servidor web, o extraer los datos de localización del dispositivo en el momento en el que se tomó una fotografía.

Para la recolección de la información se recomienda:

a) Establecer el orden en el que se realizará la extracción de los mensajes de datos de los diferentes dispositivos, con el fin de evitar pérdidas de la información. Para el efecto, se debe evaluar el riesgo de que cierta información desaparezca con el tiempo si no se recolecta oportunamente (ej. si el computador se reinicia o apaga)[26]; la complejidad de

[26] Este fenómeno se denomina "volatilidad de la información". Esto puede ocurrir, por ejemplo, cuando el sistema en el cual se almacena la evidencia digital es reiniciado o apagado. Al respecto, ver: Ministerio de las Tecnologías de la Información y las Comunicaciones. *Seguridad y Privacidad de la Información.* Guía No. 13, "Evidencia Digital", 2016.

obtener ciertos datos (ej. información almacenada en memorias ocultas del dispositivo); los permisos requeridos para acceder a la información (ej. datos protegidos con contraseñas) y la necesidad de conectarse a una red particular para extraer los datos.

b) Definir en la estructura orgánica de la entidad quien será la persona responsable de llevar a cabo el procedimiento de extracción. Debe ser un profesional experto en recursos tecnológicos o ingeniero de soporte[27], debido al profundo conocimiento que se requiere sobre los aparatos electrónicos *(hardware*) y los sistemas operativos (*software*). El experto debe estar acompañado al menos de otro funcionario de la entidad, quien fungirá como testigo del procedimiento[28].

c) Contar con herramientas informáticas especializadas para asegurar la integridad de la información al momento de ser recolectada. Por ejemplo, programas que permitan copiar todos los datos cambiantes de la memoria de un computador antes de que desaparezcan[29].

d) Evaluar el impacto o la consecuencia de desconectar un dispositivo de línea (internet) o de desvincularlo de la red interna de la entidad por un tiempo prolongado para poder extraer la información.

e) Guardar únicamente los elementos digitales que cuenten con información y prescindir de aquellos que no tengan ningún tipo de datos.

f) Usar herramientas especializadas de extracción de archivos de imágenes, si se deben extraer este tipo de datos (ej. fotografías). Tras la recolección, se debe verificar la integridad de la imagen y compararlos con los de la imagen original, a través de procedimientos forenses adecuados[30].

g) Asegurar y almacenar inmediatamente la información después de extraída y realizar copias de la misma.

h) Hacer copias de la información, si se pretende efectuar verificaciones para comprobar que no haya sufrido alteraciones o modificaciones y sea apta para aportarse como evidencia digital. Se debe evitar hacer verificaciones sobre la información original[31].

---

[27] Los expertos y/o ingenieros que se involucren en el proceso deben acompañar todo el trámite de recolección, aseguramiento y almacenamiento de la evidencia, hasta que la información sea entregada al juez o a un perito experto contratado por la entidad o designado en el proceso judicial.

[28] El o los acompañantes que participan como testigos debe(n) estar presente(s) desde el inicio y a lo largo de todo el procedimiento de recolección.

[29] Información volátil.

[30] Por ejemplo, utilizando el algoritmo SHA1/MD5 para comparar los datos de las dos imágenes y evidenciar alteraciones.

[31] La verificación de la integridad de la información recolectada debe hacerse con herramientas especializadas como, por ejemplo, el cálculo de resumen de los mensajes. Esta herramienta genera un valor determinado que, al compararse, debe ser igual en la fuente original y en la copia de la información extraída. Al respecto, ver: Ministerio de las Tecnologías de la Información y las Comunicaciones. *Seguridad y Privacidad de la Información.* Guía No. 13, "Evidencia Digital", 2016.

i) Detectar si hay algún espacio en el dispositivo o aparato electrónico que guarde información no visible (ej. carpetas ocultas).

j) Siempre que sea posible, recuperar la información borrada y escondida del dispositivo con base en las características técnicas y el estado del sistema en el que reside la información.

k) Estudiar la viabilidad de descifrar o romper la protección, si se recolectan archivos encriptados o protegidos.

l) Llevar un registro de la información encontrada y las actividades desarrolladas durante el proceso. Esto permitirá:

- Contar con un resumen que facilitará hacer el recuento del caso o de los hechos, así como del proceso de extracción en sí.

- Identificar rápidamente la información prioritaria y hacer una línea de tiempo de la evidencia. Para efectos de la reconstrucción de los hechos, se debe tener en cuenta que la evidencia digital puede manejar varias estampas o atributos de tiempo, tales como fecha de modificación, fecha de acceso, fecha de creación, entre otras.

m) Dejar constancia del procedimiento de extracción de la información en un 'Acta de Recolección de Evidencias Digitales'. Para ello, debe considerarse:

- Describir detalladamente el proceso de recolección e incluir:

  ✓ Cargo y especialidad de la persona encargada de la recolección.

  ✓ Estado en el que se encontró el dispositivo y los mensajes de datos.

  ✓ Herramientas tecnológicas utilizadas para la recolección.

  ✓ Paso a paso de las actividades realizadas durante el procedimiento de recolección de evidencias.

  ✓ Evidencias fotográficas de todo el proceso de recolección. Es importante que en el registro fotográfico se pueda observar a quienes participaron en la diligencia e identificar su rol.

- Verificar que todos los involucrados (participantes directos y testigos) comparezcan, suscriban y firmen el acta[32].

[32] Estos participantes pueden ser convocados a testimoniar en el eventual proceso judicial para explicar las acciones y procedimientos que desarrollaron o presenciaron durante la etapa de recolección de evidencias.

2.3. **Etapa de aseguramiento**. Consiste en proteger los mensajes de datos para garantizar la integridad de la información recolectada, con el fin de evitar incidencias y/o alteraciones sobre la evidencia. Para el efecto, se recomienda a las entidades:

a) Utilizar mecanismos especializados, ejecutados por expertos tecnológicos, para asegurar la información en forma de mensajes de datos[33].

b) Garantizar que los mecanismos utilizados conserven inalterados los mensajes de datos, hasta el proceso judicial o actuación administrativa en la que se pretende hacer valer como prueba.

2.4. **Etapa de almacenamiento**. Consiste en guardar los mensajes de datos extraídos y asegurados en condiciones propicias para su preservación hasta el momento en que deban presentarse a la actuación administrativa o judicial[34]. Para ello, las entidades deben:

a) Almacenarlos en (i) medios digitales, por ejemplo, a través de sistemas de almacenamiento en la red y programas de archivos compartidos *'filesharing';* o (ii) en soportes físicos, como memorias USB, discos duros, CD's, entre otros.

b) Garantizar la seguridad del empaque en el que se guardará el soporte o dispositivo físico (ej. USB, disco duro, etc.) que almacena la información. Para el efecto, se recomienda que el empaque:

- Evite daños por efectos ambientales como polvo, temperatura, humedad y salinidad.

- Este sellado de modo que sea evidente cualquier alteración que intente afectar el embalaje. Pueden incorporarse sellos de seguridad con logos de la entidad pública.

- Guardarse en un sitio con las medidas de seguridad que garanticen que sean limitadas las personas con acceso a la información, para mitigar el riesgo de que la evidencia sea alterada y/o eliminada por usuarios o personas no autorizadas.

c) Considerar que acceder a la evidencia digital con posterioridad a su almacenamiento puede conllevar a cambios en fechas de acceso, modificaciones y otras alteraciones de la

[33] Para el efecto, puede recurrirse a herramientas como el estampado cronológico (Cfr. Artículo 3 del Decreto 333 de 2014, compilado en el Artículo 2.2.2.48.1.3. del D.U.R. 1074/2015), la encriptación, el cifrado, los sellos de tiempo, entre otros.
[34] El artículo 18 del Decreto 2609 de 2012 dispone que los sistemas de archivo electrónico implementados en las entidades públicas deben garantizar la autenticidad, integridad, confidencialidad y la conservación a largo plazo de los documentos electrónicos, así como su disponibilidad, legibilidad (visualización) e interpretación, independientemente de las tecnologías utilizadas en la creación y almacenamiento de los documentos. Además, los artículos 22 y 23 del mencionado Decreto establecen, respectivamente, la responsabilidad para las entidades públicas en materia de gestión de documentos electrónicos y las características de los documentos electrónicos para efectos de su gestión documental o archivo.

información, si no se utilizan adecuadamente elementos que la bloqueen o herramientas especializadas que garanticen su inalterabilidad[35].

2.5. **Etapa de entrega de la evidencia digital**. Consiste en aportar los mensajes de datos a la actuación administrativa o judicial en la que se pretenden hacer valer como evidencia digital. Para ello, las entidades deben:

a) Entregar el soporte físico en el que se almacenó la evidencia (ej. USB, CD, etc.) o, si la actuación lo permite, enviar la información por un canal digital (ej. correo electrónico, "filesharing", carpetas compartidas en línea, etc.).

b) Preservar la originalidad del mensaje de datos y garantizar su confiabilidad a quienes la reciben[36].

c) Realizar copias de respaldo del procedimiento de entrega y de la información.

d) Entregar constancias de la cadena de custodia de la evidencia digital.

3. **Cadena de custodia[37].** Consiste en garantizar (i) que la información o evidencia está intacta al momento de presentarse; (ii) que la hora y fecha en la que se hace entrega al proveedor o las autoridades sea exacta y (iii) que no fue manipulada o alterada[38]. Esto se logra con el cumplimiento de las diferentes etapas señaladas anteriormente. Para ello, las entidades deben:

a) Verificar que las personas que intervienen estén en todo el procedimiento de adquisición de la información, desde la identificación hasta el almacenamiento, y dejen las correspondientes constancias.

---

[35] Comúnmente a estos instrumentos se les denomina "elementos" o "sistemas" de bloqueo.

[36] La Corte Constitucional ha explicado que la confiabilidad del mensaje de datos radica en su integralidad, inalterabilidad, rastreabilidad, recuperabilidad y conservación. Estos elementos se explican en los siguientes términos: "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" Corte Constitucional. Sentencia C-604 de 2016. M.P. Luis Ernesto Vargas Silva.

[37] El CGP y CPACA no reglan la cadena de custodia. Sin embargo, la Ley 906 de 2004 (CPP) en el artículo 254 define y determina el alcance de la cadena de custodia de la siguiente manera: *"APLICACIÓN. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos. | La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente. | PARÁGRAFO. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos"*. Esta norma y el Manual de Procedimientos para Cadena de Custodia expedido por la Fiscalía General de la Nación pueden aplicarse como una buena práctica a procesos diferentes al ámbito penal. El fundamento para aplicar esta reglamentación a otro tipo de procesos consiste en que la prueba debe ser custodiada o preservada para garantizar su autenticidad e integridad. De esta manera, al custodiar el material probatorio se podrá demostrar al juez que la prueba fue recolectada y traída al proceso sin ninguna alteración que le reste mérito.

[38] Ministerio de las Tecnologías de la Información y las Comunicaciones. *Seguridad y Privacidad de la Información.* Guía No. 13, "Evidencia Digital", 2016.

b) Designar a un profesional experto en recursos tecnológicos o ingeniero de soporte de la entidad como responsable de ingresar y mantener bajo cadena de custodia la información recolectada.

c) Asegurar la preservación tanto del soporte físico donde reposa la evidencia digital (computadores, USB, entre otros), como de la integridad de los mensajes de datos, para garantizar su plena validez jurídica y probatoria.

d) Registrar e identificar a todas las personas que tienen contacto con la evidencia desde su recolección hasta la entrega y señalar su identidad, estado original, condiciones de recolección, preservación, embalaje y envío de la evidencia.

e) Documentar la información de la cadena de custodia ligada a la evidencia digital e incluir:

- Hoja de ruta que contenga:

  ✓ Descripción general de los mensajes de datos.
  ✓ Datos principales sobre el lugar y forma de custodia, incluyendo ubicaciones, espacios, fechas, horas, etc.
  ✓ Identificación de los custodios, con cargos y firmas de quien recibe y quien entrega.

- Registros de entradas y salidas.

- Rótulos o etiquetas que están pegados al empaque de la evidencia (si aplica).

f) Validar que todos los involucrados suscriban el 'Acta de Recolección de Evidencias Digitales'.

g) Verificar que la custodia de la información se mantenga hasta el momento que se realice la entrega de la evidencia digital al juez, o a un perito designado por la entidad o en el marco del eventual proceso. Esta verificación corresponde al abogado defensor que represente los intereses litigiosos de la entidad en conjunto con el experto informático.

III. Los mensajes de datos como evidencia digital en los procesos judiciales

1. La evidencia digital tiene unas características particulares que la diferencian de las pruebas tradicionales, en tanto es: (i) volátil[39], (ii) eliminable[40], (iii) duplicable[41], (iv) anónima[42] y (v)

[39] Puede desaparecer perderse si no se recolecta de oportunamente.
[40] Puede ser eliminada por una acción voluntaria o involuntaria de quien la accede, manipula o custodia.
[41] Se pueden generar duplicados por medio de procedimientos forenses.
[42] Hay dificultad de vincularla mediante un nexo causal directo al sujeto relacionado, lo que -en ocasiones- vuelve complejo verificar la autenticidad.

alterable o modificable[43]. Lo anterior, amerita que su tratamiento probatorio esté sujeto a unas normas especiales en sede judicial.

2. Los mensajes de datos tienen plena admisibilidad y fuerza probatoria[44]. Se valoran de conformidad con las reglas de la sana crítica, teniendo en cuenta, entre otros factores, la confiabilidad en (i) la forma en la que se haya generado, archivado o comunicado el mensaje; (ii) la forma en que se haya conservado la integridad de la información; y (iii) la forma en la que se identifique a su iniciador[45].

3. El Código General del Proceso no hace referencia explícita a los mensajes de datos como un medio de prueba autónomo, sino que lo subsume en la categoría de prueba documental[46]. Por tanto, les resultan aplicables las normas probatorias sobre documentos[47], sin perjuicio de las disposiciones especiales sobre mensajes de datos que se aplicarán de forma prevalente.

4. Cuando los abogados defensores del Estado pretendan hacer valer o controvertir mensajes de datos en el curso de procesos judiciales o arbitrales deben:

4.1. Solicitar y aportar la evidencia digital a los procesos judiciales y arbitrales en las oportunidades procesales pertinentes[48]. La incorporación de mensajes de datos se podrá

---

[43] Puede ser objeto de manipulación por parte de terceros.

[44] Artículo 10 de la Ley 527 de 1999 "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 *[debe entenderse Código General del Proceso]*. | 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 en razón de no haber sido presentado en su forma original." Ver también arts. 55 y 216 del CPACA.

[45] Artículo 11 de la Ley 527 "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." Adicionalmente, el artículo 247 del CGP dispone: "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."

[46] Cfr. Artículos 165 y 243 del CGP.

[47] Entre esas disposiciones está -y tal vez es la más importante- la regla de presunción de autenticidad de los documentos (art. 244 CGP), que hace expresa referencia a los mensajes de datos.

[48] En el proceso contenciosos administrativo, el artículo 212 del CPACA establece sobre las oportunidades probatorias: "Artículo 212. Oportunidades probatorias. Para que sean apreciadas por el juez las pruebas deberán solicitarse, practicarse e incorporarse al proceso dentro de los términos y oportunidades señalados en este Código. | En primera instancia, son oportunidades para aportar o solicitar la práctica de pruebas: la demanda y su contestación; la reforma de la misma y su respuesta; la demanda de reconvención y su contestación; las excepciones y la oposición a las mismas; y los incidentes y su respuesta, en este último evento circunscritas a la cuestión planteada.
Las partes podrán presentar los dictámenes periciales necesarios para probar su derecho, o podrán solicitar la designación de perito, en las oportunidades probatorias anteriormente señaladas. | En segunda instancia, cuando se trate de apelación de sentencia, en el término de ejecutoria del auto que admite el recurso, las partes podrán pedir pruebas, que se decretarán únicamente en los siguientes casos: 1. Cuando las partes las pidan de común acuerdo. En caso de que existan terceros diferentes al simple coadyuvante o impugnante se requerirá su anuencia. | 2. Cuando fuere negado su decreto en primera instancia o no obstante haberse decretado se dejaron de practicar sin culpa de la parte que las pidió. En este

llevar a cabo por[49]: (i) aporte de la prueba por una de las partes[50]; (ii) decreto de oficio por parte del juez[51]; (iii) inspección judicial[52] y/o (iv) exhibición[53].

4.2. Incorporar la evidencia digital en el formato original (mensaje de datos propiamente dicho) o en una copia impresa (reproducción o copia simple del mensaje de datos)[54]. La incorporación original debe realizarse a través de medios electrónicos con soporte físico o enteramente digitales (ej. dispositivo móvil, USB, grabadora, cámara digital, sistema de almacenamiento en red, enlace de transferencia de archivos, etc.)[55].

4.3. Aportar los soportes que den cuenta de un correcto procedimiento de identificación, recolección, aseguramiento, almacenamiento y entrega del mensaje de datos, así como una adecuada cadena de custodia[56], encaminados a demostrar la confiabilidad de la información.

último caso, solo con el fin de practicarlas o de cumplir requisitos que les falten para su perfeccionamiento. | 3. Cuando versen sobre hechos acaecidos después de transcurrida la oportunidad para pedir pruebas en primera instancia, pero solamente para demostrar o desvirtuar estos hechos. | 4. Cuando se trate de pruebas que no pudieron solicitarse en la primera instancia por fuerza mayor o caso fortuito o por obra de la parte contraria. Sin embargo, es posible que el juez, a su discreción y en cualquier momento, solicite la incorporación oficiosa de las pruebas por considerarlas necesarias para esclarecer el asunto objeto de debate, permitiendo a las partes aportar o solicitar, en el término ejecutoria del auto que decrete la prueba de oficio, nuevas pruebas, en los términos del artículo 213 del CPACA. | 5. Cuando con ellas se trate de desvirtuar las pruebas de que tratan los numerales 3 y 4, las cuales deberán solicitarse dentro del término de ejecutoria del auto que las decreta. | PARÁGRAFO. Si las pruebas pedidas en segunda instancia fueren procedentes se decretará un término para practicarlas que no podrá exceder de diez (10) días hábiles." En materia arbitral, las oportunidades probatorias son las consagradas en el CGP, por ausencia de norma, en los términos del artículo 173 del CGP. Las oportunidades son las siguientes: (i) recurso de reposición contra el auto admisorio; (ii) demanda; (iii) corrección, aclaración y reforma a la demanda; (iv) contestación de la demanda; (iv) contestación a la corrección, aclaración y reforma a la demanda; (v) excepciones de mérito; (vi) traslado de las excepciones; (vii) demanda en reconvención; (viii) contestación de la demanda en reconvención; (ix) trámite de incidentes y (x) traslado del dictamen pericial.

[49] Tanto los aparatos electrónicos como la evidencia digital pueden ser incorporadas a un proceso. Sin embargo, el uso de los dispositivos electrónicos tendrá lugar únicamente cuando se considere necesario probar el medio físico en el que venía contenida la evidencia digital.

[50] Cfr. Artículo 212 del CPACA.

[51] Cfr. Artículo 213 del CPACA.

[52] Cfr. Artículo 236 del CGP.

[53] Cfr. Artículo 265 del CGP.

[54] Es la mera reproducción en un soporte físico de papel de un contenido expresado originalmente a través de dispositivos electrónicos (ej, impresión de un correo electrónico). Si se incorpora en copia, debe justificarse por qué no se aporta el mensaje en el formato original. Será valorada bajo los estándares de la prueba documental (art. 247 CGP), ello implica que tendrá presunción de autenticidad mientras no sea tachada de falsedad o sea desconocida por la otra parte. En el evento de desconocimiento, la parte contra la cual se aduce la prueba deberá demostrar que no fue el iniciador del mensaje de datos. El medio más idóneo para tal fin es el dictamen pericial por parte de un perito experto en informática forense. En todo caso, la parte contra la que se aduzca copia del mensaje de datos podrá solicitar su cotejo con el original, o a falta de este, con otra copia expedida con anterioridad a aquella.

[55] Para el efecto, se debe conocer el formato de generación, envío y/o recepción, para que sea el mismo en el que se entrega a la autoridad judicial. Por ejemplo, si se tiene un documento electrónico que se encuentra en formato XML, debe aportarse en este mismo formato al proceso. En el caso de los correos electrónicos, mensajes de redes sociales o grabaciones deben aportarse en el mismo formato en que se originaron, buscando el soporte físico o medio digital adecuado para cumplir tal finalidad.

[56] Esto se logra, por ejemplo, aportando los registros en los que constan las herramientas y las técnicas de informática forense utilizadas, todo lo cual mostrará que se surtió una adecuada cadena de custodia desde que se extrajo la información hasta que se aportó al proceso judicial.

4.4. Acreditar, al aportar un mensaje de datos y con el fin de que sea valorado como tal[57], el cumplimiento de los siguientes principios probatorios:

a) Conducencia: idoneidad legal del mensaje de datos para demostrar un determinado hecho.

b) Pertinencia: relación directa entre el mensaje de datos y el hecho alegado en el proceso.

c) Utilidad: el mensaje de datos debe ser ampliamente demostrativo para esclarecer o probar con suficiencia el hecho que se alega en el proceso (certeza y convencimiento).

d) Licitud: que el mensaje de datos (i) no sea violatorio de derechos fundamentales y (ii) no incumpla los requisitos formales de la prueba.

e) Legitimidad: el mensaje de datos se debió originar de manera libre y voluntaria, sin que medie dolo, error o violencia (libre de vicios). Además, quien aporta la prueba debe demostrar que la tiene legítimamente y que no es producto de una intromisión indebida en una fuente de evidencia digital.

f) Originalidad: los mensajes de datos deben ser aportados en su forma original, esto es, en el mismo formato en el cual fueron generados, enviados o recibidos, o en algún otro formato que los reproduzca con exactitud[58].

4.5. Cumplir con los estándares y requisitos probatorios inherentes a los mensajes de datos[59]:

a) Disponibilidad de la información[60]: se demuestra mediante la utilización de cualquier programa, formato o herramienta digital (ej. word, visor de imágenes, reproductor de audios, etc.) que permita conocer el contenido del mensaje de datos en el marco de la actuación.

b) Integridad[61]: se acredita mediante la aplicación y registro de procesos de extracción y copia de la información, así como mediante la demostración de que se surtió una adecuada cadena de custodia.

---

[57] Cfr. Artículo 247 del CGP. Sobre el particular, la jurisprudencia ha expresado: "solo si el mensaje electrónico es aportado en el mismo formato en que fue remitido o generado, de un lado, se considerará un mensaje de datos y, del otro, deberá ser probatoriamente valorado como tal" Corte Constitucional. Sentencia C-604 de 2016. M.P. Luis Ernesto Vargas Silva.

[58] Puede utilizarse cualquier método o sistema de almacenamiento de información que permita cumplir dicha condición (ej. disco duro, cintas de medios magnéticos, enlace de 'WeTransfer', etc.).

[59] Cfr. Artículo 11 de la Ley 527 de 1999. En relación con los 3 elementos, ver: C.E., Secc. Quinta, Sent. 2020-00016, dic. 03/2020, C.P.: Lucy Jeannette Bermúdez Bermúdez.

[60] Se refiere a la posibilidad de consultar la información con posterioridad a su creación. Se vincula al adecuado archivo y conservación del mensaje de datos. La jurisprudencia ha indicado que esta noción abarca la integralidad, inalterabilidad, rastreabilidad, recuperabilidad y conservación. Al respecto, ver: Corte Constitucional. Sentencia C-604 de 2016. M.P. Luis Ernesto Vargas Silva.

[61] Demostración de que la información se ha conservado completa e inalterada desde el momento en que se generó por primera vez en su forma definitiva.

c) Autenticidad[62]: se satisface con el aporte de cualquier elemento probatorio que demuestre plenamente que el mensaje de datos corresponde a un sujeto determinado.

5. Tratándose de publicaciones y mensajes de datos intercambiados a través de redes sociales o aplicaciones móviles (ej. Facebook, WhatsApp, Telegram, etc.), para la demostración de los mencionados requisitos probatorios, se recomienda a las entidades, con el apoyo del experto informático, lo siguiente:

a) Frente a la disponibilidad de la información:

- Acreditar la navegabilidad de la página web o aplicación en la que se efectuó la publicación o desde la que se envió el mensaje, mediante un procedimiento informático especializado.

- Acreditar la posibilidad de publicar y/o enviar notas, enlaces, videos, imágenes, mensajes, etc. dentro de la web o red social en relación con el servidor.

- Aportar un video en el que se evidencie el acceso al perfil del originador del mensaje, con el debido registro y constancia de las fechas y horas de la navegación, así como de los rasgos del perfil.

- Recolectar y asegurar la información lo antes posible, para prevenir posibles escenarios de modificación, alteración o eliminación de la publicación o mensaje objeto de controversia.

b) Frente a la integridad del mensaje:

- Asegurar el mensaje de datos con herramientas especializadas, tales como estampado cronológico, encriptado, cifrado, sello de tiempo, función hash o mecanismo semejante, junto con la certificación de la fecha y hora en que la información fue recolectada.

c) Frente a la autenticidad:

- Utilizar todos los elementos que permitan evidenciar que la página o perfil efectivamente corresponde al sujeto o individuo determinado. Debe presentarse evidencia convincente para demostrar con certeza la autoría de un mensaje o publicación (iniciador), no es suficiente la identificación del nombre de la persona o la foto de perfil en una red social o página web.

- Aportar, de ser necesario, un dictamen pericial de un forense informático que:

[62] Verificación de la identidad del iniciador del mensaje de datos.

- ✓ Recolecte e identifique datos únicos e inequívocos de la cuenta o usuario en la página web o aplicación de la red social (ej. fechas, likes, horas, comentarios, etc);

- ✓ Dé cuenta de la existencia de la página o aplicación, de la publicación y/o el mensaje;

- ✓ Contraste los metadatos del mensaje de datos o su contenido con elementos de la realidad del iniciador del mensaje (ej. ubicación geográfica en la fecha y hora en que se tomó una foto).

- Acudir, de ser necesario, a otros medios de prueba tales como:

  - ✓ Declaración de parte sobre la existencia de la página o aplicación, de la publicación y/o el mensaje, si quién realizó la publicación o envió el mensaje funge como demandante o demandado del proceso.

  - ✓ Testimonio que acredite la existencia de la página o aplicación, de la publicación y/o el mensaje por parte de quien tiene conocimiento directo de la autoría.

6. En la mayoría de las ocasiones, basta aportar los mensajes de datos con la muestra de su disponibilidad, integridad y autenticidad, o incluso su copia simple o reproducción, para que se entienda acreditado el hecho que el mensaje de datos pretende probar.

7. No obstante, en caso de que los mensajes de datos por sí mismos no den cuenta de su disponibilidad, integridad y autenticidad, las partes del proceso podrán acudir a un dictamen pericial[63] para demostrar o desvirtuar estos elementos. El dictamen debe ser elaborado por un experto en informática forense y puede utilizarse con el fin de:

7.1. Desvirtuar que un mensaje de datos fue identificado, recolectado, asegurado, almacenado y entregado de forma correcta desde el punto de vista técnico, cuando haya serias razones para dudar del procedimiento surtido.

7.2. Acreditar que un mensaje de datos aportado como prueba ha sido identificado, recolectado, asegurado, almacenado y entregado de forma adecuada desde el punto de vista técnico, cuando los propios elementos del mensaje de datos no sean suficientes para demostrar el cumplimiento de tales requisitos.

7.3. Probar o desvirtuar la ejecución y cumplimiento de la cadena de custodia respecto de un mensaje de datos.

[63] En cuanto a las generalidades de la prueba pericial, los dictámenes y peritos, se recomienda revisar el Lineamiento sobre uso adecuado de la prueba pericial elaborado por la ANDJE, que puede descargar en el siguiente enlace: Lineamiento prueba pericial - Comunidad Jurídica del Conocimiento (defensajuridica.gov.co)

7.4. Cuestionar la confiabilidad de una información (autenticidad, integridad o adecuada disponibilidad -archivo y conservación- de la información en el formato original) aportada como evidencia digital.

7.5. Acompañar la diligencia de exhibición o inspección del mensaje de datos. En tal caso, el perito deberá validar la conformidad del mensaje de datos, sin intervenir o analizar el contenido de la información. Su intervención debe limitarse a los mensajes de datos relacionados con la controversia.

CAMILO GÓMEZ ALZATE
Director General

Revisó: Luis Jaime Salgar Vegalara/Diana Lucía Herrera Riaño
Elaboró: Marco Vita Mesa/María Fernanda Suárez Celly