

Bogotá D.C. 9 de enero de 2024

NÚMERO 001

TEMA DE CONSULTA: Comunicaciones Oficiales / Fechas / Firmas

COMPETENCIA:

Previo a resolver la consulta, se señala que de conformidad con el Decreto No. 158 de 2022 *"Por el cual se establece la estructura del Archivo General de la Nación y se determinan las funciones de las diferentes dependencias"*. Es función de la Subdirección de Política y Normativa liderar y consolidar la emisión de conceptos técnicos y/o recomendaciones sobre la implementación de la política archivística.

MOTIVO DE LA CONSULTA:

"solicito información y asesoría jurídica sobre la elaboración o creación y expedición de documentos administrativos-jurídicos en las instituciones del Gobierno Nacional como oficios, memorandos, comunicados oficiales, entre otros, tanto de forma impresa-digital escaneada como en forma electrónica de tipo Firma PKI o Certificado Digital; ya que al encontrar en el encabezado de algún documento institucional una determinada fecha y lugar que luego al ser revisada en el mismo la parte final del documento se le encuentra otra fecha distinta con una determinada fecha de firmado, de ello surgen interrogantes: 1- ¿La fecha que ponen al inicio de un documento es la fecha de creado de un borrador, o es la fecha de elaborado, o es la fecha de revisado, o es la fecha de aprobado para posterior firma, o es la fecha de expedido, o es la fecha de firmado; y cómo se puede interpretar la fecha que muestra al inicio cada documento?; 2- ¿Hay alguna o algunas normatividades que regulen jurídicamente o permita este aspecto de consignar determinadas fechas al inicio de cualquier documento y luego en la parte final del mismo otra fecha distinta?; 3- ¿Eso es normal consignar dos fechas distintas en un documento, o se puede constituir en un delito de Falsedad ideológica en documento público al consignar en el encabezado una fecha antigua y al final del documento firmarlo con otra fecha que puede inducir al usuario lector o usuario final en generarle confusión interpretativa de su fecha de expedido?." (Sic.)

CONSIDERACIONES

Sobre la respuesta, conviene precisar en primer término, que las consultas que se presentan a esta entidad, se resuelven de manera general, abstracta e impersonal, de acuerdo con las funciones conferidas en el ejercicio de las atribuciones de dirección y coordinación de la función archivística del estado

colombiano, expresamente señalada en la Ley 594 de 2000 y se circunscribe a hacer claridad en cuanto al texto de las normas de manera general, para lo cual armoniza las disposiciones en su conjunto, de acuerdo con el asunto que se trate y emite su concepto, ciñéndose en todo a las normas vigentes sobre la materia.

RESPUESTA

Como primer referente normativo colombiano es necesario remitirnos a la Ley 527 de 1999, el cual da los parámetros para la aplicación de los requisitos jurídicos de los mensajes de datos así:

"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 en razón de 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.

Artículo 12. 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:

- a) Que la información que contengan sea accesible para su posterior consulta.*
- b) 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*
- c) 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.*

Artículo 13. Conservación de mensajes de datos y archivo de documentos a través de terceros. El cumplimiento de la obligación de conservar documentos, registros o informaciones en mensajes de datos se podrá realizar directamente o a través de terceros, siempre y cuando se cumplan las condiciones enunciadas en el artículo anterior.

[...]

Artículo 30. Actividades de las entidades de certificación. Las entidades de certificación acreditadas por el Organismo Nacional de Acreditación de Colombia para prestar sus servicios en el país, podrán realizar, entre otras, las siguientes actividades:

- 1. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.*
- 2. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.*
- 3. Emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999.*
- 4. Ofrecer o facilitar los servicios de generación de los datos de creación de las firmas digitales certificadas.*

5. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.
6. Ofrecer o facilitar los servicios de generación de datos de creación de las firmas electrónicas.
7. Ofrecer los servicios de registro, custodia y anotación de los documentos electrónicos transferibles.
8. Ofrecer los servicios de archivo y conservación de mensajes de datos y documentos electrónicos transferibles.
9. Cualquier otra actividad relacionada con la creación, uso o utilización de firmas digitales y electrónicas"

Así mismo, la *Ley General de Archivos* (Ley 594 de 2000) en su artículo 19 menciona:

"Artículo 19. Soporte Documental. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos:

- a. Organización archivística de los documentos.*
- b. Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos como la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.*

Parágrafo 1. Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información. (Resaltado fuera de texto)

Parágrafo 2. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.[...]

Artículo 21. Programas de gestión documental. Las entidades públicas deberán elaborar programas de gestión de documentos, pudiendo contemplar el uso de nuevas tecnologías y soportes, en cuya aplicación deberán observarse los principios y procesos archivísticos. Parágrafo. Los documentos emitidos por los citados medios gozarán de la validez y eficacia de un documento original, siempre que quede garantizada su autenticidad, su integridad y el cumplimiento de los requisitos exigidos por las leyes procesales."

En el artículo 1 del Decreto 2364 de 2012 se define la Firma Electrónica de la siguiente manera:

Firma electrónica. Métodos 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.

El mismo estableció los criterios que le dan confiabilidad a una firma electrónica en el Artículo 4:

Artículo 4°. Confiabilidad de la firma electrónica. La firma electrónica se considerará confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.

2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.

Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona:

1. Demuestre de otra manera que la firma electrónica es confiable; o

2. Aduzca pruebas de que una firma electrónica no es confiable

Por su parte el Decreto 1080 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura” menciona:

Artículo 2.8.2.7.1. Aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos. Es responsabilidad de las Entidades Públicas cumplir con los elementos esenciales tales como: autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y conservación, que garanticen que los documentos electrónicos mantienen su valor de evidencia a lo largo del ciclo de vida, incluyendo los expedientes mixtos (híbridos), digitales y electrónicos. (Resaltado fuera de texto)

Para la implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA, el Archivo General de la Nación ha trabajado los últimos años en la formulación de políticas y documentos técnicos que le permitan a las entidades llevar a cabo la implementación del documento electrónico en la administración, así como la implementación de herramientas tecnológicas que permitan el almacenamiento, uso, permanencia y disposición de documentos de archivo, respondiendo a los criterios de la gestión documental.

Por tal motivo, y para mayor claridad, recomendamos revisar los siguientes documentos elaborados por la entidad:

- **Modelo de requisitos para la implementación de un sistema de gestión de documentos electrónicos:** busca establecer los requisitos mínimos para implementar un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), proponiéndolos como una lista de verificación.

URL:

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Conulte/Recursos/Publicacionees/ModeloDeRequisitosSistemaDeGestionElectronicos.pdf

- **Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA:** propone a las entidades que antes de adquirir una herramienta tecnológica como soporte a la gestión documental electrónica, las organizaciones deben tener claras las necesidades, implicaciones y retos que conllevan a adquirir e implementar una solución informática que apoye los procesos de la gestión documental, basada en la adopción de mejores prácticas y metodologías aplicables durante el ciclo de vida del proyecto.

URL:

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Conulte/Recursos/Publicacionees/V16_Guia_SGDEA.pdf

- **Guía para la gestión de documentos y expedientes de documentos electrónicos:** realizada por un grupo de profesionales del Ministerio de las Tecnologías de la Información

y las Comunicaciones y del Archivo General de la Nación, con el fin de brindar parámetros que permitan, a las entidades públicas y privadas que cumplen funciones públicas, comprender la importancia del documento electrónico de archivo, su estructura y sus características, así como las etapas para su gestión durante todo su ciclo vital, la conformación de los expedientes electrónicos y los elementos que lo integran, incluyendo la gestión de los metadatos mínimos obligatorios.

URL:

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicaciones/DocumentoOficialV1_GuiaDocumentoYExpedienteElectronico26_ENE%202018_v3.pdf

Esta última, menciona algunos aspectos fundamentales para la validación de los documentos electrónicos:

"Para otorgar autenticidad a los documentos electrónicos las entidades pueden hacer uso de las siguientes técnicas:

- a) *Estampas de tiempo: Consiste en una secuencia de caracteres utilizada para certificar el momento específico en que se lleva a cabo un suceso sobre un documento electrónico o que éste no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y hora exacta en que ocurre dicho evento y específicamente cuando fue creado o firmado en un sistema de cómputo. Mediante la emisión de una stampa de tiempo es posible garantizar el instante de creación, modificación, recepción, firma, etc., de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana.*
- b) *Firmas electrónicas: Métodos 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.*
- c) *Firmas digitales: La firma digital se configura como un valor numérico que se asocia a un mensaje de datos y permite determinar que dicho valor ha sido generado a partir de la clave originaria, sin modificación posterior. La firma digital se basa en un certificado seguro y permite a una entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos. Como medida, en el marco de la conservación de los documentos electrónicos a largo plazo, se recomienda la actualización de la firma digital. Esta medida de control consiste en el resellado o la refirma, como medios para prevenir la obsolescencia o la vulneración del sistema de firma. La diferencia entonces es fundamentalmente probatoria, pues si bien la firma digital de manera automática incorpora la autenticidad, integridad y no repudio, en la firma electrónica es necesario probarla, además de determinar que se trata de un mecanismo confiable y apropiado. Nota: Si se trata de una firma biométrica electrónica o electrónica manuscrita, tendrá el mismo valor de una firma electrónica, siempre que cumpla con los requisitos exigidos por los arts. 3º y 5º del decreto 2364 de 2012, sea o no emitida por una entidad certificadora. De lo contrario, si por ejemplo la firma es tomada en un "digital pad" y es fijada en un documento que es impreso, podrá ser tenida como una firma o rubrica común, impuesta mediante un mecanismo electrónico, es decir, una firma de puño y letra del autor, pero fijada, por decirlo así, con tinta electrónica.*

- d) *Certificados digitales: Los certificados digitales se conocen como una parte de la información que se asocia a un mecanismo para acreditar la validez de un documento perteneciente a un autor (autenticación), verificar que no ha sido manipulado ni modificado (integridad), al igual que impide que el autor niegue su autoría (no repudio) mediante validación de la clave pública del autor, quedando de esta manera vinculado al documento de la firma.*
- e) *Código seguro de verificación (CSV): Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente pueden tener la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.*
Nota: El Código seguro de verificación (CSV) es una comprobación de la autenticidad del documento ingresando un código alfanumérico en la sede electrónica correspondiente.
- f) *Marcas de agua digitales: Corresponde a datos incrustados en documentos electrónicos tales como fotografías, películas, audios, y otros contenidos digitales y constituyen un medio seguro para certificar el origen, propiedad y autenticidad de los activos digitales.*
Nota: Los mecanismos de seguridad "per-se" no garantizan la autenticidad."¹

Así las cosas, la Ley 527 de 1999, la Ley 594 de 2000 y el Decreto 1080 de 2015, exigen que los documentos electrónicos, ya sean producidos de manera nativa o mediante un proceso de digitalización, cuenten con unas características técnicas para que puedan ser considerados con valor probatorio; las más importantes son: Autenticidad, Integridad, Fiabilidad, Disponibilidad. Para ello es necesario utilizar tecnologías como: las firmas electrónicas o digitales, los estampados cronológicos, aplicación de Hash, Sistemas de Gestión de Documento Electrónico de Archivo que cuenten con logs de auditoría, Repositorios Digitales que estén orientados a la preservación digital a largo plazo, etc.

Cada entidad, empresa u organización que quiera darle autenticidad a sus documentos electrónicos de archivo mediante firmas electrónicas, debe realizar el estudio respectivo que busque analizar el cumplimiento de la norma mencionada en relación con el tipo de firma electrónica a usar, situación que debe realizarse para cada tipología documental que se considere digitalizar, dependiendo de los valores primarios que la misma tenga y las posibilidades de que sea utilizada como evidencia o prueba ante una autoridad judicial, gubernamental o de control. Adicionalmente son estas instancias quienes en últimas deciden si un documento electrónico de archivo tiene las características de autenticidad, fiabilidad, integridad y disponibilidad que lo avale como con valor probatorio.

¹ Archivo General de la Nación y Ministerio de Tecnologías de la Información y las Comunicaciones "G.INF.07 Guía para la gestión de documentos y expedientes electrónicos" Bogotá, 2018, pp. 18-20.

Respecto a la fechas, es importante tener presente que son distintos los momentos de gestión de los documentos (proyección, revisión, aprobación, firma, remisión), no obstante, para el caso de los documentos electrónicos de archivo se debe tener en cuenta la fecha en la que el documento se declara como documento de archivo, es decir, cuando se produzca alguna acción que lo reconozca como documento de archivo, por ejemplo: una firma o una estampa cronológica², con la cual se le da total validez al documento a partir de la competencia funcional del servidor público encargado de la firma.

Por los tanto, la fechas en los documentos electrónicos que son tramitados en un sistema de gestión de documentos electrónicos de archivos deben coincidir, tanto la fecha que se encuentra en la parte superior como la fecha de la firma del documento. En caso de presentarse alguna diferencia, la fecha que deberá tenerse en cuenta es la fecha de la firma del documento dado que es ese el momento en el cual se declara como documento de archivo, y no constituye un delito de falsedad.

En los anteriores términos se absuelve la consulta planteada, la cual debe considerarse dentro de los parámetros establecidos en el Código Contencioso de Procedimiento administrativo y de lo Contencioso Administrativo, artículo 28, del Título II, Derecho de Petición, capítulos I, II y III, sustituidos por la Ley 1755 de 2015, sobre el Alcance de los Conceptos.

Atentamente,

YENNI MARCELA GASCA MUETE

Subdirectora

Subdirección de Política y Normativa Archivística

Anexos: N/A

Copia: N/A

Proyecto: Diego Alejandro García Jiménez – Profesional especializado - SPA

Revisó: Yenni Marcela Gasca Mueete – Subdirectora - SPA

Archivado en: 300.08.04 - Conceptos Técnicos

² Archivo General de la Nación y Ministerio de Tecnologías de la Información y las Comunicaciones “G.INF.07 Guía para la gestión de documentos y expedientes electrónicos” Bogotá, 2018, pp.51-52