

**Al contestar por favor cite este número
Radicado N° 202601400014433**

COMUNICACIÓN INTERNA

Bogotá D.C, Martes, 28 de Julio de 2026

PARA: Henry David Ortiz Saavedra
Subdirector Tecnio
SUBDIRECCIÓN DE GESTIÓN CORPORATIVA

ASUNTO: Validez, eficacia probatoria y alcance de la firma electrónica implementada en la plataforma SIGMA para actuaciones internas de la Entidad. / Radicado 202604000014203.

Respetado doctor Ortiz

La Oficina Jurídica procede a resolver la consulta formulada por la Subdirección de Gestión Corporativa sobre la utilización de la firma electrónica disponible en el Sistema de Gestión Documental SIGMA, con fundamento en los antecedentes y documentos allegados, conforme se indica a continuación:

I. ANTECEDENTES

De la solicitud y sus anexos se extraen los siguientes antecedentes relevantes:

1. La Región Metropolitana Bogotá-Cundinamarca utiliza SIGMA para la gestión, trámite y conservación de documentos electrónicos institucionales.
2. La dependencia informa que, para la suscripción de comunicaciones y trámites internos, se ha utilizado firma digital con estampa cronológica y que se han generado aproximadamente mil cuatrocientos documentos.
3. Con el propósito de optimizar la gestión documental se propone habilitar, para determinadas actuaciones internas, una firma electrónica asociada al perfil individual del usuario en SIGMA.
4. Según la información aportada, el mecanismo requiere credenciales de acceso y un PIN remitido al correo institucional. La estampa visible incorpora el nombre, cargo y dependencia del firmante, así como datos temporales de la actuación.
5. Los anexos permiten observar solicitudes de firma, aprobaciones, rechazos, cargas y modificaciones del documento, además de registros sobre usuarios, fechas y horas dentro del historial del sistema.



Correo institucional:

contactenos@regionmetropolitana.gov.co
NIT: 901665578-7



Dirección:

Avenida Calle26 #57-83,
Edificio CEMSA Torre 8 / Piso 15



Teléfono Commutador:

+57 (601) 7431943

La dependencia solicita determinar: (i) la validez jurídica de la firma electrónica; (ii) su eficacia y fuerza probatoria; (iii) los requisitos de legitimidad, autenticidad y confiabilidad; (iv) los documentos internos susceptibles de suscripción por este medio, y (v) el ajuste del mecanismo de SIGMA a la normativa vigente.

II. PROBLEMAS JURÍDICOS

A partir de la consulta, la Oficina Jurídica identifica los siguientes problemas:

¿Puede la firma electrónica generada mediante SIGMA satisfacer válidamente el requisito de firma en las actuaciones internas de la Entidad?

En caso afirmativo, ¿qué condiciones jurídicas, técnicas, probatorias y archivísticas deben acreditarse, y para qué clases de documentos resulta apropiado su uso?

Para resolverlos se estudiarán la equivalencia funcional de los mensajes de datos; la diferencia entre firma electrónica y firma digital; la confiabilidad exigida por el ordenamiento; el uso de firmas en la actividad pública; su eficacia probatoria y documental, y la aplicación de estas reglas al mecanismo de SIGMA.

III. CONSIDERACIONES

1. Alcance del concepto

La Oficina Jurídica se pronuncia sobre el marco normativo aplicable y las condiciones que debe observar la Entidad. La evaluación se basa exclusivamente en la solicitud y en las evidencias aportadas. Por consiguiente, no sustituye la validación técnica de seguridad de la información, la prueba funcional del sistema, el análisis de riesgos ni la certificación que corresponda al administrador o proveedor de SIGMA.

La viabilidad jurídica del mecanismo debe distinguirse de la comprobación de su cumplimiento técnico. La primera puede establecerse mediante este concepto; la segunda requiere evidencias especializadas que demuestren cómo se autentica al usuario, cómo se vincula la aprobación con la versión exacta del documento y cómo se detectan modificaciones posteriores.

2. Equivalencia funcional de los mensajes de datos

La Ley 527 de 1999 [\[1\]](#) reconoce que la información no puede ser privada de efectos jurídicos por el solo hecho de encontrarse en forma de mensaje de datos. Sus artículos 6, 7 y 8 establecen los



criterios para que un mensaje satisfaga los requisitos de escrito, firma y original.

Cuando una disposición exige la firma de una persona, el artículo 7 considera satisfecho el requisito si se utiliza un método que permita identificarla y expresar su aprobación del contenido, siempre que el método sea confiable y apropiado para la finalidad y las circunstancias. La equivalencia funcional no depende de reproducir visualmente una firma manuscrita, sino de cumplir las funciones jurídicas de identificación, aprobación e integridad.

Por lo mismo, la estampa gráfica incorporada en el documento de SIGMA es un elemento informativo, pero no constituye por sí sola la firma electrónica ni demuestra su confiabilidad. El análisis debe abarcar el proceso completo de autenticación, aprobación, vinculación con el mensaje, control de integridad y conservación de la evidencia.

3. Firma electrónica y firma digital

La firma electrónica y la firma digital son mecanismos jurídicamente admitidos, pero no son expresiones intercambiables. La firma electrónica es una categoría amplia que comprende métodos como códigos, contraseñas, datos biométricos o claves criptográficas privadas, siempre que permitan identificar al firmante en relación con un mensaje de datos y sean confiables y apropiados para su finalidad.

La firma digital es una modalidad específica definida por la Ley 527 de 1999 como un valor numérico adherido al mensaje mediante un procedimiento matemático vinculado con la clave del iniciador. Cuando reúne los atributos del artículo 28 de esa ley [\[2\]](#), tiene la misma fuerza y efectos de la firma manuscrita y se beneficia de las presunciones allí previstas.

Esta distinción tiene dos consecuencias. Primero, la firma electrónica de SIGMA no pierde validez por no corresponder a una firma digital certificada. Segundo, tampoco puede atribuírsele automáticamente el régimen probatorio especial de esta última: su confiabilidad debe demostrarse atendiendo las características concretas del método utilizado.

En concordancia con lo anterior, el Departamento Administrativo de la Función Pública, mediante el Concepto 174501 de 2022 [\[3\]](#), señaló que la suscripción de documentos mediante mecanismos digitales resulta jurídicamente viable cuando se cumplen los requisitos y protocolos aplicables. Asimismo, destacó la importancia de garantizar la identificación del firmante, el control sobre el mecanismo utilizado, su vinculación con el mensaje, y la integridad, autenticidad, disponibilidad y conservación de la información. Estos criterios resultan pertinentes para SIGMA, particularmente respecto de la protección de credenciales, la identificación del usuario, la asociación de la firma con la versión exacta del documento y la detección de cambios.



4. Confiabilidad de la firma electrónica

Los artículos 2.2.2.47.1 a 2.2.2.47.8 del Decreto 1074 de 2015 [4] regulan la firma electrónica. De acuerdo con el artículo 2.2.2.47.4, se considera confiable cuando los datos de creación corresponden exclusivamente al firmante, en el contexto en que se utilizan, y cuando es posible detectar cualquier alteración no autorizada del mensaje realizada después de la firma.

La norma permite probar la confiabilidad por cualquier medio admisible y reconoce los acuerdos sobre el uso del mecanismo. Sin embargo, la parte que pretenda hacerlo valer conserva la carga de demostrar su validez y confiabilidad. De ahí que la Entidad deba conservar un conjunto probatorio suficiente, integrado por el documento, sus metadatos, los registros de autenticación, la manifestación de aprobación, la huella de integridad, las bitácoras y la evidencia temporal.

5. Firmas electrónicas y digitales en la actividad pública

El Decreto 1789 de 2021 adicionó los artículos 2.2.2.47.9 y 2.2.2.47.10 al Decreto 1074 de 2015. El primero dispone la utilización de firmas electrónicas o digitales por servidores públicos y particulares que ejercen funciones públicas o administrativas, en el marco de la transformación digital.

La habilitación no es uniforme ni automática para todos los procesos. La autoridad debe determinar previamente el grado de confianza requerido —muy alto, alto, medio o bajo— según la naturaleza del proceso y los lineamientos de autenticación digital. Esta exigencia obliga a valorar la finalidad del documento, sus efectos jurídicos, el impacto de una suplantación o alteración, la sensibilidad de la información y las consecuencias administrativas, contractuales, presupuestales, laborales o frente a terceros.

La decisión institucional no debe recaer genéricamente sobre todas las «actuaciones internas». Debe existir una clasificación por procesos, trámites o series documentales, que permita asignar el mecanismo de firma proporcionado al riesgo.

6. Eficacia probatoria y gestión documental

Los artículos 10 y 11 de la Ley 527 de 1999 reconocen la admisibilidad de los mensajes de datos y ordenan valorar su fuerza probatoria conforme a la sana crítica, teniendo en cuenta la confiabilidad de su generación, archivo y comunicación, la conservación de la integridad, la identificación del iniciador y los demás factores relevantes.



Los artículos 53 a 59 [\[5\]](#) del Código de Procedimiento Administrativo y de lo Contencioso Administrativo admiten el empleo de medios electrónicos en la actuación administrativa. En particular, el artículo 55 reconoce validez y fuerza probatoria a los documentos públicos autorizados o suscritos electrónicamente.

El Acuerdo 001 de 2024 del Archivo General de la Nación exige que los documentos y expedientes electrónicos mantengan autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y preservación durante su ciclo de vida. En consecuencia, la evidencia de la firma debe incorporarse al expediente, asociarse a los metadatos y conservarse conforme a las tablas de retención y al plan de preservación digital.

7. Análisis del caso concreto

Los documentos aportados muestran elementos favorables: asociación del trámite con usuarios identificados; empleo de credenciales y de un PIN; manifestaciones de aprobación o rechazo; registro del nombre, cargo y dependencia; datos de fecha y hora, e historial de actuaciones.

Tales elementos permiten considerar que SIGMA dispone de una base funcional susceptible de configurar una firma electrónica. No obstante, las capturas y el historial no acreditan por sí solos la totalidad de las condiciones de confiabilidad.

La Entidad debe verificar y documentar, al menos, los siguientes aspectos: carácter personal, exclusivo y no reutilizable de las credenciales y del PIN, vigencia limitada y entrega mediante canal controlado; administración del ciclo de vida de los usuarios: creación, modificación, suspensión y retiro oportuno; presentación al firmante de la versión completa y definitiva antes de expresar su aprobación; vinculación inequívoca de la firma con esa versión, huella digital u otro control verificable; bloqueo o detección de toda modificación posterior y reinicio del flujo cuando cambie el documento; integridad, inalterabilidad, disponibilidad y exportación de las bitácoras de auditoría; fuente horaria sincronizada y conservación de fecha, hora y zona horaria; verificabilidad del documento y de su evidencia fuera de la sesión de SIGMA y durante el periodo de retención; segregación de funciones, copias de seguridad, continuidad, gestión de incidentes y auditorías periódicas.

El historial evidencia varias cargas o modificaciones de la imagen principal antes de la firma final. Esta circunstancia no invalida el trámite, pero hace indispensable que el sistema identifique técnicamente cuál fue la versión sometida a aprobación y permita detectar cualquier cambio posterior.

La utilización puede autorizarse inicialmente para vistos buenos, revisiones, remisiones,



memorandos, solicitudes, instrucciones, constancias y aprobaciones internas de riesgo ordinario que no creen por sí solas obligaciones frente a terceros. Los actos administrativos internos, decisiones de personal, certificaciones, informes de supervisión, autorizaciones contractuales, presupuestales o financieras requieren evaluación reforzada.

Los contratos, convenios, actos dirigidos a terceros, operaciones financieras, garantías y documentos sometidos a solemnidad o a una exigencia especial no quedan habilitados automáticamente. Para ellos debe revisarse la normativa particular y conservarse la firma digital u otro mecanismo de mayor aseguramiento cuando así se exija o lo determine el análisis de riesgo.

En síntesis, la firma electrónica de SIGMA es jurídicamente viable, pero su implementación debe ser gradual y condicionada a: (i) informe técnico; (ii) evaluación del grado de confianza por proceso; (iii) política institucional de uso; (iv) matriz de documentos y firmas; (v) piloto para actuaciones de bajo riesgo, y (vi) integración con la gestión y preservación documental.

IV. LA OFICINA JURÍDICA RESPONDE

Con fundamento en las consideraciones precedentes, se responden los interrogantes formulados:

1. ¿La firma electrónica generada a través de SIGMA tiene validez jurídica para suscribir documentos institucionales utilizados en actuaciones internas?

Sí. Puede satisfacer válidamente el requisito de firma cuando permita identificar al firmante, evidencie su aprobación del contenido, sea confiable y apropiada para la finalidad, y permita detectar alteraciones posteriores. Su validez no proviene de la estampa visible, sino del funcionamiento integral y demostrable del mecanismo.

2. ¿Cuál es su eficacia y fuerza probatoria?

El documento electrónico es admisible como prueba. Su fuerza probatoria dependerá de la confiabilidad de su generación, conservación y comunicación; de la integridad de la información; de la identificación del firmante, y de la evidencia disponible sobre el proceso de suscripción. La firma electrónica no recibe automáticamente todas las presunciones específicas de la firma digital.

3. ¿Qué requisitos deben acreditarse para garantizar su autenticidad y confiabilidad?

Deben acreditarse la identificación y autenticación individual; el control exclusivo de los datos de creación; la manifestación inequívoca de aprobación; la vinculación con la versión exacta; la detección de alteraciones; bitácoras íntegras; fecha y hora confiables; conservación, disponibilidad



y preservación; política de uso; gestión de usuarios y riesgos, y evidencia técnica suficiente para probar estas condiciones.

4. ¿Qué documentos o actuaciones internas pueden suscribirse mediante esta firma?

Prioritariamente, documentos internos de trámite o de riesgo ordinario. Las actuaciones decisorias, contractuales, presupuestales, financieras, laborales o con efectos frente a terceros exigen evaluación específica y reforzada. Cuando exista una solemnidad, exigencia normativa o nivel de riesgo superior, deberá utilizarse firma digital u otro mecanismo idóneo.

5. ¿El mecanismo implementado en SIGMA se ajusta actualmente a las disposiciones vigentes?

La evidencia aportada permite apreciar elementos de autenticación, aprobación y trazabilidad, pero no es suficiente para afirmar el cumplimiento técnico integral de los requisitos de exclusividad y detección de alteraciones. El ajuste normativo definitivo queda condicionado al informe técnico, la evaluación del grado de confianza, la política institucional, la matriz de usos y las pruebas del sistema indicadas en este concepto.

El presente concepto se emite en los términos del artículo 28 de la Ley 1437 de 2011 y, por tanto, constituye una orientación jurídica que no es de obligatorio cumplimiento o ejecución.

Cordialmente,

[1] Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

ARTICULO 6o. 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.

ARTICULO 7o. 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.

ARTICULO 8o. 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.

[2] ARTICULO 28. ATRIBUTOS JURIDICOS DE UNA FIRMA DIGITAL. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

PARAGRAFO. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

[3] Concepto 174501 de 2022 Departamento Administrativo de la Función Pública REF: ENTIDADES. Validez de las firmas digitales. RAD. 20222060132702 del 23 de marzo de 2022

[4] Por el cual se reglamenta el artículo 18 de la Ley 2069 de 2020 y se adicionan los artículos 2.2.2.47.9 y 2.2.2.47.10 al Decreto 1074 de 2015, en lo relacionado con el uso de la firma electrónica y digital como una herramienta para facilitar la innovación y la transformación digital"

[5] CAPÍTULO IV. Utilización de medios electrónicos en el procedimiento administrativo

Gotardo Antonio Yáñez Álvarez

Jefe Oficina Jurídica

OFICINA JURÍDICA

Proyectó: Gian Carlo Suescún Sanabria - OFICINA JURÍDICA



Correo institucional:

contactenos@regionmetropolitana.gov.co
NIT: 901665578-7



Dirección:

Avenida Calle26 #57-83,
Edificio CEMSA Torre 8 / Piso 15



Teléfono Commutador:

+57 (601) 7431943