DOCUMENTO DE 2022

(junio 10)

<Fuente: Archivo interno entidad emisora>

AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

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,

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 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:

- 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].

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].

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.

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.

- 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 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)].

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].

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 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.

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) 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 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.

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.

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:

- 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.

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 ÁLZATE

Director General

<NOTAS DE PIE DE PÁGINA>

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. E ra P(E: (r

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma del Instituto Nacional de Vigilancia de Medicamentos y Alimentos - INVIMA
n.d.
Última actualización: 30 de agosto de 2024 - (Diario Oficial No. 52.847 - 13 de agosto de 2024)