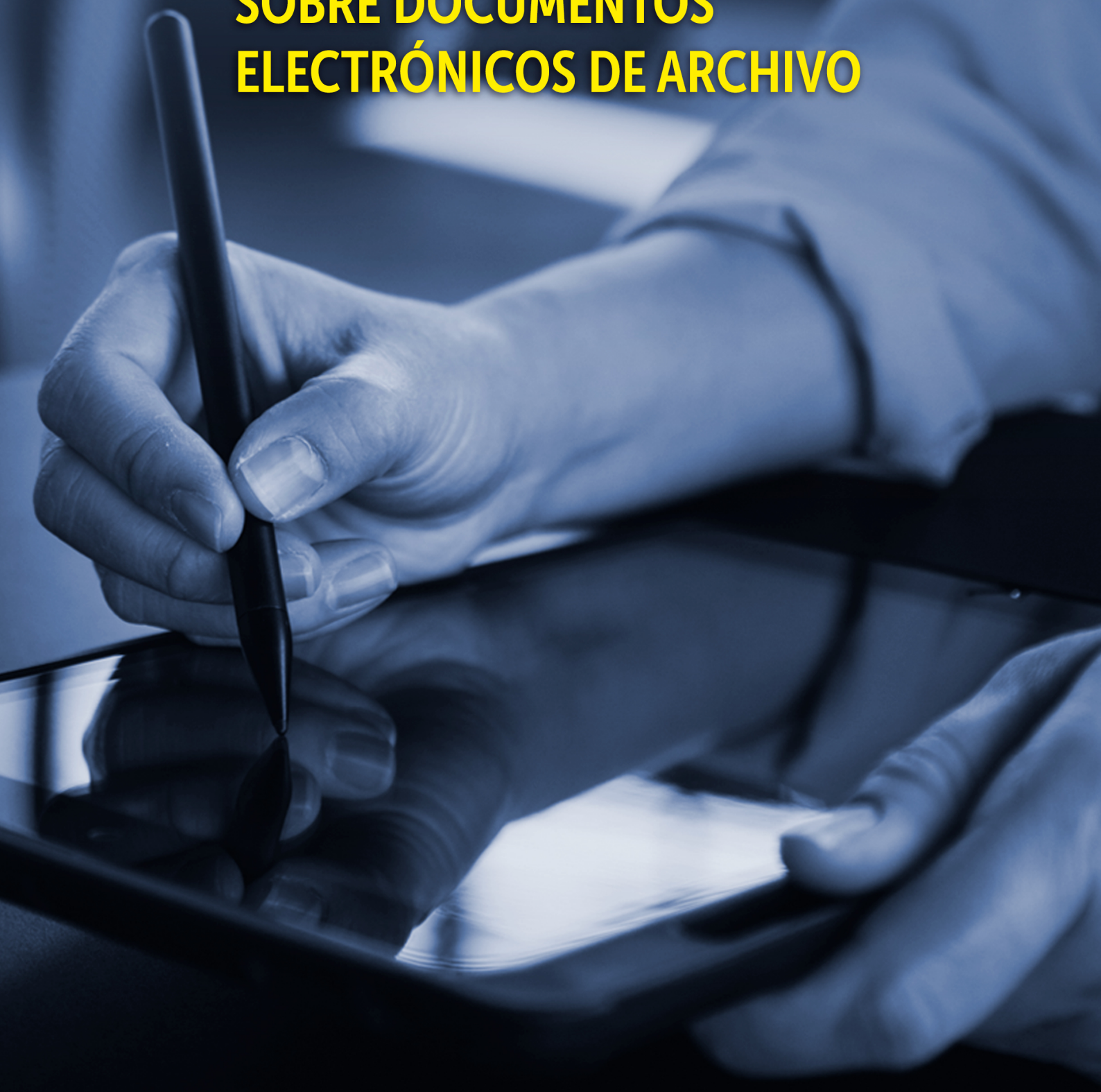


GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO





GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Documento digital

© **Secretaría General de la Alcaldía Mayor de Bogotá D.C.**

Cualquier reproducción debe ser previa y expresamente autorizada.

Dirección Distrital de Archivo de Bogotá / Calle 6B # 5-75 / PBX 601 381 30 00 ext. 4113

<https://archivobogota.secretariageneral.gov.co>

Primera edición: Bogotá D.C., 2026

Coordinación general

Jorge Enrique Cachiotis Salazar
Director Dirección Distrital de Archivo de Bogotá

Diego Alejandro García Jiménez
Subdirector del Sistema Distrital de Archivos

Alix Johana Guzmán
Subdirector del Sistema Distrital de Archivos

Elaboración técnica

Equipo técnico de la Subdirección del Sistema Distrital de Archivos

Diana Patricia Bula Guzmán, Jessica Inés Pinzón Ducuara, John Alexander Pulido Chaparro, Marly Yolie Quintana Daza, Nancy Angélica Rodríguez Marín, Wilson Ramiro Sánchez Yopaza

Revisión técnica

Oficina Consejería Distrital de Tecnologías de información y las comunicaciones - TIC

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Contenido

1	INTRODUCCIÓN.....	1
2	OBJETIVO	2
3	ALCANCE	2
4	CONCEPTOS BÁSICOS.....	2
5	PRINCIPIOS ORIENTADORES.....	13
6	CONTEXTO INSTITUCIONAL	16
7	HOJA DE RUTA PARA LA ADOPCIÓN E IMPLEMENTACIÓN DE FIRMAS ELECTRÓNICAS DIGITALES.....	17
8	PLANEACIÓN DE LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES	18
8.1.1	Propósito de la fase de planeación.....	18
8.1.2	Alistamiento institucional y definición del alcance.....	19
8.1.3	Revisión normativa y marco de referencia aplicable	22
8.1.4	Diagnóstico de producción documental electrónica.....	24
8.1.5	Caracterización y priorización de tipos documentales sujetos a firma e identificación de firmantes responsables.....	29
8.1.6	Criterios para definir el mecanismo de firma.....	32
8.1.7	Definición del lineamiento institucional para el uso de firmas electrónicas y digitales	39
8.1.8	Definición de arquitectura objetivo.....	40
8.1.9	Lista de chequeo previo a la implementación	42
	ANEXO 1. MARCO NORMATIVO Y TÉCNICO	45
	BIBLIOGRAFÍA.....	52

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

ÍNDICE DE TABLAS Y FIGURAS

Tabla 1. Comparación de familias de firma electrónica: CAdES, XAdES y PAdES	10
Tabla 2. Perfiles de firma de largo plazo y evidencias de validación asociadas	12
Tabla 3. Principios orientadores para la selección del mecanismo de firma	13
Tabla 4. Roles y responsabilidades del equipo interdisciplinario del proyecto	20
Tabla 5. Matriz de análisis para el diagnóstico de producción documental electrónica	27
Tabla 6. Elementos para la caracterización de tipos documentales sujetos a firma	30
Tabla 7. Criterios para la priorización de tipos documentales sujetos a firma	31
Tabla 8. Mecanismos de autenticación, firma y validación de documentos electrónicos	33
Tabla 9. Criterios para definir el mecanismo de firma aplicable	35
Tabla 10. Matriz orientadora de aplicación del mecanismo de firma por escenario documental	37
Tabla 11. Componentes del Modelo de Referencia de Arquitectura Empresarial (MRAE) aplicables a la firma	41
Tabla 12. Lista de chequeo previo a la implementación	43
Tabla 13. Marco normativo y técnico aplicable a la firma electrónica y digital de documentos de archivo	45

Índice de figuras

Figura 1. Hoja de ruta para la adopción e implementación de firmas electrónicas y digitales, por fases	18
Figura 1. Momentos de aplicación de la firma en el ciclo de vida del documento (producción, trámite, organización y preservación)	26

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

1 INTRODUCCIÓN

La incorporación de mecanismos de autenticación, firma y validación sobre documentos electrónicos de archivo constituye uno de los principales desafíos que enfrentan actualmente las entidades en el marco de la transformación digital y la administración de documentos electrónicos. Aunque muchas entidades ya utilizan mecanismos de firma electrónica o digital en algunos de sus procesos, no siempre estas decisiones han estado precedidas por un ejercicio de planeación que permita articularlas con la gestión documental, la producción de documentos electrónicos de archivo, su administración y su preservación digital.

Esta situación puede generar diferencias en los criterios para la aplicación de los mecanismos de firma, dificultades para integrar los documentos firmados a los expedientes electrónicos o limitaciones para garantizar su autenticidad, integridad y usabilidad durante todo su ciclo de vida. Por esta razón, antes de adoptar nuevas soluciones o ampliar el uso de las ya existentes, resulta conveniente definir criterios institucionales que orienten estas decisiones de manera articulada con los procesos, los instrumentos archivísticos y las necesidades propias de cada entidad.

La presente guía puede ser utilizada por entidades que se encuentran en diferentes niveles de avance; para aquellas que aún no han iniciado este proceso, ofrece una ruta de planeación que facilita la definición de criterios institucionales antes de abordar etapas de implementación. Para las entidades que ya disponen de mecanismos de autenticación, firma o validación, constituye un referente para revisar su articulación con la gestión documental, los instrumentos archivísticos, las políticas institucionales y las estrategias relacionadas con la administración, conservación y preservación de los documentos electrónicos de archivo.

La presente guía corresponde al primer entregable y se concentra en la fase de planeación. Su propósito es orientar a las entidades en la definición del contexto institucional, el análisis de la producción documental electrónica, la caracterización de los documentos sujetos a firma, la definición de criterios para la selección de mecanismos de autenticación, firma y validación, y la formulación del lineamiento institucional que servirá de base para las decisiones posteriores.

El segundo entregable desarrollará la fase de implementación, en la cual se abordarán aspectos relacionados con la arquitectura de solución, los requisitos funcionales, técnicos y de integración, la parametrización de plataformas, la incorporación de mecanismos de firma en los sistemas de información y los procesos de puesta en operación.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

El tercer entregable estará orientado a la preservación digital de los documentos electrónicos firmados, abordando aspectos relacionados con la conservación de las evidencias electrónicas, los perfiles de firma de largo plazo, los mecanismos de validación futura, el estampado cronológico, la administración del material de validación y las estrategias necesarias para mantener la autenticidad, integridad, disponibilidad y usabilidad de los documentos electrónicos de archivo durante todo su período de conservación.

Aunque cada guía puede consultarse de manera independiente, las tres hacen parte de una misma ruta metodológica y se complementan entre sí para apoyar a las entidades en la adopción de firmas electrónicas y digitales sobre documentos electrónicos de archivo.

2 OBJETIVO

Establecer una ruta práctica para planear la adopción de firmas electrónicas y digitales sobre documentos electrónicos de archivo, definiendo criterios, responsabilidades, requisitos e instrumentos que orienten su implementación de manera segura, trazable y articulada con la gestión documental institucional.

3 ALCANCE

La guía está dirigida a equipos de gestión documental, tecnología, jurídica, seguridad de la información, planeación, control interno y áreas productoras que participen en proyectos de adopción de firmas. Puede usarse tanto para iniciar un proyecto institucional como para ordenar una implementación que ya se encuentre en curso.

4 CONCEPTOS BÁSICOS

Los conceptos desarrollados en este capítulo constituyen el marco conceptual necesario para la comprensión y aplicación de la presente guía. En atención a la naturaleza técnica del instrumento, las definiciones se presentan de manera contextualizada y articulada con su contenido; por tal razón, no se incorpora un glosario independiente, evitando la duplicidad de definiciones dentro del documento. Para la consulta de la terminología archivística de carácter general, se recomienda acudir al Anexo 1 – Definiciones del Acuerdo 001 de 2024 del Archivo General de la Nación, disponible en:

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Conulte/Recursos/Publicaciones/Acuerdo-001-Anexo1_Definiciones.pdf

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Mensaje de datos y documento electrónico de archivo

La Ley 527 de 1999 define el mensaje de datos como la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos. Todo documento electrónico es un mensaje de datos, pero no todo mensaje de datos es un documento de archivo. Un documento electrónico de archivo es aquel producido o recibido en ejercicio de las funciones institucionales y que forma parte del patrimonio documental de la entidad. Para que tenga valor archivístico debe cumplir cuatro atributos: autenticidad, integridad, fiabilidad y disponibilidad.

Los anteriores atributos deben estar presentes en los diferentes tipos o clases de documentos electrónicos, los cuales son:

- Documentos textuales: son aquellos que su contenido se elabora y presenta a través del uso de símbolos que conforman un texto.
- Fotografías digitales: son aquellos que están conformados por pixeles y cuentan con una resolución y profundidad de bits. Esta clase de documentos cuenta con dos categorías: Imágenes digitales (producidas digitalmente) o imágenes escaneadas.
- Documentos de audio: son aquellos que su contenido está representado por medio de ondas sonoras.
- Documentos de video: son un conjunto de imágenes y sonido digital reproducidos a una velocidad constante.
- Documentos geoespaciales: son aquellos que dentro de su contenido permite el mapeo, análisis o visualización de una ubicación geográfica o georreferenciación de la superficie terrestre.
- Correo electrónico: son comunicaciones electrónicas entre varias personas o entidades, realizadas a través de herramientas de comunicación electrónica.
- Mensaje de datos: son comunicaciones electrónicas entre varias personas o entidades, realizadas a través de herramientas de mensajería.
- Datos estructurados: son archivos o conjuntos de datos organizados de forma sistemática en un modelo o estructura que facilita su almacenamiento, procesamiento, análisis, búsqueda y recuperación.

Los sistemas de información, programas informáticos, aplicaciones móviles, sedes electrónicas, sitios web y portales web no constituyen por sí mismos una clase de documento electrónico. Los registros que estos produzcan o reciban en ejercicio de las funciones institucionales, sin importar en que sistema o herramienta se hayan generado, pueden constituir documentos electrónicos de archivo, y deberán gestionarse de acuerdo con su

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

contexto, su vínculo con la función o proceso que los originó conforme a los requisitos archivísticos aplicables.

La aplicación práctica de estos conceptos en el análisis de la producción documental electrónica se desarrolla en el numeral 8.1.4 Diagnóstico de producción documental electrónica, mientras que su utilización para seleccionar el mecanismo de firma se presenta en el numeral 8.1.6 Criterios para definir el mecanismo de firma

Autenticidad, integridad, fiabilidad disponibilidad y usabilidad

La autenticidad garantiza que el documento es lo que dice ser, fue producido por quien afirma haberlo hecho, y fue producido en la fecha que se indica.

La integridad garantiza que su contenido no fue modificado desde su creación o desde el momento de la firma.

La fiabilidad se refiere a que el documento refleja fielmente los hechos o actos que documenta.

La disponibilidad es la capacidad de acceder a él cuando sea necesario, durante todo su período de conservación.

La usabilidad es la capacidad del documento de ser localizado, recuperado, presentado e interpretado cuando sea necesario. Un documento puede estar disponible, auténtico e íntegro, pero perder su utilidad como evidencia si no puede recuperarse, presentarse o interpretarse adecuadamente. Por ejemplo, un documento guardado en un formato que ningún programa actual puede leer se puede ubicar y descargar sin problema (está disponible), pero no se puede abrir ni ver su contenido (no es usable).

Estos atributos no son declaraciones abstractas: son requisitos operativos. Una firma bien aplicada contribuye a acreditar la autenticidad y la integridad. Pero ninguna firma reemplaza los demás atributos si el sistema no está adecuadamente gestionado.

Estos atributos constituyen criterios de evaluación durante el diagnóstico institucional (numeral 8.1.4) y son la base para determinar el mecanismo de firma apropiado en el numeral 8.1.6 Criterios para definir el mecanismo de firma.

Documento electrónico como evidencia

Uno de los aspectos más importantes dentro de la gestión de documentos electrónicos de archivo consiste en su capacidad para servir como evidencia de las actuaciones, decisiones y actividades realizadas por una entidad.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

En el entorno digital, esta condición se encuentra asociada al principio de equivalencia funcional, reconocido en la Ley 527 de 1999, según el cual un mensaje de datos puede producir los mismos efectos jurídicos que un documento físico, siempre que sea posible conservarlo, consultarlo y verificar condiciones relacionadas con autenticidad e integridad.

Esto significa que el documento electrónico no pierde valor jurídico por el hecho de encontrarse en formato digital. Su valor depende de que pueda mantenerse íntegro, accesible y asociado de manera confiable a quien lo produjo.

En este contexto, las firmas electrónicas y digitales cumplen una función importante como mecanismos de autenticación y validación, ya que permiten identificar al autor, asociar manifestaciones de voluntad y fortalecer condiciones de autenticidad e integridad sobre los documentos electrónicos de archivo.

En Colombia, la Ley 527 de 1999 reconoce el uso de firmas electrónicas y digitales como mecanismos válidos para identificar a una persona y relacionarla con el contenido de un mensaje de datos. En el caso de la firma digital, su utilización incorpora controles técnicos y jurídicos que permiten fortalecer la autenticidad e integridad del documento electrónico.

Así mismo, el ordenamiento jurídico colombiano reconoce los mensajes de datos como medios válidos de prueba documental, siempre que puedan mantenerse accesibles, íntegros y verificables durante el tiempo requerido.

En las actuaciones administrativas, el uso de medios electrónicos también exige que los documentos conserven condiciones adecuadas de autenticidad, integridad, conservación y posibilidad de consulta.

Pero aquí hay un punto importante. El valor del documento electrónico como evidencia no depende únicamente de la firma. También intervienen aspectos relacionados con el contexto de producción documental; la trazabilidad de las actuaciones realizadas; la relación con expedientes y series documentales; administración de metadatos; conservación y preservación; y capacidad de mantener verificabilidad en el tiempo.

Cuando estas condiciones no existen o funcionan de manera fragmentada, un documento puede encontrarse autenticado y aun así presentar debilidades como evidencia institucional.

Por esa razón, las firmas electrónicas y digitales no deben entenderse como elementos aislados del documento electrónico de archivo, sino como parte de un conjunto más amplio de

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

condiciones documentales, archivísticas, jurídicas y tecnológicas necesarias para mantener documentos electrónicos confiables, verificables y utilizables durante todo su ciclo de vida.

Evidencia electrónica

Para efectos de esta guía, la evidencia electrónica es el conjunto de información digital que permite sustentar y verificar una actuación, un evento de firma o las condiciones de autenticidad e integridad de un documento electrónico. Puede comprender el documento, la firma, los sellos de tiempo, los metadatos de contexto, los registros de auditoría, los certificados y los datos de validación.

La evidencia electrónica no es sinónimo de firma ni determina por sí sola la fuerza probatoria. Su valoración depende, entre otros factores, de la confiabilidad de la forma en que la información fue generada, archivada o comunicada, de la conservación de su integridad y de la identificación de su iniciador.

Diferencia entre autenticación, firma electrónica y firma digital

Esta distinción es crítica porque su confusión genera errores graves de implementación. Autenticarse es verificar la identidad de quien accede a un sistema. Una contraseña, un dispositivo criptográfico (en adelante token) o un certificado de cliente permiten saber que el usuario es quien dice ser. Pero ese acto de acceso no firma ningún documento. El Acuerdo 001 de 2024 del AGN define la autenticación electrónica como "la acreditación por medios electrónicos de la identidad de una persona o autoridad, para elaborar o firmar documentos, o para adelantar trámites y procedimientos administrativos". La autenticación puede ser un paso previo a la firma, pero no la sustituye.

La firma electrónica es el género: comprende cualquier método que permita identificar a una persona en relación con un mensaje de datos, siempre que sea confiable y apropiado para el propósito del acto. Así la define el Decreto 2364 de 2012. La firma digital es una especie dentro de ese género: es un tipo de firma electrónica que utiliza criptografía asimétrica y un certificado digital emitido por una entidad de certificación acreditada. La Ley 527 de 1999 la regula de forma específica y le reconoce una presunción legal de autenticidad e integridad que la firma electrónica simple no tiene automáticamente.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

La firma digital: fundamentos y cadena de confianza

La firma digital vincula de forma única al firmante con el contenido del documento mediante un mecanismo matemático. Si alguien modifica el documento después de firmado, la firma queda invalidada de forma detectable. Esto es posible porque el proceso combina una función de resumen criptográfico (en adelante hash), que genera una especie de huella única del documento, con un par de claves criptográficas exclusivas del firmante.

Certificado digital, PKI y claves

El firmante dispone de una clave privada, que solo él conoce y usa para firmar, y una clave pública, que cualquiera puede emplear para verificar que la firma proviene de él. Ambas hacen parte de una Infraestructura de Clave Pública (PKI).

Para que esa infraestructura sea confiable, las claves deben estar respaldadas por un certificado digital emitido por una entidad de certificación legalmente habilitada, que vincula la identidad del firmante con su clave pública de forma verificable.

Conviene distinguir tres roles: el suscriptor es la persona a cuyo nombre se expide el certificado; el firmante es quien lo usa para firmar un documento; y el iniciador es quien genera o envía el mensaje de datos. En muchos casos los tres roles coinciden en una misma persona, pero no siempre.

Revocación: CRL y OCSP

Un certificado tiene un período de validez, pero puede ser suspendido o revocado antes de su vencimiento, por ejemplo, si la clave privada fue comprometida o si el suscriptor dejó el cargo. Para saber si un certificado era válido en el momento exacto de la firma existen dos mecanismos: las Listas de Certificados Revocados (CRL), que se publican periódicamente, y el protocolo OCSP, que permite consultar en tiempo real el estado del certificado. Ambos son necesarios para demostrar que la firma fue válida cuando se aplicó.

ONAC, entidades de certificación digital

En Colombia, las entidades de certificación que ofrecen servicios al público deben estar acreditadas. El Organismo Nacional de Acreditación de Colombia (ONAC) verifica que las autoridades de certificación cumplen con los requisitos técnicos y organizativos exigidos por la normativa. Un certificado para uso institucional no puede provenir de cualquier proveedor; debe ser expedido por una entidad debidamente acreditada.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Módulo de Seguridad de Hardware (HSM)

Dispositivo físico especializado, certificado bajo estándares de seguridad reconocidos que genera, almacena y gestiona claves criptográficas privadas en un entorno protegido y resistente a manipulaciones. Su función principal es garantizar que la clave privada nunca abandone el dispositivo.

Firma electrónica

La firma electrónica responde a un principio de neutralidad tecnológica: la validez no depende de una sola tecnología, sino de que el método identifique a la persona, muestre su aprobación del contenido y sea confiable para el propósito. Este principio tiene fundamento en el artículo 2° de la Ley 1341 de 2009 (modificada por la Ley 1978 de 2019), que consagra la neutralidad tecnológica como principio rector de la sociedad de la información, según el cual la validez jurídica de un acto no depende de una tecnología específica, pero la selección del mecanismo de firma debe responder a criterios de idoneidad demostrable para el propósito archivístico y probatorio de que se trate.

Puede apoyarse en código de un solo uso (OTP), aceptación en plataforma con credenciales robustas, biometría, claves criptográficas privadas u otros mecanismos equivalentes. La pregunta correcta al momento de elegir un mecanismo de firma electrónica es cuál deja evidencia suficiente de quién, cuándo y sobre qué contenido, acorde a la naturaleza de documento objeto de firma.

Formatos técnicos de firma y perfiles de aplicación.

Este capítulo fija las definiciones operativas y técnicas que necesita una entidad distrital para entender los perfiles de largo plazo y qué papel cumple el sello de tiempo dentro de la evidencia electrónica.

Se distingue entre dos lenguajes vigentes actualmente. El primero es el lenguaje histórico, todavía frecuente en documentos institucionales, que habla de CAdES-A, XAdES-A y PAdES-LTV. El segundo es el lenguaje ETSI del Instituto Europeo de Normas de Telecomunicaciones vigente, que organiza las firmas en perfiles formatos técnicos de firma y perfiles de aplicación (baseline) y extendidos.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Contexto general de los perfiles CAdES, XAdES y PAdES

Estos perfiles no son 'niveles de seguridad', sino tres familias de formato. La diferencia principal no está en la fuerza jurídica por sí sola, sino en la estructura técnica del objeto firmado: CAdES se apoya en CMS, XAdES en XML y PAdES en PDF.

Por esa razón, la primera decisión no suele ser jurídica sino documental: si el documento nativo es un PDF, la familia natural es PAdES; si es XML estructurado, la familia natural es XAdES; y si corresponde a un objeto binario, un contenedor o una firma separada del contenido, la familia más habitual es CAdES.

CAdES

CAdES corresponde a CMS Advanced Electronic Signatures. Técnicamente parte de CMS, la sintaxis criptográfica normalizada por IETF (Internet Engineering Task Force) para encapsular firmas, certificados y otros atributos. En lenguaje simple, CAdES es útil cuando la firma debe vivir como un objeto criptográfico independiente, adjunto o incrustado sobre datos que no son XML ni PDF. Esta familia es, por tanto, la aplicable a documentos no estructurados o semiestructurados como fotografías, audio, video o documentos geoespaciales, dado que no corresponden a XML ni a PDF.

Su ventaja institucional es la flexibilidad: puede aplicarse sobre archivos binarios, paquetes de intercambio o firmas desacopladas del documento visual. Su desventaja práctica es que no siempre resulta amigable para lectura humana directa, porque la firma no está pensada para 'verse' dentro del documento como sí ocurre en PDF.

XAdES

XAdES corresponde a XML Advanced Electronic Signatures. Su lógica es distinta: la firma se expresa como un conjunto de elementos XML y, por tanto, encaja especialmente bien en flujos donde el documento o mensaje ya vive en XML y donde interesa firmar el documento completo o partes específicas de su estructura.

XAdES es especialmente útil cuando la actuación administrativa depende de intercambio estructurado entre sistemas, conocido como interoperabilidad, validaciones automáticas o esquemas XML ya definidos. No es el formato natural para un PDF final de lectura humana; su campo natural es el documento o mensaje estructurado.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

PADES

PADES corresponde a PDF Advanced Electronic Signatures. Es la familia diseñada para documentos PDF y por eso suele ser la más comprensible para el usuario final: la firma vive dentro del mismo PDF, puede mostrarse en interfaces conocidas y permite que el archivo se conserve como unidad documental cerrada.

Para entidades públicas, PADES suele ser la opción técnica más natural cuando el documento final con valor de consulta, prueba o archivo está en PDF: actos administrativos finales, certificaciones, conceptos, constancias, resoluciones o comunicaciones oficiales cerradas en ese formato.

Tabla 1. Comparación de familias de firma electrónica: CAdES, XAdES y PADES

Familia	Base técnica	Dónde vive la firma	Usos	Referencia vigente principal
CAdES	CMS / Cryptographic Message Syntax	En un objeto criptográfico separado o adjunto	Datos binarios, evidencias, intercambios no PDF/XML	ETSI EN 319 122-1 y 122-2; ISO 14533-1:2022
XAdES	XML Signature + propiedades XAdES	Dentro de la estructura XML	Mensajes y documentos XML estructurados	ETSI EN 319 132-1 y 132-2; ISO 14533-2:2021
PADES	PDF + firma avanzada para PDF	Dentro del mismo PDF	Documento final en PDF para lectura humana y archivo	ETSI EN 319 142-1 y 142-2; ISO 14533-3:2025

Nota: las referencias a las normas ETSI EN 319 122, 132 y 142 corresponden a las versiones vigentes al momento de publicación de esta Guía. Por tratarse de estándares técnicos sujetos a actualización periódica por parte del organismo europeo de normalización, se recomienda a las entidades verificar la versión vigente de cada referencia en el portal oficial de ETSI (www.etsi.org) antes de su aplicación, y consultar las actualizaciones que sobre la materia publique el Archivo General de la Nación.

Variantes y perfiles de largo plazo

En la práctica archivística interesa distinguir entre una firma básica y una firma preparada para verificación futura. Una firma básica acredita autoría e integridad al momento de firmar; una firma de largo plazo añade o conserva la evidencia necesaria para seguir validando la firma

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

cuando el certificado expire, cuando se necesite probar el estado de revocación histórico o cuando la verificación ocurra años después.

CAdES-A

CAdES-A es el perfil histórico de archivado de la familia CAdES. Su lógica es preservar la capacidad de verificación, agregando sellos de tiempo de archivo y los datos que permiten reconstruir, con posterioridad, la cadena de confianza y el estado de validez del certificado. En términos de negocio, sirve cuando la firma no solo debe probar quién firmó, sino también que la verificación futura seguirá siendo posible aun cuando el contexto original haya cambiado. La referencia histórica aparece en ETSI TS 101 733 y su marco actual se entiende mejor a la luz de ETSI EN 319 122-1 y 122-2, junto con ISO 14533-1:2022.

XAdES-A

XAdES-A cumple la misma función, pero en el mundo XML. Añade propiedades de archivado y sellos de tiempo para conservar la prueba de existencia y la capacidad de validación futura. Es una opción razonable cuando el expediente o intercambio principal es XML y la entidad necesita sostener la verificabilidad a largo plazo sin convertir el activo principal a PDF. Su antecedente histórico está en ETSI TS 101 903 y hoy debe leerse con ETSI EN 319 132-1 y 132-2, además de ISO 14533-2:2021.

PAdES-LTV

PAdES-LTV es el nombre más extendido, en lenguaje de implementación, para el PDF que incorpora o deja referenciada la evidencia necesaria para su validación futura: cadena de certificados, información de revocación y sellos de tiempo. En documentos públicos que se producen y conservan en PDF, este es el concepto más útil para equipos jurídicos, archivísticos y de TI porque apunta a un objetivo claro: que el propio PDF viaje con la mayor parte de su evidencia de validación. En la documentación ETSI actual, la familia relevante se encuentra en ETSI EN 319 142-1 y 142-2, donde aparecen perfiles adicionales como PAdES-E-LTV.

Qué evidencia debe acompañar a un perfil de largo plazo

Sin importar la familia elegida, como mínimo, la entidad debe pensar en cuatro piezas: el documento firmado, la cadena de certificados necesaria para validar la firma, los datos de revocación o validación histórica y uno o más sellos de tiempo emitidos conforme al perfil técnico aplicable.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Tabla 2. Perfiles de firma de largo plazo y evidencias de validación asociadas

Perfil	Familia	Qué añade	Cuándo tiene sentido
CAAdES-A	CAAdES	Sellos de tiempo de archivo y evidencia para validación futura	Objetos binarios o firmas CMS que deban sostenerse por largos periodos
XAdES-A	XAdES	Propiedades de archivado, sellos de tiempo y material de validación	Mensajes o documentos XML con exigencia de conservación prolongada
PAdES-LTV PAdES-E-LTV	PAdES	Datos de validación y sellos de tiempo vinculados al PDF	Documento final en PDF que debe poder verificarse años después

Sello de tiempo y autoridad de Sellado de Tiempo (TSA)

El sello de tiempo no es una firma del autor del documento. Es una prueba de un tercero sobre el momento en que ciertos datos existían. RFC 3161 define el Time-Stamp Protocol y el formato del token de estampado.

En lenguaje sencillo, una TSA toma la huella o resumen criptográfico del objeto, la vincula con una fecha y hora confiables, y emite un token firmado con su propia clave. Ese token no aprueba el contenido ni identifica al autor material del acto; lo que hace es acreditar que el dato existía antes de un momento determinado y que la TSA respondió por esa afirmación técnica.

En Colombia, la ley y sus reglamentos usan con mayor frecuencia la expresión estampado cronológico y vinculan este servicio al ecosistema de entidades de certificación. Por prudencia institucional, cuando se hable de 'TSA acreditada' debe verificarse el alcance acreditado vigente del prestador en el Directorio Oficial de ONAC y no asumir que toda acreditación cubre, por sí sola, todos los servicios posibles.

Para efectos de planeación, esta guía distingue tres usos técnicos del estampado cronológico. Estas denominaciones son orientadoras y no constituyen categorías jurídicas autónomas:

- Uso asociado a la firma: incorpora un token de tiempo para demostrar que la firma y los datos protegidos existían en un momento determinado y apoyar la validación temporal del certificado del firmante.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

- Uso de archivo: protege la firma y su material de validación para que puedan verificarse posteriormente; puede requerir sellos de tiempo sucesivos antes de que los algoritmos o las evidencias de validación resulten insuficientes, como ocurre en perfiles CAdES-A, XAdES-A o PAdES con validación de largo plazo.
- Uso en preservación digital: consiste en renovar o añadir evidencias temporales durante la conservación para mantener demostrables la existencia y la integridad del objeto digital. No crea una nueva firma ni sustituye las estrategias de preservación; se articula con registros de evidencia y sellos de tiempo de archivo.

5 PRINCIPIOS ORIENTADORES

Toda entidad que requiera seleccionar, adquirir e implementar un esquema de firmas electrónicas o digitales para sus documentos electrónicos de archivo deberá tener en cuenta los siguientes principios orientadores, los cuales constituyen el marco de referencia previo a cualquier decisión de carácter normativo, documental o tecnológico. Estos principios se organizan en cuatro dimensiones —archivística, de gobernanza, tecnológica y de valor probatorio— que deben leerse de manera articulada, dado que ninguna de ellas resulta suficiente por sí sola para garantizar la autenticidad, integridad, fiabilidad, disponibilidad y usabilidad de los documentos electrónicos de archivo durante todo su ciclo de vida. Su aplicación orienta las decisiones que se desarrollan con mayor detalle en el capítulo 8 de esta guía, correspondiente a la fase de planeación.

Tabla 3. Principios orientadores para la selección del mecanismo de firma

Dimensión	Principio	Enfoque en la firma
	Firma alineada con la valoración documental	El mecanismo de firma se selecciona según la serie o subserie, su tiempo de retención y su disposición final en las TRD: la firma debe garantizar la autenticidad e integridad del documento durante todo el tiempo que la TRD exige conservarlo.
	Firma integrada al documento o a su paquete de evidencia verificable	La firma se integra a la estructura lógica del documento como parte de su contenido probatorio, esto es: embebida en el documento; encapsulada en un contenedor asociado; o acompañada de material de

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Dimensión	Principio	Enfoque en la firma
Archivística		validación separado, pero lógicamente vinculado.
	Firma sensible a la integridad	Cualquier cambio sobre el contenido posterior a la firma la invalida; por ello el momento y las condiciones de firma deben definirse dentro del flujo documental.
	Formatos y perfiles de firma con material de validación de largo plazo	Cuando el documento debe conservarse a largo plazo, el mecanismo de firma debe permitir su verificación durante todo ese periodo, mediante perfiles y formatos con disponibilidad e integridad del material de validación a lo largo del tiempo.
Gobernanza	Firma ligada a la función institucional	El mecanismo de firma asignado responde a la función que materializa el documento y al valor, importancia y objeto de la actuación, no a la conveniencia del área.
	Firma con responsables definidos	La entidad define qué dependencias asignan, administran y controlan los mecanismos de firma, y qué roles están autorizados a firmar cada tipo documental.
	Firma sostenible	La selección considera la sostenibilidad técnica, administrativa y financiera del mecanismo a corto, mediano y largo plazo, reconociendo que la firma digital tiene costos asociados a la certificación acreditada ante ONAC.
	Firma dentro del marco de gobierno documental	La definición, alcance e implementación de los mecanismos de firma se establece dentro de la política de gestión documental, el PINAR y los instrumentos archivísticos.
Tecnológica	La firma se decide por gestión documental, se habilita por tecnología	Qué se firma, con qué mecanismo y bajo qué condiciones lo define gestión documental; TI implementa la solución, sin que la herramienta disponible determine la decisión archivística.
	Firma planeada con independencia de la madurez	La incorporación de firmas se planifica analizando sistemas, repositorios, flujos e

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Dimensión	Principio	Enfoque en la firma
		infraestructura, cuenta o no la entidad con un SGDEA implementado.
	Firma alineada con la seguridad de la información	El proceso de firmado se integra al SGSI: control de acceso, registro de eventos, gestión de incidentes, protección de datos y continuidad operativa.
	Firma alineada con protección de datos personales	La firma debe integrar elementos que protejan los datos personales de los firmantes. Si la firma involucra datos personales susceptibles a anonimización se requiere formular el consentimiento informado en donde se indique el uso que se le va a dar a los datos personales.
	Firma interoperable y sin dependencia de proveedor	Los mecanismos adoptados permiten verificar los documentos firmados con independencia de la solución utilizada, evitando la dependencia de un único proveedor o plataforma.
Valor probatorio	Firma como evidencia	La firma se incorpora para que el documento se mantenga como evidencia válida de las actuaciones institucionales durante todo su ciclo de vida.
	Firma seleccionada por criterios, no por disponibilidad	El mecanismo se elige analizando tipo documental, finalidad, nivel de riesgo, impacto jurídico y tiempo de conservación como evidencia.
	Firma electrónica para identificación y trazabilidad	Resulta suficiente cuando basta identificar al autor, manifestar aprobación o dejar trazabilidad, siempre que la entidad pueda demostrar la confiabilidad del mecanismo.
	Firma digital para mayor respaldo	Se utiliza cuando se requiere mayor seguridad, control y respaldo probatorio: actuaciones administrativas, documentos con efectos jurídicos relevantes o con verificabilidad a largo plazo.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

6 CONTEXTO INSTITUCIONAL

La incorporación de firmas electrónicas y digitales dentro de la entidad no debería entenderse únicamente como la sustitución de la firma manuscrita en ambientes electrónicos. Su alcance es mayor, el cual termina impactando la producción documental, la validez de actuaciones administrativas, la trazabilidad institucional y la capacidad de mantener los documentos electrónicos de archivo auténticos, íntegros, fiables y usables durante todo su ciclo de vida.

En muchas entidades ya se cuenta con mecanismos de firma funcionando dentro de plataformas, trámites o procedimientos específicos. Sin embargo, estas soluciones suelen haberse desarrollado de manera independiente, sin una articulación suficiente con los instrumentos archivísticos, los expedientes electrónicos, los sistemas de gestión documental o las estrategias de preservación digital.

Cuando la adopción de firmas electrónicas o digitales se realiza sin un adecuado análisis del contexto institucional, pueden presentarse situaciones que afectan la gestión documental, la operación de los procesos y la administración de los documentos electrónicos de archivo. Entre ellas se encuentran la adquisición de servicios o paquetes de firmas que no responden a necesidades reales de la entidad, la falta de interoperabilidad con los sistemas de información productores de documentos, la creencia de que únicamente la firma digital permite garantizar autenticidad, integridad y fiabilidad, o la utilización de formatos documentales que no favorecen la preservación de la información en el tiempo.

De igual forma, pueden generarse documentos firmados que no quedan vinculados a los expedientes electrónicos, evidencias de firma almacenadas de manera aislada, flujos documentales sin trazabilidad completa o mecanismos de autenticación que, aunque funcionan técnicamente, no se encuentran articulados con los procesos de gestión documental y archivo de la entidad.

En este contexto, resulta necesario que la entidad aborde estas iniciativas desde una perspectiva institucional, promoviendo la articulación entre las áreas de gestión documental, tecnología, seguridad de la información, jurídica y demás dependencias involucradas. Esto permite comprender las necesidades reales de la organización, establecer criterios para la adopción de mecanismos de autenticación, firma y validación, y orientar las decisiones que deberán desarrollarse durante la fase de planeación y servirán de base para las etapas posteriores de implementación.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Asimismo, cuando la entidad identifique brechas relacionadas con la gestión documental, la preservación digital, la administración de documentos electrónicos o las capacidades tecnológicas requeridas para este tipo de iniciativas, podrá incorporarlas en instrumentos de planeación institucional, como el Plan Institucional de Archivos (PINAR), con el fin de programar acciones de fortalecimiento y avanzar progresivamente en su implementación.

A partir de este contexto, la entidad podrá desarrollar las actividades de planeación descritas en el siguiente capítulo, orientadas a identificar necesidades institucionales, analizar documentos y procesos, definir criterios para la selección de mecanismos de autenticación, firma y validación, y establecer las condiciones requeridas para una adopción articulada con la gestión documental y la administración de documentos electrónicos de archivo.

Las condiciones institucionales identificadas en este capítulo constituyen el punto de partida para la Hoja de Ruta para la adopción e implementación de firmas electrónicas y digitales (capítulo 7) y para las actividades de planeación desarrolladas en el capítulo 8.

7 HOJA DE RUTA PARA LA ADOPCIÓN E IMPLEMENTACIÓN DE FIRMAS ELECTRÓNICAS DIGITALES

La presente hoja de ruta propone una secuencia progresiva de análisis y toma de decisiones, orientada a que las entidades incorporen el uso de firmas electrónicas y digitales de manera articulada con la gestión documental, la planeación institucional y las tecnologías de información de la entidad.

Este enfoque reconoce que el uso de firmas no es un asunto exclusivamente tecnológico y que este depende de las condiciones bajo las cuales se produce, se gestiona y se conserva el documento electrónico de archivo.

Por esta razón, la hoja de ruta se estructura en fases progresivas, donde cada una genera insumos que permiten avanzar a la siguiente, evitando decisiones aisladas o desarticuladas.

La presente guía desarrolla únicamente la primera fase de esta hoja de ruta, correspondiente a la planeación institucional. Las fases relacionadas con la implementación tecnológica y la preservación digital serán desarrolladas en guías posteriores de esta colección.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO



Figura 1. Hoja de ruta para la adopción e implementación de firmas electrónicas y digitales, por fases

8 PLANEACIÓN DE LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES

La planeación de la adopción de firmas electrónicas y digitales constituye el primer momento de la línea de trabajo. Su finalidad es preparar a la entidad antes de seleccionar, adquirir, configurar o implementar una solución tecnológica de firma.

En esta etapa la entidad debe comprender su contexto documental, jurídico, funcional y tecnológico; identificar los documentos que requieren mecanismos de autenticación y validación; reconocer los riesgos asociados; definir criterios para seleccionar el mecanismo de firma aplicable; y establecer los requisitos que deberán orientar la implementación posterior.

La planeación no tiene como resultado una solución funcionando. Su resultado principal es un modelo institucional de firmas, acompañado de requisitos funcionales, técnicos, jurídicos, archivísticos y de seguridad, que permitan pasar a la fase de implementación de manera ordenada.

8.1.1 Propósito de la fase de planeación

La fase de planeación tiene como propósito definir las condiciones institucionales, documentales, jurídicas, funcionales y tecnológicas necesarias para adoptar firmas electrónicas y digitales sobre documentos electrónicos de archivo.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Esta fase permite evitar decisiones aisladas, como aplicar un mismo mecanismo de firma a todos los documentos, adquirir una solución sin criterios documentales, usar firmas digitales donde bastaría una firma electrónica confiable, o implementar mecanismos de autenticación sin garantizar trazabilidad, evidencia, conservación y verificabilidad futura.

Así mismo, la fase de planeación permite identificar capacidades institucionales existentes, necesidades de fortalecimiento y condiciones requeridas para avanzar posteriormente hacia etapas de implementación, operación y sostenibilidad de mecanismos de firma electrónica y digital

8.1.2 Alistamiento institucional y definición del alcance

El alistamiento institucional permite poner en marcha el proceso de planeación de manera ordenada. En esta etapa la entidad reconoce la necesidad de adoptar o fortalecer el uso de firmas electrónicas y digitales, define el alcance inicial del análisis, conforma el equipo responsable y establece las condiciones básicas de coordinación.

La necesidad institucional puede surgir de diferentes situaciones: trámites que requieren mayor trazabilidad, documentos que se imprimen únicamente para firma, riesgos probatorios, uso de firmas escaneadas, aprobación de documentos por medios no controlados, dispersión documental, transformación digital o necesidad de fortalecer el expediente electrónico.

Esta fase no implica seleccionar una herramienta ni definir todavía el mecanismo de firma aplicable a cada documento. Su finalidad es preparar el trabajo institucional para que las siguientes actividades se desarrollen con claridad, respaldo directivo y participación de las áreas competentes.

El alcance preliminar puede definirse por proceso, trámite, dependencia, tipo documental, sistema de información o conjunto de documentos priorizados. Para iniciar, se recomienda un alcance controlado y escalable que permita validar criterios en escenarios concretos antes de extender la adopción a toda la entidad.

Como parte del alistamiento, la entidad debe recopilar los elementos de referencia institucional que servirán de marco para el diagnóstico de producción documental electrónica descrito en el numeral siguiente: las necesidades funcionales identificadas por las áreas productoras de documentos, las restricciones presupuestales disponibles para el proyecto, el calendario de implementación esperado por la entidad, y las restricciones tecnológicas existentes en los

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

sistemas de información y la infraestructura institucional. Estos elementos evitan que el diagnóstico se desarrolle sin un marco de referencia institucional previamente definido.

Las decisiones sobre firma electrónica deben tomarse en un cuerpo colegiado que reúna a quienes producen los documentos, a quienes los conservan, a quienes los protegen tecnológicamente y a quienes responden por su validez jurídica. El equipo interdisciplinario no es una formalidad: es el mecanismo que sostiene la trazabilidad de las decisiones y, llegado el caso, la defensa probatoria del documento firmado.

La composición que se presenta a continuación corresponde a un núcleo mínimo de capacidades y no implica crear cargos o dependencias nuevas. En entidades grandes o con alta producción documental, cada rol puede corresponder a una o varias personas. En entidades pequeñas o con estructuras limitadas, una misma persona puede asumir más de un rol, o la entidad puede asignar funciones a perfiles equivalentes, contratar servicios especializados, acudir a esquemas de cooperación interinstitucional o solicitar acompañamiento técnico externo. En todos los casos deben mantenerse la responsabilidad institucional, la supervisión, la separación de funciones incompatibles y la prevención de conflictos de interés; por ejemplo, quien diseña los controles no debería ser quien los audita.

El criterio que distingue una buena conformación de una conformación nominal es simple: todos los roles deben tener capacidad real de decisión y dedicación efectiva en sus áreas. Un equipo en el papel pero sin tiempos asignados es la principal causa de retraso en estos proyectos.

Tabla 4. Roles y responsabilidades del equipo interdisciplinario del proyecto

Rol / Perfil	Área de la entidad	Responsabilidades específicas en el proyecto
Líder patrocinador o del proyecto	Alta dirección (Secretaría General, Dirección Administrativa o equivalente)	Aprueba el alcance y resuelve diferencias entre áreas. Garantiza que las decisiones del equipo sean elevadas al Comité Institucional de Gestión y Desempeño. Sin este patrocinio, el proyecto no avanza.
Coordinador gerente o del proyecto	Gestión documental o el área designada	Construye y mantiene el cronograma, articula con todas las áreas, lleva la bitácora de decisiones y los riesgos. Es el punto único de contacto del proyecto.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Rol / Perfil	Área de la entidad	Responsabilidades específicas en el proyecto
Líder archivístico	Grupo o Subdirección de Gestión Documental	Lidera la caracterización de tipos documentales y series, identifica el ciclo vital y los plazos de retención que condicionan los formatos de firma a usar (por ejemplo, perfiles de larga duración tipo PAdES-LTV o XAdES-A para documentos de conservación permanente).
Profesional jurídico	Oficina Jurídica o Asesoría Legal	Valida los requisitos de fiabilidad del art. 2.2.2.47.4 del Decreto 1074 de 2015, las obligaciones contractuales con entidades de certificación digital (acreditadas ante ONAC) y los aspectos probatorios. Revisa cláusulas de los contratos con proveedores y términos de uso para firmantes.
Arquitecto o líder de TI	Oficina de TI / Oficina TIC	Diseña la arquitectura técnica de la solución de firma, la integración con el SGDEA, ECM o sistemas misionales, los repositorios y los servicios asociados (sello de tiempo, validación OCSP/CRL).
Oficial de seguridad de la información	Equipo de profesionales asignados a la seguridad de la información	Realiza el análisis de riesgos en los términos del MSPI y de la guía ETSI TR 119 100. Define controles para la custodia de claves privadas (HSM, certificados en token, certificados en la nube), valida cadena de confianza y protocolos de revocación.
Líder de proceso o dueño de la información	Áreas misionales productoras de los documentos	Aporta el conocimiento del proceso real: quién firma, en qué momento, con qué riesgo, con qué volumen, ante qué destinatario. Sin su participación, las decisiones se toman en abstracto.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Roles complementarios según el contexto: responsable de comunicaciones y gestión del cambio (la adopción de firma falla más por resistencia al cambio que por temas técnicos), enlace con la entidad de certificación digital escogida, y especialista en preservación digital cuando se trate de documentos con valor secundario o de conservación total.

La entidad no debería desarrollar este ejercicio de cero, en muchas ya existen diagnósticos, evaluaciones y ejercicios institucionales relacionados con gestión documental, tecnología o transformación digital. El problema es que normalmente se analizan por separado. Este ejercicio no busca repetirlos, sino conectarlos y utilizarlos como base para entender las condiciones reales de la entidad. Entre ellos se encuentran:

- Diagnóstico integral de archivo
- Modelo de Gestión Documental y Administración de Archivos (MGDA)
- Instrumentos de evaluación de seguridad y privacidad de la información
- Ejercicios de arquitectura empresarial,
- Evaluaciones de madurez institucional,
- Modelos relacionados con transformación digital y gestión de información.

Las actividades desarrolladas durante esta etapa permiten a la entidad contar con una base inicial de articulación institucional y comprensión del contexto documental, jurídico, tecnológico y organizacional relacionado con la adopción de firmas electrónicas y digitales, armonizándolas con lo consignado en el Plan institucional archivos – PINAR y el Plan Estratégico de Tecnologías de la Información PETI.

El nivel de profundidad y desarrollo de estas actividades dependerá del alcance definido, las capacidades institucionales existentes y el grado de madurez de la entidad frente a la gestión de documentos electrónicos de archivo.

8.1.3 Revisión normativa y marco de referencia aplicable

La revisión del marco normativo es uno de esos pasos que muchas entidades creen tener resuelto porque cuentan con un normograma o porque ya identificaron algunas normas relacionadas con firma electrónica y firma digital. Pero aquí el problema no es listar normas. El verdadero reto es entender cómo esas disposiciones impactan la producción documental de la entidad y qué implicaciones tienen cuando los documentos empiezan a producirse, aprobarse, firmarse y preservarse en entornos electrónicos.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

No todos los documentos requieren el mismo nivel de control, tampoco todas las actuaciones necesitan el mismo mecanismo de autenticación o validación, ya que las exigencias cambian según el tipo documental, la finalidad del proceso, el nivel de riesgo y el valor jurídico o probatorio que pueda tener el documento dentro de la actuación administrativa. Por esa razón, esta revisión debe permitir identificar y analizar las disposiciones normativas relacionadas con:

- La aplicación de los requisitos jurídicos de los mensajes de datos.
- El régimen de uso de la firma electrónica y de la firma digital.
- La presunción de autenticidad, la integridad, la inalterabilidad, la fiabilidad y la disponibilidad de los documentos electrónicos de archivo.
- Los requisitos de autenticación, identificación, trazabilidad y metadatos asociados a la gestión documental electrónica.
- La conservación y preservación digital de los documentos electrónicos de archivo, incluidos sus componentes y evidencias asociadas.

Este análisis no debería quedarse únicamente en la interpretación normativa. También necesita mostrar cómo está realmente la entidad frente a esas exigencias y qué tan preparadas están sus condiciones documentales, administrativas y tecnológicas para sostener el uso de mecanismos de firma dentro de los procesos institucionales.

Porque una cosa es que la norma reconozca validez jurídica sobre documentos electrónicos y otra muy distinta es que la entidad tenga capacidad real para garantizar autenticidad, integridad, fiabilidad, usabilidad y trazabilidad en el tiempo.

En muchos casos las dificultades no aparecen al momento de firmar el documento, sino después. Empiezan cuando no existe claridad sobre el proceso documental, cuando los documentos no quedan vinculados al expediente correspondiente, cuando los mecanismos de validación dejan de funcionar o cuando años después ya no es posible demostrar adecuadamente las condiciones bajo las cuales se produjo y firmó el documento, transacción o evidencia electrónica.

En este punto también resulta importante entender que la decisión sobre qué mecanismo de firma utilizar, no debería tomarse únicamente por facilidad operativa, disponibilidad tecnológica o costumbre institucional. La decisión debe responder al contexto jurídico, tecnológico, administrativo y documental. Existen casos donde una firma electrónica puede resultar suficiente para identificar al autor y expresar aprobación sobre el contenido. Pero también existen actuaciones que, por su impacto jurídico, nivel de riesgo o necesidad probatoria,

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

requieren mecanismos con mayores condiciones de validación y respaldo, como ocurre con la firma digital soportada en certificados emitidos por entidades de certificación acreditadas.

Cuando esta diferenciación no se realiza correctamente, las entidades terminan aplicando el mismo mecanismo para todo. Y ahí empiezan los problemas: documentos sobredimensionados en controles que no necesitaban o, peor todavía, actuaciones críticas respaldadas con mecanismos insuficientes frente al nivel de riesgo o exigencia jurídica.

Así mismo, la revisión normativa debe permitir identificar posibles riesgos relacionados con autenticidad documental; pérdida de trazabilidad; preservación de documentos electrónicos; capacidad de validación futura; y sostenibilidad de la evidencia electrónica en el tiempo.

Como actividades clave para llevar a cabo se enlistan las siguientes:

- Identificar las normas aplicables según las funciones y procesos institucionales.
- Analizar requisitos relacionados con documentos electrónicos, mensajes de datos y mecanismos de firma.
- Evaluar el estado actual de la entidad frente a las exigencias normativas identificadas.
- Identificar brechas jurídicas y archivísticas que puedan afectar la incorporación de mecanismos de firma.
- Definir criterios iniciales para orientar la selección y uso de mecanismos de autenticación y validación.

El desarrollo de esta actividad permite a la entidad identificar condiciones normativas, requisitos jurídicos y criterios archivísticos relacionados con el uso de firmas electrónicas y digitales sobre documentos electrónicos de archivo.

Los resultados del análisis podrán articularse con instrumentos archivísticos, lineamientos institucionales y estrategias relacionadas con gestión documental, preservación digital y administración de documentos electrónicos de archivo.

Como instrumento de apoyo en esta actividad se relaciona el *Anexo 1. Normograma*

8.1.4 Diagnóstico de producción documental electrónica

El diagnóstico de producción documental electrónica permite conocer cómo se producen, tramitan, aprueban, almacenan, consultan y preservan los documentos electrónicos dentro de

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

la entidad. Su propósito es identificar las condiciones institucionales que pueden facilitar o dificultar la adopción de mecanismos de autenticación, firma y validación sobre documentos electrónicos de archivo.

La finalidad de esta actividad no es realizar un diagnóstico archivístico integral de la entidad, sino identificar las condiciones existentes que pueden incidir en la adopción de mecanismos de autenticación, firma y validación sobre documentos electrónicos de archivo. Por ello, el análisis debe concentrarse en los documentos, procesos, sistemas de información y repositorios comprendidos dentro del alcance definido para la iniciativa.

Este análisis debe identificar los procesos y procedimientos donde se generan documentos electrónicos, los sistemas de información involucrados, los repositorios donde se almacenan, los mecanismos actuales de aprobación o firma, el uso de metadatos, la trazabilidad disponible y la relación de los documentos con expedientes electrónicos.

Dentro de este análisis, la entidad necesita revisar cómo se encuentra organizada actualmente la producción de documentos electrónicos y qué condiciones existen para garantizar autenticidad, integridad, trazabilidad, conservación y preservación durante todo su ciclo de vida.

Como parte del diagnóstico, resulta importante revisar la forma en que se encuentra organizada la producción documental electrónica y las condiciones existentes para garantizar autenticidad, integridad, trazabilidad, preservación y usabilidad durante el ciclo de vida de los documentos. Para ello, la entidad podrá analizar aspectos como la incorporación de documentos electrónicos en las Tablas de Retención Documental (TRD), la existencia de definiciones institucionales sobre formatos documentales, su articulación con estrategias de preservación digital y la incorporación de lineamientos relacionados con documentos electrónicos dentro del Programa de Gestión Documental (PGD) o instrumentos equivalentes.

La aplicación o uso de la firma se puede presentar en diferentes momentos del ciclo de vida del documento, y de acuerdo con su asignación, su alcance es diferente. Es por ello que dentro de la acción del diagnóstico se debe identificar los momentos en los cuales se puede asignar la firma. Entre los cuales se pueden encontrar:

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

PROCESO	ACCIÓN	OBJETO
Producción	• Producción de documentos • Radicación de documento	Autenticidad e integridad del documento Demostrar acciones de radicación
Trámite	• Digitalización del documento	Demostrar obtención fiable de la imagen
Organización	• Cierre del expediente	Firma del índice electrónico
Preservación	• Refirmado del documento	Asegurar la autenticidad del documento cuando la firma original pierde validez

Figura 2. Momentos de aplicación de la firma en el ciclo de vida del documento (producción, trámite, organización y preservación)

También resulta importante identificar si los documentos electrónicos siguen flujos documentales claramente definidos, si existen mecanismos de autenticación o validación implementados y si los sistemas conservan los metadatos necesarios para mantener el contexto, la trazabilidad y la usabilidad de los documentos a lo largo del tiempo.

Cuando la entidad ya cuenta con mecanismos de firma electrónica o digital, el análisis debe permitir establecer cómo estos se encuentran integrados con la gestión documental, los expedientes electrónicos y los sistemas de información institucionales.

En estos casos, resulta importante identificar dónde se producen los documentos firmados, o en qué momento se debe hacer uso de la firma, cómo se incorporan a las series y expedientes, qué evidencias generan y qué condiciones existen para conservar su autenticidad, integridad y usabilidad en el tiempo. Así mismo, se recomienda revisar si existen lineamientos, procedimientos, responsables y actos administrativos que regulen su utilización dentro de la entidad.

En este análisis resulta importante recordar que el problema normalmente no aparece en el momento de firmar el documento. Con frecuencia las dificultades surgen posteriormente, cuando el documento debe mantenerse vinculado al expediente electrónico, conservar la trazabilidad de las actuaciones realizadas y permanecer disponible y usable durante el tiempo que la entidad requiera conservarlo.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Cuando la entidad aún no cuenta con mecanismos de firma electrónica o digital, el diagnóstico debe orientarse a identificar las capacidades institucionales existentes y los aspectos que requieren fortalecimiento para avanzar en este tipo de iniciativas. Esto incluye la revisión de procesos documentales, sistemas de información, administración de expedientes electrónicos, capacidades de interoperabilidad, seguridad de la información y preservación digital.

El diagnóstico también debe permitir reconocer situaciones que puedan afectar la adopción de mecanismos de firma, tales como documentos electrónicos sin relación clara con series o subseries documentales, aprobaciones realizadas por medios no controlados, utilización de firmas escaneadas, almacenamiento en repositorios dispersos, ausencia de metadatos, deficiencias de trazabilidad o dificultades para mantener la autenticidad, integridad y usabilidad de los documentos con el paso del tiempo.

Como instrumento de apoyo, la entidad podrá utilizar una matriz de análisis como la siguiente:

Tabla 5. Matriz de análisis para el diagnóstico de producción documental electrónica

Elemento a diagnosticar	Aspecto a verificar
Procesos y procedimientos	Dónde se producen documentos electrónicos y cómo circulan dentro de los procesos institucionales.
Tipos documentales	Qué tipos de documentos se generan (textuales, imagen, audio, video, entre otros) con qué finalidad y que necesidades de autenticación o validación presentan
Momento de aplicación de la firma	La aplicación del mecanismo de firma puede ser en diferentes momentos del ciclo de vida del documento: - Producción - Trámite - Organización - Preservación
Alcance de la firma	Objeto o el para qué se requiere la firma, por ejemplo: - Autenticidad e integridad del documento - Cierre del expediente electrónico - Refirmado
Sistemas de información	Dónde se crean, tramitan, firman o almacenan los documentos.
Repositorios	Dónde se conservan los documentos y bajo qué reglas.
Flujos de aprobación	Quién elabora, revisa, aprueba y firma.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Elemento a diagnosticar	Aspecto a verificar
Mecanismos actuales de firma	Firma manuscrita, firma escaneada, aprobación por correo, firma electrónica, firma digital u otros mecanismos existentes.
Metadatos	Qué información se registra sobre creación, autoría, fecha, trámite y conservación.
Metadatos de firma	Los metadatos necesarios provenientes de la firma electrónica o digital que se requieren integrar al sistema de gestión documental, de acuerdo con lo establecido en el Esquema de Metadatos de Bogotá para Documentos de Archivo (EMBDA) 2.0, corresponden a los siguientes campos obligatorios de firma: - Tipo de firma - Formato de firma - Emisor de firma - Número de serie certificado - Algoritmo de firma - En calidad de - Fecha y hora de firma - Fecha y hora de verificación - Resultado de verificación - Fecha y hora inicio validez - Fecha y hora fin validez - Clave pública
Trazabilidad	Qué eventos quedan registrados y pueden auditarse.
Expediente electrónico	Si el documento queda vinculado a expediente, serie y subserie documental.

El desarrollo de esta actividad permite a la entidad comprender las condiciones reales bajo las cuales se producen, gestionan, aprueban, firman y preservan los documentos electrónicos de archivo, así como identificar prácticas, riesgos y necesidades que deberán considerarse en las siguientes etapas de caracterización documental, definición de mecanismos de firma y planeación de la implementación.

Los resultados obtenidos podrán articularse con los instrumentos archivísticos y demás iniciativas institucionales relacionadas con gestión documental, administración de documentos electrónicos de archivo y preservación digital.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

8.1.5 Caracterización y priorización de tipos documentales sujetos a firma e identificación de firmantes responsables

La caracterización de tipos documentales permite identificar qué documentos requieren firma y cuáles son los cargos, roles o instancias responsables de suscribirlos. Este análisis debe realizarse por tipo documental, y no de manera genérica para toda la entidad.

La decisión sobre la necesidad de firma debe estar articulada con los lineamientos e instrumentos de gestión documental. No es suficiente afirmar que un documento “requiere firma”; es necesario determinar qué documento es, el proceso o procedimiento que lo produce, la serie o subserie documental a la que pertenece, su valor documental, el responsable de suscribirlo o firmarlo, el tiempo de retención, la disposición final y las condiciones bajo las cuales deberá mantenerse para garantizar su autenticidad, integridad, fiabilidad, disponibilidad y usabilidad durante todo el ciclo de vida.

No todos los documentos electrónicos requieren firma. Esta necesidad de firma dependerá de la función que cumple el documento, los efectos jurídicos, administrativos, fiscales o probatorios que produce, los riesgos asociados a su utilización, de su valor documental y de las condiciones de conservación definidas por la entidad. Por esta razón, la caracterización constituye el principal insumo para identificar las tipologías documentales sujetas a firma dentro de la gestión documental electrónica Institucional.

La identificación del firmante responsable debe realizarse con base en la competencia funcional, la delegación existente, el procedimiento aplicable y el rol institucional facultado para suscribir el documento. Esta definición no debe depender únicamente del uso operativo de una herramienta tecnológica, sino de la responsabilidad asignada al cargo, dependencia o instancia que produce, aprueba o formaliza el documento.

Para orientar este análisis, la entidad podrá considerar, entre otros, los siguientes elementos de caracterización:

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Tabla 6. Elementos para la caracterización de tipos documentales sujetos a firma

Elemento de caracterización	Descripción
Tipo documental	Nombre del documento que será objeto de análisis. (Puede ser que la tipología documental se presente en varias series o subseries documentales, por lo cual se debe analizar e identificar en cada una de ellas, ya que cada serie o subserie puede presentar un valor documental, tiempo de retención y disposición final diferente).
Proceso o procedimiento productor	Actividad institucional, trámite o procedimiento en el que se produce, recibe, gestiona o formaliza el documento.
Serie o Subserie Documental TRD	Identificación de la serie o subserie documental a la que pertenece el documento, de acuerdo con la Tabla de Retención Documental. La TRD refleja el ejercicio de valoración documental mediante la asignación de tiempos de retención y disposición final; por tanto, el mecanismo de firma seleccionado deberá ser consecuente con dichas condiciones.
Formato	Formato en el que se produce el documento: PDF, XML, JPG, AVI, documento ofimático, formulario electrónico, registro de sistema u otro formato aplicable.
Medio de producción	Sistema de información, repositorio, plataforma o herramienta tecnológica mediante la cual se genera, recibe, tramita, firma, almacena o conserva el documento.
Necesidad de firma	Determina si el tipo documental requiere firma, considerando su valor jurídico o probatorio, destinatario, riesgo, impacto institucional, cumplimiento normativo, responsabilidad asociada, tiempo de retención y disposición final.
Firmante responsable	Cargo, rol o instancia competente para firmar el documento, de acuerdo con la función, delegación, competencia o procedimiento aplicable. El firmante responsable no debe confundirse con los roles que intervienen en la preparación del documento, como quien lo proyecta, elabora, revisa o tramita, salvo que alguno de estos cuente también con competencia expresa para suscribirlo.
Observaciones documentales funcionales	Condiciones particulares relacionadas con el volumen de producción, criticidad del documento, datos personales, dependencia de sistemas específicos, datos personales, trazabilidad requerida, interoperabilidad, preservación digital o restricciones operativas.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Elemento de caracterización	Descripción
Prioridad de adopción para la implementación	Nivel de prioridad asignado al tipo documental para su incorporación progresiva al modelo institucional de firmas electrónicas y digitales, de acuerdo con la matriz de priorización definida por la entidad.

El desarrollo de esta actividad permite identificar las tipologías documentales que requieren firma y los cargos, roles o instancias responsables de suscribirlas, para la priorización.

Priorización de tipos documentales

Una vez caracterizados los tipos documentales sujetos a firma, la entidad deberá establecer su orden de adopción para la implementación. La adopción de firmas electrónicas y digitales no necesariamente debe realizarse de manera simultánea para todas las tipologías documentales; podrá desarrollarse de forma progresiva, de acuerdo con la criticidad documental, las necesidades y las capacidades institucionales disponibles.

Para este propósito, se recomienda aplicar una matriz de priorización, que contenga como mínimo, los siguientes criterios:

Tabla 7. Criterios para la priorización de tipos documentales sujetos a firma

Criterio	Aspectos por evaluar
Volumen de producción	Cantidad y frecuencia con la que se producen, reciben o tramitan los documentos de la tipología analizada. Un mayor volumen puede representar mayores beneficios en eficiencia, reducción de tiempos, costos operativos y control documental.
Impacto institucional	Incidencia del documento en la toma de decisiones, la prestación de servicios, el cumplimiento de funciones, la atención a la ciudadanía y la gestión administrativa, contractual, financiera o misional de la entidad.
Urgencia normativa	Existencia de disposiciones legales, reglamentarias, contractuales, archivísticas o de control que exijan implementar oportunamente mecanismos de firma, autenticación, trazabilidad, conservación o validación.
Criticidad documental y nivel de riesgo	Importancia del documento para evidenciar actuaciones institucionales, garantizar derechos, sustentar decisiones o servir como prueba. Considera los riesgos jurídicos, administrativos, fiscales, operativos, reputacionales o de pérdida de autenticidad, integridad, fiabilidad y disponibilidad que podrían derivarse de su alteración, desconocimiento, uso indebido o ausencia.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Criterio	Aspectos por evaluar
Viabilidad técnica	Capacidad de los sistemas y plataformas para integrar el mecanismo de firma, gestionar identidades y metadatos, conservar las evidencias de validación, asegurar la interoperabilidad y mantener el documento durante el tiempo establecido en la TRD.
Disponibilidad de recursos	Existencia de presupuesto, infraestructura tecnológica, servicios de certificación o confianza, soporte técnico, talento humano y demás recursos necesarios para implementar y sostener el mecanismo de firma.
Madurez institucional para la adopción	Nivel de preparación organizacional para adoptar la firma electrónica o digital. Comprende la existencia de procedimientos formalizados, roles y responsabilidades definidos, instrumentos archivísticos actualizados, capacidades de gestión del cambio, personal capacitado, mecanismos de seguridad y condiciones para administrar documentos y expedientes electrónicos

La caracterización y priorización de los tipos documentales constituye un ejercicio técnico archivístico indispensable para delimitar el alcance de la adopción de firmas electrónicas y digitales, establecer una secuencia de implementación sustentada y asegurar su articulación con los procesos, los instrumentos de gestión documental y los sistemas de información institucionales. Sus resultados permiten consolidar una matriz institucional de aplicación de firmas por tipología documental, definir los responsables competentes para su suscripción y orientar la implementación de mecanismos que preserven el vínculo archivístico y el contexto de producción, mantengan la trazabilidad de las actuaciones y aseguren la autenticidad, integridad, fiabilidad, disponibilidad y usabilidad de los documentos electrónicos de archivo durante todo su ciclo de vida.

8.1.6 Criterios para definir el mecanismo de firma

Una vez caracterizados los tipos documentales sujetos a firma y los firmantes responsables, la entidad debe definir qué mecanismo de firma resulta adecuado para cada tipología documental. Esta decisión no puede adoptarse de manera uniforme para toda la entidad ni depender únicamente de la herramienta disponible. Debe construirse a partir de un análisis conjunto del valor del documento, su tiempo de conservación, su destinatario, el riesgo de la actuación y la viabilidad operativa.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Para apoyar esta actividad, a continuación, se presenta una referencia práctica de mecanismos, criterios y reglas orientadoras de aplicación. La clasificación combina categorías jurídicas reconocidas por la Ley 527 de 1999 y el Decreto 2364 de 2012 con capacidades funcionales que las entidades suelen adquirir o implementar, tales como la autenticación previa al firmado, el estampado cronológico o la validación de largo plazo.

Por ello, la columna "Mecanismo" no debe leerse como un inventario de tecnologías cerradas ni como una taxonomía legal exhaustiva. Algunas categorías corresponden a mecanismos de firma propiamente dichos y otras a servicios o capacidades complementarias que pueden formar parte de una misma solución institucional.

Esta clasificación debe entenderse como una referencia práctica para orientar la toma de decisiones. La entidad no debe seleccionar el mecanismo de firma únicamente por disponibilidad tecnológica, costo o facilidad operativa.

Tabla 8. Mecanismos de autenticación, firma y validación de documentos electrónicos

Mecanismo	Qué es	Características básicas
Autenticación electrónica previa al firmado	Verifica la identidad del usuario antes del acto de firma, pero no constituye por sí sola una firma documental.	Puede apoyarse en credenciales robustas, múltiples factores de autenticación, tokens o certificados de cliente. Habilita el acceso y el control del flujo, pero no reemplaza la evidencia de aprobación sobre el documento.
Firma electrónica en flujo	Firma electrónica aplicada dentro de una plataforma o proceso digital que deja evidencia de aprobación del contenido.	Suele implementarse mediante aceptación en plataforma, confirmación por correo o web y registros de auditoría. Es útil para documentos internos o de menor riesgo, siempre que exista trazabilidad suficiente del quién, cuándo y sobre qué contenido.
Firma electrónica con evidencia reforzada	Firma electrónica que añade mayores controles de identidad, autenticación, trazabilidad y conservación de evidencias.	Puede incorporar código de un solo uso (OTP), biometría, hash del documento, aceptación expresa y registro de auditoría. Sigue siendo firma electrónica

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Mecanismo	Qué es	Características básicas
		en sentido jurídico, pero con mayor soporte funcional y probatorio.
Firma digital basada en certificado digital de Entidad de Certificación Digital (ECD) acreditada	Firma digital soportada en certificado digital y criptografía asimétrica, emitido por una Entidad de Certificación Digital acreditada.	Permite verificar identidad e integridad mediante infraestructura de clave pública. Resulta especialmente pertinente para actuaciones con efectos jurídicos relevantes, necesidad de validación independiente por terceros o mayor exigencia probatoria.
Firma digital con estampado cronológico (sello de tiempo)	Firma digital complementada con una evidencia confiable de fecha y hora emitida por un prestador habilitado para ese servicio.	El sello de tiempo no reemplaza la firma del autor. Su implementación técnica suele basarse en la Request for Comments (RFC) 3161. Es útil cuando la oportunidad de firma, expedición, radicación o cierre del documento tiene relevancia administrativa, técnica o probatoria.
Firma digital con evidencias de validación de largo plazo	Firma digital que conserva o incorpora la evidencia necesaria para verificarla en el futuro.	Puede apoyarse en perfiles como PAdES-LTV o PAdES-E-LTV para Portable Document Format (PDF), XAdES-A para Extensible Markup Language (XML) o CAdES-A para firmas basadas en CMS. Resulta útil para documentos con retención prolongada, conservación permanente o alta necesidad de verificabilidad futura.

En términos de adquisición, las soluciones disponibles suelen organizarse por capas: autenticación e identidad, firma electrónica en flujo, firma digital basada en certificado digital y capacidades adicionales de estampado cronológico, validación de largo plazo, integración y custodia de evidencias. La entidad debe traducir esa oferta de mercado a criterios documentales y jurídicos propios, y no al contrario.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Una vez identificados los mecanismos de autenticación, firma y validación aplicable a los documentos electrónicos de archivo, el siguiente paso consiste en definir cuál de ellos resulta adecuado para cada tipología documental. Esta decisión debe realizarse con base en criterios documentales, funcionales, jurídicos, tecnológicos, de seguridad y de preservación.

Para orientar esta decisión, la entidad podrá aplicar los cinco criterios de análisis, descritos a continuación.

Tabla 9. Criterios para definir el mecanismo de firma aplicable

Criterio	Explicación
1. Valor jurídico, administrativo o probatorio	Permite establecer la importancia del documento dentro de la actuación institucional. Analiza si el documento crea derechos, impone obligaciones, vincula a terceros, soporta decisiones formales, acredita actuaciones o puede ser usado como evidencia.
2. Tiempo de retención y conservación según TRD	Permite identificar durante cuánto tiempo debe conservarse el documento y si será necesario verificar su autenticidad e integridad en el futuro. Este criterio conecta la decisión de firma con la TRD, la conservación documental y la preservación digital.
3. Destinatario y necesidad de validación externa	Permite determinar quién recibirá, consultará o validará el documento firmado. No es lo mismo un documento de uso interno que uno dirigido a ciudadanos, proveedores, contratistas, jueces, entes de control u otras entidades. Este criterio ayuda a valorar la necesidad de que la firma pueda ser validada fuera del entorno interno de la entidad.
4. Riesgo de la actuación documental	Permite analizar las consecuencias de una eventual impugnación, alteración, pérdida de trazabilidad o desconocimiento de la firma. Considera aspectos como cuantía, afectación de derechos, posibilidad de litigio, impacto institucional, auditoría, control fiscal, disciplinario o administrativo.
5. Volumen y modalidad de implementación	Permite evaluar la sostenibilidad práctica del mecanismo de firma. Analiza cuántos documentos se firman, cuántos firmantes intervienen, con qué frecuencia, qué tiempos de respuesta exige el proceso y qué modalidad de servicio o infraestructura podría requerirse, por ejemplo, token, firma centralizada, firma en la nube o módulo de seguridad de hardware (HSM).

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Aplicación integrada de los criterios

Los cinco criterios deben leerse de manera conjunta. Los cuatro primeros, valor jurídico, retención, destinatario y riesgo ayudan a definir el nivel de robustez que requiere el documento. El quinto criterio, volumen y modalidad de implementación, no reduce ese nivel de exigencia, sino que orienta la forma de implementación más sostenible.

Cuando un tipo documental cumpla simultáneamente varias condiciones, deberá prevalecer el criterio que exija mayor nivel de autenticidad, integridad, trazabilidad, valor probatorio o verificabilidad futura. Por ejemplo, un documento de bajo volumen, pero con alto valor jurídico o conservación prolongada, no debe tratarse como un caso simple solo porque operativamente sea fácil de firmar. A continuación, se describe una secuencia de análisis aplicada a los criterios:

- Si el documento es interno, de menor riesgo y con retención corta, la entidad puede valorar una firma electrónica en flujo o una firma electrónica con evidencia reforzada, según el grado de control que requiera el proceso. En estos casos, la pregunta central no es cuánta tecnología se usa, sino cuánta evidencia queda disponible para demostrar quién aprobó, cuándo lo hizo y sobre qué contenido exacto.
- Cuando el documento produce efectos jurídicos relevantes, puede ser controvertido, debe validarse de manera independiente por terceros o exige mayor respaldo probatorio, la firma digital basada en certificado digital emitido por una Entidad de Certificación Digital acreditada suele ofrecer mejores condiciones de autenticidad, integridad y verificabilidad.
- Una vez definido que el documento requiere firma digital, la entidad debe establecer si además necesita estampado cronológico o evidencias de validación de largo plazo. Esta decisión depende principalmente del tiempo de conservación, de la necesidad de acreditar fecha cierta y de la posibilidad de que la firma deba verificarse años después de producida.
- El volumen y la frecuencia de uso no cambian por sí solos el nivel jurídico o archivístico del mecanismo exigido. Lo que sí cambian es la modalidad de implementación: token individual, firma centralizada, firma en la nube, integración con plataformas de trámite o uso de un módulo de seguridad de hardware (HSM), entre otras alternativas equivalentes.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

- En documentos con varios firmantes debe procurarse coherencia en el mecanismo aplicado. La entidad debería evitar mezclar niveles de firma en un mismo documento, salvo que exista justificación funcional, jurídica y técnica suficientemente documentada.

Matriz orientadora de aplicación

Como apoyo para la planeación institucional, la entidad podrá utilizar una matriz orientadora como la siguiente. Sus categorías no son reglas legales automáticas ni sustituyen el análisis del caso concreto; sirven para ordenar la toma de decisiones por tipo documental.

Tabla 10. Matriz orientadora de aplicación del mecanismo de firma por escenario documental

Escenario predominante	Lectura integrada de criterios	Mecanismo orientador	Precisión institucional
Documento interno, operativo o de bajo riesgo, con retención corta	Bajo valor jurídico, destinatario interno, riesgo reducido y necesidad básica de trazabilidad.	Firma electrónica en flujo.	Puede escalar a firma electrónica con evidencia reforzada si el proceso exige mayor control de identidad, auditoría o trazabilidad.
Documento interno con necesidad reforzada de control, auditoría o trazabilidad	No crea derechos frente a terceros, pero sí exige mayor control sobre quién aprobó, cuándo y sobre qué contenido.	Firma electrónica con evidencia reforzada.	Puede incluir biometría u otros factores adicionales cuando ello resulte proporcional, legalmente procedente y técnicamente justificado.
Documento con efectos jurídicos relevantes o con posible validación por terceros	Actos administrativos, certificaciones, u otros tipos de documentos que soporten decisiones formales, respuestas con efectos jurídicos, relaciones con contratistas u otras entidades, o documentos	Firma digital basada en certificado digital de Entidad de Certificación Digital acreditada.	La decisión no depende del destinatario externo aislado, sino del conjunto entre valor jurídico, necesidad de validación independiente y nivel de riesgo.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Escenario predominante	Lectura integrada de criterios	Mecanismo orientador	Precisión institucional
	susceptibles de controversia.		
Documento cuya fecha y hora tengan relevancia probatoria o de control	La actuación exige demostrar oportunidad de firma, expedición, radicación, cierre o cumplimiento de plazo.	Firma digital con estampado cronológico.	El sello de tiempo complementa la firma; no la reemplaza ni se confunde con ella.
Documentos con requerimientos de validación a largo plazo o conservación total	La TRD o el riesgo institucional exige mantener capacidad de validación durante periodos extensos.	Firma digital con evidencias de validación de largo plazo.	Puede apoyarse en perfiles como PAdES-LTV, XAdES-A o CAdES-A, según el formato del documento y la arquitectura adoptada.
Proceso masivo, firma en serie o por lotes	Es pertinente cuando un mismo firmante autorizado suscribe numerosos documentos homogéneos, generados por un proceso controlado y sujetos a una misma regla de decisión, siempre que la revisión individual no sea un requisito esencial de la actuación. El volumen, por sí solo, no justifica la firma por lotes.	El mecanismo se define por los criterios anteriores; la firma en serie o por lotes es una modalidad de implementación.	Cada documento debe conservar trazabilidad individual: identificador, resumen criptográfico, firmante y competencia, fecha y hora, identificador del lote, resultado de firma y datos de validación. Además, debe poder verificarse y recuperarse de forma independiente.

Los resultados de este análisis servirán como base para la definición de lineamientos institucionales y para la implementación progresiva de mecanismos de firma electrónica y digital en los procesos priorizados por la entidad.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

8.1.7 Definición del lineamiento institucional para el uso de firmas electrónicas y digitales

La definición del lineamiento institucional corresponde al momento en que la entidad consolida y adopta las decisiones resultantes del proceso de análisis desarrollado durante la fase de planeación; su finalidad es proporcionar una referencia institucional que permita aplicar de manera consistente los mecanismos de autenticación, firma y validación definidos para los diferentes documentos electrónicos de archivo.

Las decisiones adoptadas durante esta etapa podrán formalizarse mediante los instrumentos institucionales que cada entidad tenga definidos para ese propósito, tales como resoluciones, directivas, circulares u otros actos administrativos equivalentes. La entidad podrá utilizar el instrumento que considere más adecuado, siempre que permita documentar los criterios definidos y orientar su aplicación dentro de los procesos, sistemas de información y dependencias involucradas.

La definición y adopción del lineamiento deberá contar con el liderazgo y respaldo de la alta dirección, a través de las instancias y mecanismos institucionales definidos por cada entidad, garantizando la participación de las áreas responsables de gestión documental, tecnología, gestión jurídica, seguridad de la información y demás dependencias involucradas.

En cuanto a su contenido, el lineamiento debería establecer como mínimo los criterios para la selección de los mecanismos de autenticación, firma y validación, los tipos documentales a los cuales aplican, los responsables involucrados, las condiciones generales de uso, las evidencias requeridas y las condiciones de conservación y preservación de las evidencias asociadas durante el ciclo de vida de los documentos.

Para asegurar su integración con la gestión documental y la administración de documentos electrónicos de archivo, las decisiones definidas deberán mantenerse articuladas con la Política de Gestión Documental, el Programa de Gestión Documental (PGD), su Programa Específico de Gestión de Documentos Electrónicos de Archivo, el modelo de requisitos del Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), el Sistema Integrado de Conservación (SIC), especialmente con el Programa de Preservación Digital a Largo Plazo y las políticas de seguridad de la información.

El lineamiento debe entenderse como un instrumento dinámico, por lo tanto, se recomienda revisar y actualizar periódicamente su contenido frente a cambios normativos, tecnológicos o institucionales, modificaciones en los instrumentos archivísticos, ampliación del alcance a nuevos procesos o tipologías documentales y resultados derivados de procesos de

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

seguimiento, evaluación o mejora continua. Estas revisiones deberían articularse, cuando resulte pertinente, con la actualización del PGD, el PINAR, el Sistema Integrado de Conservación y los demás instrumentos relacionados.

La formalización de estas decisiones a través del lineamiento definido a nivel institucional no garantiza por sí sola su aplicación efectiva. La incorporación de mecanismos de autenticación, firma y validación también involucra cambios en las prácticas de trabajo y en la forma en que los diferentes actores comprenden y gestionan los documentos electrónicos de archivo.

Por esta razón, se recomienda que la entidad contemple acciones de divulgación, sensibilización y fortalecimiento de capacidades que permitan comprender el alcance, los efectos jurídicos y las responsabilidades asociadas al uso de estos mecanismos. Así mismo, podrán desarrollar actividades de acompañamiento y apropiación dirigidas a los diferentes actores involucrados, con el fin de favorecer su aplicación consistente dentro de los procesos y sistemas de información institucionales.

Como resultado de este ejercicio, la entidad contará con un lineamiento institucional para el uso de firmas electrónicas y digitales sobre documentos electrónicos de archivo, en el que se formalizan los criterios y decisiones adoptados durante la fase de planeación y se orienta la aplicación uniforme de mecanismos de autenticación, firma y validación de acuerdo con las características documentales, funcionales, jurídicas y tecnológicas identificadas de acuerdo con la madurez que tenga la entidad en estos aspectos.

8.1.8 Definición de arquitectura objetivo

Para efectos de planeación institucional, este capítulo organiza la arquitectura objetivo con base en los dominios del Modelo de Arquitectura Empresarial del Marco de Referencia de Arquitectura Empresarial (MRAE) versión 3.0 adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones. Esta aproximación no reemplaza un ejercicio completo de Arquitectura Empresarial, pero sí establece una base mínima y realista para que la iniciativa de firmas pueda articularse con el Plan Estratégico de Tecnologías de la Información (PETI), la gestión documental y la hoja de ruta institucional.

En esta guía, la arquitectura objetivo se entiende como una descripción inicial del estado objetivo (TO-BE) para el alcance priorizado. No corresponde todavía a la implementación de una solución ni a la selección de un proveedor específico; su propósito es ordenar, por

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

dominios, las decisiones mínimas que deben quedar definidas para producir, firmar, validar, conservar, consultar y verificar documentos electrónicos de archivo.

Una vez definidos los criterios para seleccionar el mecanismo de firma, el lineamiento institucional y los requisitos funcionales, técnicos y de integración, la entidad debe consolidar una arquitectura objetivo que permita visualizar cómo se integrarán esos elementos dentro de su ecosistema documental y tecnológico.

Esquema orientador para construir la arquitectura objetivo

La arquitectura objetivo debe expresar la relación entre procesos, información, sistemas, servicios tecnológicos y controles de seguridad, evitando diseños centrados únicamente en la herramienta de firma. Su utilidad está en mostrar cómo el documento firmado conserva trazabilidad, metadatos, vínculo con el expediente, condiciones de validación y capacidad de consulta durante el tiempo de retención definido.

Tabla 11. Componentes del Modelo de Referencia de Arquitectura Empresarial (MRAE) aplicables a la firma

Dominio del MRAE	Qué debe quedar definido en el alcance de firmas	Productos o artefactos base esperados
Arquitectura institucional	Proceso o servicio impactado, roles responsables, puntos de firma, instancias de decisión, dependencias involucradas y relación con el expediente o trámite.	Extracto del modelo operativo institucional para el alcance; mapa de procesos o cadena de valor impactada; identificación de capacidades y servicios institucionales comprometidos.
Arquitectura de información	Objetos de información y documentos sujetos a firma, metadatos y evidencias asociadas, intercambios de información y reglas mínimas de consulta, conservación y preservación.	Modelo de Información Institucional ajustado al alcance; diagrama de integración de datos e información; catálogo mínimo de metadatos y evidencias de firma.
Arquitectura de sistemas de información	Sistemas que generan, firman, validan, radican, gestionan, conservan y consultan documentos; integraciones requeridas y servicios involucrados.	Caracterización de los sistemas de información involucrados; inventario o catálogo del alcance; documento de arquitectura de solución o integración para el servicio de firma.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Dominio del MRAE	Qué debe quedar definido en el alcance de firmas	Productos o artefactos base esperados
Arquitectura de tecnología	Servicios tecnológicos, ambientes, infraestructura, interoperabilidad, continuidad, disponibilidad y componentes requeridos para soportar el servicio.	Catálogo de elementos de infraestructura y servicios tecnológicos del alcance; vista conceptual de capacidades de TI; definición inicial de disponibilidad y continuidad.
Arquitectura de seguridad	Controles de identidad, autenticación, gestión de certificados, trazabilidad, protección de datos, registro de eventos, análisis de riesgos y manejo de incidentes.	Catálogo de servicios de seguridad aplicables; análisis de impacto del negocio y análisis de riesgos del alcance; definición de controles de seguridad y auditoría.

Si la entidad aún no cuenta con un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) implementado, un repositorio unificado o un servicio central de firma, la arquitectura objetivo puede definirse de manera incremental. En estos casos, la prioridad es dejar documentadas las brechas, las integraciones requeridas y los riesgos que deban escalarse a las instancias institucionales de arquitectura, seguridad, gestión documental o gobierno digital.

8.1.9 Lista de chequeo previo a la implementación

Antes de iniciar la implementación, adquisición, parametrización o integración de una solución de firma electrónica o digital, la entidad debe verificar que los insumos definidos en la fase de planeación se encuentran suficientemente desarrollados para el alcance que se pretende abordar. La lista se organiza en cinco bloques de verificación de alto nivel que consolidan los productos de cada etapa.

La verificación se hace sobre un alcance priorizado y no sobre la totalidad de la entidad: algunos criterios pueden estar plenamente definidos y otros desarrollarse de manera incremental, siempre que ello no comprometa la producción, firma, validación y conservación de los documentos del alcance. La columna de observaciones se utiliza para registrar el estado de cada criterio y dejar identificados los temas que deben reforzarse, completarse o ajustarse durante la implementación.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Tabla 12. Lista de chequeo previo a la implementación

Criterio de verificación	Sí	No	Observaciones
Gobernanza y alcance: la entidad definió el alcance de la adopción, conformó el equipo interdisciplinario responsable y revisó el marco normativo y técnico aplicable.			
Diagnóstico documental: se caracterizó la producción documental electrónica, se identificaron los tipos documentales sujetos a firma (en relación con TRD/CCD, procesos y procedimientos) y los firmantes, roles y ciclos de revisión, aprobación y firma.			
Modelo de firma: se definieron los criterios de selección del mecanismo de firma, se elaboró el lineamiento institucional y se cuenta con la matriz de aplicación de firmas por tipología documental.			
Arquitectura objetivo: se definió el estado objetivo (TO-BE) del alcance priorizado por dominios del MRAE (procesos, información, sistemas, tecnología y seguridad), con las brechas e integraciones documentadas.			
Preparación para implementar: se identificaron los ajustes requeridos en procedimientos, sistemas, repositorios e instrumentos archivísticos, y se cuenta con insumos suficientes para definir la priorización y el plan preliminar de implementación.			

La entidad puede avanzar hacia la implementación cuando los criterios anteriores se encuentren definidos para el alcance priorizado. Cuando algún elemento esté parcialmente desarrollado en particular el modelo de firma, la arquitectura objetivo o el respaldo institucional, las brechas registradas en la columna de observaciones deben incorporarse al plan preliminar de implementación y escalarse, según corresponda, a las instancias de arquitectura, seguridad,

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

gestión documental o gobierno digital, de modo que se atiendan de forma progresiva sin detener el avance sobre las tipologías priorizadas.

Una vez completada la lista de chequeo y verificado que los criterios definidos se encuentran suficientemente desarrollados para el alcance priorizado, la entidad contará con los insumos necesarios para avanzar hacia la fase de implementación tecnológica, que será desarrollada en el segundo entregable de esta colección. En esa fase se abordarán aspectos relacionados con la arquitectura de solución, los requisitos funcionales y técnicos, la parametrización de plataformas, la incorporación de mecanismos de firma en los sistemas de información y los procesos de puesta en operación.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

ANEXO 1. MARCO NORMATIVO Y TÉCNICO

El presente marco normativo y técnico consolida las normas aplicables a la adopción de firmas electrónicas y digitales en la gestión documental de las entidades del Distrito Capital. Se organiza en dos bloques, distinguidos visualmente en las tablas: la normativa de obligatorio cumplimiento (Constitución, leyes, decretos, resoluciones y circulares, incluida la protección de datos personales) y los acuerdos y resoluciones del Archivo General de la Nación, marcados con [AGN]. Los estándares técnicos de referencia (ISO, ETSI) no constituyen un bloque aparte, pues su actualización y aplicación corresponden principalmente a las entidades de certificación digital; se mencionan dentro del objeto de aplicación de la norma que remite a ellos.

Cada norma se presenta con su epígrafe completo, los artículos o secciones de aplicación directa y el objeto concreto que tiene dentro de la gestión documental, de modo que el lector pueda identificar con precisión cuál norma regula qué aspecto del ciclo de vida del documento firmado: desde la definición del mensaje de datos y la equivalencia funcional de la firma, hasta las condiciones aplicables a la protección de datos personales de los firmantes.

Convenciones utilizadas en las tablas del Anexo 1:

- Secciones A a E y G: normativa de obligatorio cumplimiento (Constitución, leyes, decretos reglamentarios y resoluciones/circulares).
- Sección F, marcada [AGN]: acuerdos y resoluciones del Archivo General de la Nación y demás autoridades archivísticas.
- Texto en cursiva dentro de la columna "Objeto / Aplicación": estándar técnico de referencia (ISO, ETSI) citado dentro del objeto de la norma que remite a él.

Tabla 13. Marco normativo y técnico aplicable a la firma electrónica y digital de documentos de archivo

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
A. NORMAS COLOMBIANAS — BLOQUE CONSTITUCIONAL Y ESTATUTARIO				
Constitución Política	Constitución Política de Colombia, 1991	Carta Magna del Estado colombiano	Arts. 15, 23, 74, 209	Derecho a la información, petición, acceso a documentos públicos y principios de la función administrativa. Fundamento de validez jurídica de actuaciones electrónicas.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
B. LEYES — MARCO GENERAL DE MENSAJES DE DATOS, COMERCIO ELECTRÓNICO Y FIRMAS				
Ley	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	Arts. 2°, 7°, 8°, 9°, 10° 11, 12, 28–40	Norma fundacional: equivalente electrónico de la firma, firma digital, entidades de certificación, presunción de autenticidad e integridad. Piedra angular del marco normativo.
Ley	Ley 594 de 2000	Ley General de Archivos	Arts. 2°, 19, 21, 46–48	Regula la gestión documental en Colombia; establece obligaciones de conservación, autenticidad e integridad aplicables a documentos electrónicos de archivo.
Ley	Ley 962 de 2005	Ley Antitrámites — racionalización de trámites y procedimientos administrativos	Art. 6 (Medios tecnológicos)	Impulsa el uso de medios electrónicos en la administración pública; habilita firma electrónica para trámites ante el Estado.
Ley	Ley 1341 de 2009 (modificada por L. 1978/2019)	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC (Ley TIC)	Art. 2°, numeral 6 (neutralidad tecnológica), art. 6°.	Principio de neutralidad tecnológica aplicable a la elección de tipo de firma. Reconocimiento de equivalencia funcional.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
Ley	Ley 1437 de 2011 (CPACA)	Código de Procedimiento Administrativo y de lo Contencioso Administrativo	Arts. 53–63 (actuaciones y notificaciones electrónicas), art. 64	Marco de actuaciones electrónicas en la administración pública; validez de actos administrativos en soporte electrónico y uso de firmas.
Ley	Ley 1564 de 2012 (CGP)	Código General del Proceso	Arts. 103, 105, 247 (valor probatorio de mensajes de datos)	Establece la validez jurídica de mensajes de datos como medio probatorio; reconoce firma electrónica y digital en actuaciones judiciales.
Ley	Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Arts. 15, 17, 19	Obliga a las entidades a adoptar sistemas de gestión documental; valor probatorio de documentos electrónicos publicados.
Ley	Ley 2052 de 2020	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial en materia de racionalización de trámites	Arts. 6° y 7	Habilita y promueve el uso de firma electrónica en trámites y actuaciones de la administración pública.
Ley	Ley 2069 de 2020	Por medio de la cual se impulsa el emprendimiento en Colombia	Art. 18 (firma electrónica y digital para emprendimiento)	Ordena al Gobierno reglamentar el uso de firma electrónica y digital; origen del Decreto 1789 de 2021.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
C. DECRETOS — REGLAMENTACIÓN DE FIRMAS DIGITALES Y ELECTRÓNICAS				
Decreto reglamentario	Decreto 333 de 2014	Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012 en relación con las características y requerimientos de las entidades de certificación	Arts. 1°–22 (deroga Decreto 1747/2000; fija requisitos de entidades de certificación)	Actualiza los requisitos para entidades de certificación digital; requisitos de auditoría y acreditación ante SIC.
Decreto reglamentario	Decreto 2364 de 2012 (incorporado en D. 1074/2015)	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica	Arts. 1°–7° (definición, confiabilidad, efectos jurídicos, obligaciones)	Regula la firma electrónica como género; define métodos admitidos (contraseñas, biometría, OTP, claves criptográficas); establece requisitos de confiabilidad.
Decreto reglamentario	Decreto 1074 de 2015 (arts. 2.2.2.47.1 a 2.2.2.47.10)	Decreto Único Reglamentario del Sector Comercio, Industria y Turismo — Compilación de firma electrónica	Arts. 2.2.2.47.1–2.2.2.47.10 (firma electrónica y digital)	Compila la regulación de firma electrónica; fija requisitos de confiabilidad aplicables en la gestión documental electrónica.
Decreto reglamentario	Decreto 1078 de 2015 (Título 17 de la parte 2 del libro 2)	Lineamientos generales en el uso y operación de los servicios ciudadanos digitales	Arts. 2.2.17.1.4, 2.2.17.2.1.1, 2.2.17.2.2.3, 2.2.17.2.2.4, 2.2.17.4.4, 2.2.17.6.3, 2.2.17.6.4,	Define los mecanismos de autenticación, el servicio de autenticación digital, las Condiciones mínimas para el servicio de autenticación digital, las obligaciones especiales de los prestadores del servicio de

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
				Autenticación Digital, Procedimiento para el registro de usuarios por medios electrónicos y la expedición de mecanismos de autenticación digital a usuarios. Aplicable a entidades públicas.
Decreto reglamentario	Decreto 1080 de 2015 (Parte 8 — arts. 2.8.2.1.1 y ss.)	Decreto Único Reglamentario del Sector Cultura — Gestión documental electrónica	Arts. 2.8.2.5.1–2.8.2.6.5 (SGDEA, expediente electrónico, autenticación, firma)	Regula los sistemas de gestión documental electrónica de archivo (SGDEA); exige autenticación, firma e integridad en documentos electrónicos de archivo.
Decreto reglamentario	Decreto 1789 de 2021	Por el cual se reglamenta el artículo 18 de la Ley 2069/2020 y se adicionan arts. 2.2.2.47.9 y 2.2.2.47.10 al Decreto 1074/2015	Arts. 2.2.2.47.9–2.2.2.47.10 (interoperabilidad, ecosistema digital)	Amplía el alcance de la firma electrónica y digital como herramienta de innovación y transformación digital; principio de equivalencia funcional.
D. DECRETOS — ADMINISTRACIÓN PÚBLICA, GOBIERNO DIGITAL Y TRANSFORMACIÓN				
Decreto reglamentario	Decreto 1078 de 2015 (Capítulo 1 del Título 9 de la Parte 2 del Libro 2 y Título 22 a la Parte 2 del Libro 2)	Lineamientos generales de la política de Gobierno Digital, y lineamientos y estándares de transformación digital	Arts. 2.2.9.1.2.1 y 2.2, 23.1.4.	Define la estructura del Gobierno Digital, incluyen entre sus habilitadores ellos los de servicios ciudadanos digitales, y de seguridad y privacidad de la información.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
				Establece obligaciones en materia de transformación digital, incluyendo el uso de la infraestructura de datos, la interoperabilidad, el uso de inteligencia artificial y de tecnologías emergentes.
E. ACUERDO DEL ARCHIVO GENERAL DE LA NACIÓN				
Acuerdo AGN	Acuerdo 001 de 2024 (AGN)	Por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado colombiano y se fijan otras disposiciones	Arts. 1°–5°, 12–18 (documento electrónico de archivo, autenticidad, integridad, firma, SGDEA, autenticación electrónica)	Principal norma archivística vigente. Define documentos electrónicos de archivo, atributos de autenticidad e integridad, autenticación electrónica, sistemas de gestión documental y requisitos de firma para la gestión de comunicaciones oficiales.
G. PROTECCIÓN DE DATOS PERSONALES				
Ley	Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales	Arts. 4°, 5°, 9°, 15, 17 (principios, tratamiento, autorización, deberes)	Regula el tratamiento de datos personales en Colombia; aplicable a la información personal vinculada a la identidad del firmante que se recopila, trata o almacena en los procesos de autenticación y firma electrónica y digital (biometría, certificados, datos de contacto).

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Jerarquía	Norma	Epígrafe	Artículos / Secciones relevantes	Objeto / Aplicación en gestión documental
Decreto reglamentario	Decreto 1377 de 2013 (incorporado en D. 1074/2015)	Por el cual se reglamenta parcialmente la Ley 1581 de 2012	Arts. 3°, 9°, 10, 26–27 (autorización, políticas de tratamiento, transferencia)	Desarrolla los requisitos de autorización del titular y las políticas de tratamiento de datos personales aplicables cuando los mecanismos de firma electrónica o digital involucran la captura, uso o transferencia de datos personales del firmante.

GUÍA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

BIBLIOGRAFÍA

Normativa constitucional y legal

Asamblea Nacional Constituyente (1991). *Constitución Política de Colombia*.

Congreso de la República de Colombia (1999). *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*.

Congreso de la República de Colombia (2000). *Ley 594 de 2000, Ley General de Archivos*.

Congreso de la República de Colombia (2005). *Ley 962 de 2005, por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos*.

Congreso de la República de Colombia (2009). *Ley 1341 de 2009, por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones (modificada por la Ley 1978 de 2019)*.

Congreso de la República de Colombia (2011). *Ley 1437 de 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo*.

Congreso de la República de Colombia (2012). *Ley 1564 de 2012, por medio de la cual se expide el Código General del Proceso*.

Congreso de la República de Colombia (2012). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*.

Congreso de la República de Colombia (2014). *Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*.

Congreso de la República de Colombia (2020). *Ley 2052 de 2020, por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial en materia de racionalización de trámites*.

Congreso de la República de Colombia (2020). *Ley 2069 de 2020, por medio de la cual se impulsa el emprendimiento en Colombia*.

Decretos reglamentarios

Presidencia de la República de Colombia (2012). *Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica (incorporado en el Decreto 1074 de 2015)*.

Ministerio de Comercio, Industria y Turismo (2013). *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012 (incorporado en el Decreto 1074 de 2015)*.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Ministerio de Comercio, Industria y Turismo (2014). *Decreto 333 de 2014, por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012 en relación con las entidades de certificación.*

Ministerio de Comercio, Industria y Turismo (2015). *Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.*

Ministerio de Cultura (2015). *Decreto 1080 de 2015, Decreto Único Reglamentario del Sector Cultura.*

Ministerio de Tecnologías de la Información y las Comunicaciones (2018). *Decreto 1078 de 2015. Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.*

Ministerio de Comercio, Industria y Turismo (2021). *Decreto 1789 de 2021, por el cual se reglamenta el artículo 18 de la Ley 2069 de 2020.*

Presidencia de la República de Colombia (2017). *Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015, y se crea el Modelo Integrado de Planeación y Gestión (MIPG).*

Acuerdos e instrumentos técnicos del Archivo General de la Nación

Archivo General de la Nación (2024). *Acuerdo 001 de 2024, por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado colombiano y se fijan otras disposiciones.*

Archivo General de la Nación (2020). *Modelo de Gestión Documental y Administración de Archivos (MGDA), versión 2.* Bogotá D.C.: Archivo General de la Nación.

Archivo General de la Nación (2024). *Lineamientos generales para la formulación de la Política Institucional de Gestión Documental (Anexo 2 del Acuerdo 001 de 2024).*

Ministerio de Tecnologías de la Información y las Comunicaciones y Archivo General de la Nación (2017). *Guía para la gestión de documentos y expedientes electrónicos, (G.INF.07) versión 1.0.* Bogotá D.C. Portal del Archivo General de la Nación.

Estándares técnicos internacionales

European Telecommunications Standards Institute. (2023). ETSI EN 319 122-1 V1.3.1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

European Telecommunications Standards Institute. (2023). ETSI EN 319 122-2 V1.2.1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

- European Telecommunications Standards Institute. (2024). ETSI EN 319 132-1 V1.3.1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.
- European Telecommunications Standards Institute. (2024). ETSI EN 319 132-2 V1.2.1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures.
- European Telecommunications Standards Institute. (2024). ETSI EN 319 142-1 V1.2.1: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.
- European Telecommunications Standards Institute. (2024). ETSI EN 319 142-2 V1.1.1: Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles.
- International Organization for Standardization. (2025). *ISO 14721:2025: Space data and information transfer systems — Open archival information system (OAIS) — Reference model*.
- International Organization for Standardization. (2005). *ISO 19005-1:2005: Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1)*.
- International Organization for Standardization (2022). *ISO 14533-1:2022 Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 1: Profiles for CMS Advanced Electronic Signatures (CAdES)*.
- International Organization for Standardization (2021). *ISO 14533-2:2021. Processes, data elements and documents in commerce, industry and administration — Long term signature — Part 2: Profiles for XML Advanced Electronic Signatures (XAdES)*.
- International Organization for Standardization (2025). *ISO 14533-3:2025: Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)*.
- International Organization for Standardization (s.f.). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
- Internet Engineering Task Force (2001). *RFC 3161, Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)*.

Referentes institucionales

- Departamento Administrativo de la Función Pública (2026). *Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG), versión 6.1*.

GUIA DE PLANEACIÓN PARA LA ADOPCIÓN DE FIRMAS ELECTRÓNICAS Y DIGITALES SOBRE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Ministerio de Tecnologías de la Información y las Comunicaciones. (2023) *Marco de Referencia de Arquitectura Empresarial (MRAE), versión 3.0*. Bogotá D.C.: Ministerio de Tecnologías de la Información y las Comunicaciones.

Secretaría General de la Alcaldía Mayor de Bogotá D.C. (2024). *Esquema de Metadatos de Bogotá para Documentos de Archivo (EMBDA) versión 2.0*. Bogotá D.C.: Dirección Distrital de Archivo de Bogotá.