



**El campo
es de todos**

Minagricultura

**PROGRAMA DE NORMALIZACION DE FORMAS Y FORMULARIOS PARA
DOCUMENTOS ELECTRÓNICOS**

BOGOTA D.C.

2021



TABLA DE CONTENIDO

INTRODUCCIÓN	4
1. OBJETIVO GENERAL DEL PROGRAMA	5
1.1. OBJETIVOS ESPECIFICOS DEL PROGRAMA	5
2. ALCANCE DEL PROGRAMA	5
3. NORMATIVIDAD	5
4. DEFINICIONES APLICABLES AL PROGRAMA	6
5. BENEFICIOS EN LA IMPLEMENTACIÓN DEL PROGRAMA	7
6. MODELO DE REQUISITOS MINIMOS PARA EL PROGRAMA	7
6.1. CARACTERISTICAS DEL PROGRAMA	8
6.1.1. Conformidad.	8
6.1.2. Interoperabilidad.	8
6.1.3. Seguridad.	8
6.1.4. Metadescripción.	8
6.1.5. Adición de contenidos.	8
6.1.6. Diseño y funcionamiento.	9
6.1.7. Gestión Distribuida.	9
6.1.8. Disponibilidad y acceso.	9
6.1.9. Neutralidad tecnológica.	9
7. REQUISITOS DE ACCESO Y SEGURIDAD PARA EL SISTEMA SGDEA	9
8. COPIAS DE SEGURIDAD Y RECUPERACIÓN	10
9. NIVELES DE SEGURIDAD Y ACCESO	10
10. REQUISITOS SOBRE LAS TABLAS DE RETENCION DOCUMENTAL (TRD)	11
11. REQUISITOS DE CAPTURA	11
12. MODELO DE METADATOS	12
13. REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO	12
13.1. AUTENTICIDAD	13
13.2. FIABILIDAD	16
13.3. INTEGRIDAD	17
13.4. DISPONIBILIDAD	19
13.5. MECANISMOS TECNICOS Y TECNOLOGICOS DE DISPONIBILIDAD	20
13.6. INTEROPERABILIDAD	21



13.7. TRANSFERENCIA DE DOCUMENTOS ELECTRÓNICOS	21
BIBLIOGRAFIA.....	27



INTRODUCCIÓN

En cumplimiento del Decreto 1080 de 2015 Decreto Único Reglamentario del Sector Cultura, el Ministerio de Agricultura y Desarrollo Rural – MADR, ha diseñado el siguiente Programa de Normalización de Formas y Formularios para Documentos Electrónicos el cual permite realizar el análisis diplomático de los documentos cual sea su soporte, delimitando y fijando sus características y atributos, con el propósito de crear las formas, formatos y formularios, denominándolos con nombres propios; permitiendo con ello establecer la tradición documental, autenticidad, integridad, fiabilidad y disponibilidad de la tipología de los documentos, para facilitar la identificación, clasificación y descripción de los documentos.



1. OBJETIVO GENERAL DEL PROGRAMA

Establecer las acciones que aseguren el uso de los documentos internos y externos de forma unificada, controlada y actualizada, mediante un método sistemático para la elaboración, edición, revisión, aprobación, manejo distribución, modificación y control de los documentos, con el fin de prevenir el uso no intencionado de documentos obsoletos en el Ministerio de Agricultura y Desarrollo Rural, cumpliendo con los estándares nacionales e internacionales.

1.1. OBJETIVOS ESPECIFICOS DEL PROGRAMA

- Realizar un análisis de la producción documental durante el ciclo de vida del documento y el tipo de soporte a fin de identificar las formas, formatos y formularios susceptibles de ser automatizados.
- Establecer las características de contenido y forma documental fija para los formatos y documentos electrónicos del Ministerio, de manera articulada con el Sistema de Calidad y el Programa de Gestión Documental garantizando el cumplimiento de los requisitos establecidos en la normatividad vigente.
- Determinar y socializar las directrices de la producción de formatos, formularios y documentos electrónicos, para garantizar la disminución de copias físicas de documentos electrónicos contribuyendo al ahorro de papel en el MADR.

2. ALCANCE DEL PROGRAMA

Para el Ministerio de Agricultura y Desarrollo Rural, el siguiente Programa de Normalización de requisitos de Formas y Formularios para Documentos Electrónicos es un instrumento de referencia y validación de los sistemas de producción de documentos electrónicos que será implementado durante el ciclo vital en el manejo electrónico de documentos de archivo.

3. NORMATIVIDAD

La siguiente es la normatividad aplicable para el Programa Normalización de requisitos de Formas y Formularios para Documentos Electrónicos en la gestión documental:



Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Decreto 1080 de 2015, Artículo 2.8.2.5.8. Instrumentos archivísticos para la gestión documental.

Acuerdo 04 de 2013 AGN., por el cual se reglamentan parcialmente los decretos 2578 y 2609 de 2012, y se modifica el procedimiento para la elaboración, presentación, evaluación, aprobación e implementación de las Tablas de Retención Documental y las Tablas de Valoración Documental.

Acuerdo 03 de 2015 AGN., por el cual se establecen los lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.

Acuerdo 004 de 2019 AGN, por el cual se reglamenta el procedimiento para la elaboración, aprobación, evaluación y convalidación, implementación, publicación e inscripción en el Registro único de Series Documentales – RUSD de las Tablas de Retención Documental – TRD y Tablas de Valoración Documental – TVD

ISO 15489 Información y documentación. Gestión de documentos.

4. DEFINICIONES APLICABLES AL PROGRAMA

CAMPO: En informática es un registro, espacio usado para una categoría particular de datos (Real Academia Española de la Lengua, 2014). En las bases de datos un campo es la mínima unidad de información a la que se pueda acceder, un campo o un conjunto de ellos forman un registro.

FORMULARIO: Un formulario es un documento, ya sea físico o digital, diseñado con el propósito de que el usuario introduzca datos estructurados como nombre, apellidos, dirección, teléfono, celular etc., en las zonas del documento destinadas para este propósito, para ser almacenados y procesados posteriormente. (Real Academia Española de la Lengua, 2014)

FORMULARIO ELECTRÓNICO: Formatos que pueden ser diligenciados por cualquier ciudadano para realizar trámites en línea. Por ejemplo, Formularios para peticiones quejas y reclamos. (Archivo General de la Nación, 2012)



PLANTILLA DE DOCUMENTOS: Documento base sobre el cual se construyen varios documentos respetando su estructura y configuración. Los usuarios pueden ver siempre la versión más actualizada que ha sido normalizada al ver la última plantilla en uso.

5. BENEFICIOS EN LA IMPLEMENTACIÓN DEL PROGRAMA

Con el siguiente Programa de requisitos se normalizará y facilitará la producción, organización y consulta de los documentos que son creados electrónicamente por funcionarios y contratistas del MADR, de acuerdo con las Tablas de Retención Documental al ser implementados por éstos en la Entidad. Por otra parte, se garantizará la conservación digital y migración a corto mediano y largo plazo en la búsqueda y recuperación de la información en soportes electrónicos con sus características de autenticidad, fiabilidad, integridad y disponibilidad.

6. MODELO DE REQUISITOS MINIMOS PARA EL PROGRAMA

En modelo está enmarcado dentro de un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA). Se relacionarán un conjunto de aplicaciones que permitan la gestión de los documentos en formatos electrónicos y evidencien la trazabilidad y recuperación de los documentos de la entidad.

Según el Decreto 1080 de 2015 el SGDEA debe ser un Sistema que administre y gestione los documentos electrónicos que sean cargados al Sistema por lo tanto en el Ministerio de Agricultura y Desarrollo Rural debe tener en cuenta que este Sistema cumpla con las siguientes características:

- Organizar los documentos físicos y electrónicos, según las Tablas de Retención Documental.
- Asignar metadatos de acuerdo con el Cuadro de Clasificación Documental, para la búsqueda y recuperación de los documentos.
- Incluir los tiempos de conservación a corto, mediano y largo plazo de los documentos electrónicos.
- Realizar la eliminación parcial o completa de los documentos electrónicos de archivo de acuerdo con los tiempos de retención establecidos en las tablas de retención documental (TRD).
- Garantizar la autenticidad de los documentos de archivo y la información conexa (metadatos) durante el ciclo de vida de los documentos electrónicos.
- Garantizar la integridad de los documentos electrónicos de archivo, mediante agrupaciones documentales, en series y subseries y las autorizaciones de modificaciones y la trazabilidad de adulteración.
- Garantizar la fiabilidad de los documentos electrónicos de archivo por sus creadores.



- Permitir la disponibilidad de los documentos electrónicos de archivo, cuando sean requeridos por los funcionarios, contratistas y la ciudadanía.
- Organizar los documentos electrónicos de archivo por series, subseries documentales según con la estructura orgánico-funcional de la Entidad.
- Realizar las migraciones correspondientes según las nuevas versiones de software y hardware para los diferentes soportes de almacenamiento electrónico existentes en el mercado para la recuperación y reproducción de la información en estos soportes magnéticos.

6.1. CARACTERÍSTICAS DEL PROGRAMA

A continuación, se relacionan las características que se deben contemplar para la implementación del programa mediante los módulos del SGDEA en el Ministerio de Agricultura y Desarrollo Rural:

6.1.1. Conformidad.

Respaldar la gestión de la información disponible electrónicamente a partir de los procesos administrativos de la entidad.

6.1.2. Interoperabilidad.

Permitir la interoperabilidad con los otros sistemas de información, a lo largo del tiempo, basado en el principio de neutralidad tecnológica, el uso de formatos abiertos y estándares nacionales o internacionales adoptados por las autoridades o instancias competentes.

6.1.3. Seguridad.

Mantener la información administrativa en un entorno seguro.

6.1.4. Metadescripción.

Generar los metadatos normalizados, sean manuales o automatizados, desde los mismos sistemas y aplicativos.

6.1.5. Adición de contenidos.

Agregados nuevos contenidos a los documentos, en forma de metadatos, sin que se altere la autenticidad, valor probatorio e integridad de los documentos.



6.1.6. Diseño y funcionamiento.

Permitir la creación y captura de documentos con el fácil manejo para los usuarios, haciéndola tan simple como sea posible.

6.1.7. Gestión Distribuida.

Ofrecer capacidades para importar y exportar masivamente los documentos agrupados en series, subseries, expedientes y metadatos asociados desde y hacia otros sistemas de gestión documental.

6.1.8. Disponibilidad y acceso.

Asegurar la autenticidad, integridad, inalterabilidad, accesibilidad, interpretación y comprensión de los documentos electrónicos en su contexto original, así como su capacidad de ser procesados y reutilizados en cualquier momento.

6.1.9. Neutralidad tecnológica.

Garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones para garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.

7. REQUISITOS DE ACCESO Y SEGURIDAD PARA EL SISTEMA SGDEA

Requisitos de acceso: El sistema de Gestión Documental Electrónico de Archivos debe cumplir con los siguientes requisitos de seguridad:

- Permitir que el administrador restrinja el acceso a los documentos electrónicos de archivo, expedientes y metadatos a determinados usuarios o grupos de usuarios.
- Permitir que el administrador asocie al perfil del usuario ciertos atributos que determinarán las funciones, los campos de metadatos a los documentos electrónicos de archivo y los expedientes a los que el usuario tendrá acceso
- Permitir las mismas funciones de control para los perfiles y para los usuarios.
- Establecer grupos de usuarios asociados a un conjunto de expedientes o documentos electrónicos de archivo
- Permitir que un usuario pertenezca a más de un grupo.



- Permitir a los administradores la capacidad de establecer perfiles de usuarios y asignar usuarios a los grupos.

Por otra parte, al buscar un documento electrónico de archivo, volumen o expediente o solicita acceder a él sin tener derecho a consultarlo, el SGDEA debe darle una de las siguientes respuestas que se seleccionarán cuando se configure el sistema:

- Visualizar los títulos y los metadatos de los documentos electrónicos de archivo.
- Reconocer la existencia del expediente o documento electrónico de archivo esto es, visualización del número del expediente o del documento de archivo, pero sin revelar su título ni ningún otro metadato.
- Ocultar toda información sobre el documento electrónico de archivo y de cualquier otra indicación que pueda sugerir su existencia.
- Realizar búsquedas de texto íntegro, nunca debe incluir en los resultados documentos electrónico de archivo a los que el usuario no tenga derecho a acceder.
- Permitir que los usuarios intenten acceder a expedientes, volúmenes o documentos electrónico de archivo sin la autorización debida, debe quedar constancia de tales intentos en la pista de auditoría.

8. COPIAS DE SEGURIDAD Y RECUPERACIÓN

Es necesario contar con protocolos de seguridad que involucre los siguientes tipos de copias de seguridad (Backups):

Copia de la programación de la aplicación SGDEA

Copia de la bodega de datos

De esta manera se garantizará que las copias de seguridad sean restablecidas desde diferentes posibles fallos que se puedan presentar.

La periodicidad de la información, que se registre y/o se almacene en la aplicación debe contar con una copia espejo garantizando que dicha copia se encuentre fuera de las instalaciones del MADR garantizando su recuperación en caso de catástrofe.

9. NIVELES DE SEGURIDAD Y ACCESO

Los niveles de seguridad del SGDEA deben contar con las restricciones



establecidas en el artículo 18 de la Ley 1712 de 2014 de transparencia el cual determina las excepciones que deben tener los documentos de carácter público

Los datos de acceso están relacionados con las Tablas de Control de Acceso.

10. REQUISITOS SOBRE LAS TABLAS DE RETENCION DOCUMENTAL (TRD)

El SGDEA debe garantizar la conservación de los documentos electrónicos en cumplimiento del Acuerdo 004 de 2019 AGN con los tiempos de retención asignados y el soporte formato para cada tipo documental registrados en las Tablas de Retención Documental del MADR.

De la misma manera el sistema debe cumplir con los siguientes requisitos:

- Asignar los tiempos de retención a los documentos por serie y Subserie documental establecidas en las Tablas de Retención Documental.
- Identificar los documentos electrónicos de archivo para la eliminación una vez se cumpla su periodo de retención en el archivo de gestión y archivo central por medio de la generación de inventario documental en el Formato Único de inventario documental FUID para publicación en la Página Web de la Entidad.
- Elaborar automáticamente inventarios de transferencias primarias y secundarias según los inventarios documentales y archivos electrónicos digitales para su conservación.
- Realizar las transferencias virtuales y/o alerta de transferencias automáticas al momento de cumplir con los periodos de retención establecidos en las Tablas de Retención Documental.
- Recuperar los expedientes de sistemas de archivo con búsqueda sencilla y estructurada que garantice la disponibilidad de la información.
- Soportar la búsqueda en texto completo de los documentos digitalizados asignándoles niveles de recuperación.

11. REQUISITOS DE CAPTURA

El proceso de captura de documentos electrónico de archivo en el SGDEA debe contar con los controles y la funcionalidad adecuados así:



- Registrar y gestionar todos los documentos electrónicos de archivo, con independencia del método de codificación empleado y de otras características tecnológicas.
- Garantizar que los documentos electrónicos de archivo se asocian con el un Cuadro de Clasificación Documental y a uno o más expedientes.
- Integrarse con el software de aplicaciones que genera los documentos electrónicos de archivo.
- Validar y controlar la entrada de metadatos en el SGDEA.

12. MODELO DE METADATOS

El Ministerio de Agricultura y Desarrollo Rural cuenta con la plataforma ORFEO para la radicación, captura, asignación y trámite de los documentos asociados al software de digitalización, el cual permite subir los documentos al sistema, se basa en la radicación de la correspondencia lo cual impide la alimentación de la bodega de datos por otro tipo de entrada a un SGDEA.

Es necesario establecer un modelo de metadatos que permita la indexación de los documentos electrónicos de archivo o digitales según los requerimientos establecidos y que facilite la recuperación de la información para consulta garantizando el cumplimiento de Archivo Total establecido en la Ley 594 de 2000.

El modelo de metadatos debe cumplir con lo establecido en el documento “*Guía de metadatos*” (Colombia. Archivo General de la Nación, 2014)

13. REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Es necesario establecer las características que deben tener un documento electrónico de archivo para su gestión y trámite en el sistema de archivos digitales, en este caso las tipologías documentales y series documentales deben ser identificadas para determinar cuál es la forma idónea de producción y/o digitalización.

El primer nivel de información que se debe asociar a la gestión de documentos electrónicos de archivo está directamente relacionado con el valor probatorio que tenga un documento electrónico o digital con respecto del físico, por lo tanto, se debe identificar en las Tablas de Retención Documental cuando un documento es susceptible de digitalización y/o contiene valor probatorio.

Una vez identificados los tipos documentales de acuerdo con las Tablas de Retención Documental en su soporte formato dando cumplimiento con la “*Guía 5 Cero papel*” (Colombia. Ministerio de las Tecnologías y las Comunicaciones, 2014)



se procederá a establecer los mecanismos necesarios para la implementación de firmas digitales para los documentos electrónicos de archivo que por sus características sean requeridos.

Por otra parte, sobre los documentos electrónicos de archivo que se produzcan en el MADR en desarrollo de sus funciones estos deben cumplir con los elementos esenciales tales como: autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad y conservación, que garanticen que los documentos electrónicos mantienen su valor de evidencia a lo largo del ciclo de vida, incluyendo los expedientes mixtos (híbridos), digitales y electrónicos:

A continuación, se presentan las características que deben contener los documentos archivo según sea su soporte en cumplimiento de la Norma ISO 15489:

13.1. AUTENTICIDAD

Entendida como el efecto de acreditar que un documento es lo que pretende ser, sin alteraciones o corrupciones con el paso del tiempo. Es uno de los componentes que conforman la confianza del documento respecto al contexto, estructura y contenido:

Contexto: Tiene que ver con la actividad y con la entidad, por cuanto la actividad “per-se” sin un contexto administrativo identificable quedaría incompleta.

Estructura: Tiene que ver con la forma documental fija o la presentación del contenido, que en gran medida está dada por el software y hardware.

Contenido: La materia del documento. Tiene que ver con el entorno en el cual ha sido creado el documento de acuerdo con el marco jurídico, administrativo, procedimental y documental de la entidad, para lo cual se tendrán en cuenta los metadatos que permitan demostrar su procedencia.

Por lo anterior es importante que en un documento electrónico se pueda identificar:

1. El software y hardware necesario para su representación.
2. Que el documento es lo que afirma ser.
3. La certeza sobre la persona que lo ha elaborado, enviado, firmado, o cuando exista evidencia respecto de la persona a quién se atribuya el documento.
4. Que ha sido creado o enviado en el momento que se afirma.
5. El documento electrónico es verídico y no ha sido alterado.



Requisitos para la presunción de autenticidad de los documentos electrónicos de archivo.

Se deben documentar e implementar procedimientos de seguridad y control durante todas las etapas del ciclo de vida del documento para evitar la pérdida o corrupción de los documentos de archivo o cualquier adición, supresión, modificación, utilización u ocultación no autorizadas, así como la protección de los medios de almacenamiento y la tecnología.

Con relación al documento electrónico de archivo debe poderse identificar de forma explícita metadatos tales como:

Los Sistemas de Gestión de Documentos Electrónicos de Archivo SGDEA, deberán gestionar metadatos adicionales relacionados con: nivel de acceso, privilegios de acceso, mantenimiento, modificación, transferencia, preservación y disposición, de los documentos electrónicos de archivo, en donde se refleje una relación o asociación con el documento y expediente a través de la incrustación o vinculación de metadatos.

Igualmente, el SGDEA debe contar con características y funcionalidades para almacenar documentos preservando su contenido, contexto y estructura, permitiendo verificar su autenticidad e integridad independientemente de hardware y software con el que fue creado.

Establecer las políticas, procedimientos, mecanismos técnicos y tecnológicos de autenticidad.

Para asegurar la autenticidad en los documentos electrónicos de archivo la entidad debe establecer políticas y procedimientos así:

a) Para el control de la creación, recepción, transmisión, mantenimiento, disposición y preservación de los documentos electrónicos de archivo, de manera que se asegure que los creadores de los mismos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.

b) Definir procedimientos para asegurar la cadena de preservación de los documentos electrónicos de archivo a lo largo del ciclo de vida, y en el transcurso del tiempo según con las Tablas de Retención Documental.

Para otorgar autenticidad a los documentos electrónicos de archivo el MADR puede hacer uso de las siguientes técnicas:



a) Estampas de tiempo: Consiste en una secuencia de caracteres utilizada para certificar el momento específico en que se lleva a cabo un suceso sobre un documento electrónico o que éste no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y hora exacta en que ocurre dicho evento y específicamente cuando fue creado o firmado en un sistema de cómputo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, firma de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana.

b) Firmas electrónicas: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

c) Firmas digitales: La firma digital se configura como un valor numérico que se asocia a un mensaje de datos y permite determinar que dicho valor ha sido generado a partir de la clave originaria, sin modificación posterior. La firma digital se basa en un certificado seguro y permite a la entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos.

Como medida, en el marco de la conservación de los documentos electrónicos a largo plazo, se recomienda la actualización de la firma digital. Esta medida de control consiste en el resellado o la refirma, como medios para prevenir la obsolescencia o la vulneración del sistema de firma.

La diferencia entonces es fundamentalmente probatoria, pues si bien la firma digital de manera automática incorpora la autenticidad, integridad y no repudio, en la firma electrónica es necesario probarla, además de determinar que se trata de un mecanismo confiable y apropiable.

Si se trata de una firma biométrica electrónica o electrónica manuscrita, tendrá el mismo valor de una firma electrónica, siempre que cumpla con los requisitos exigidos por los arts. 3º8 y 5º9 del Decreto 2364 de 2012, sea o no emitida por una entidad certificadora. De lo contrario, si por ejemplo la firma es tomada en un “digital pad” y es fijada en un documento que es impreso, podrá ser tenida como una firma o rubrica común, impuesta mediante un mecanismo electrónico, es decir, una firma de puño y letra del autor, pero fijada, por decirlo así, con tinta electrónica.



d) **Certificados digitales:** Los certificados digitales se conocen como una parte de la información que se asocia a un mecanismo para acreditar la validez de un documento perteneciente a un autor (autenticación), verificar que no ha sido manipulado ni modificado (integridad), al igual que impide que el autor niegue su autoría (no repudio) mediante validación de la clave pública del autor.

e) **Código seguro de verificación (CSV):** Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente pueden tener la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

El Código seguro de verificación (CSV) es una comprobación de la autenticidad del documento ingresando un código alfanumérico en la sede electrónica correspondiente.

f) **Marcas de agua digitales:** Corresponde a datos incrustados en documentos electrónicos tales como fotografías, películas, audios, y otros contenidos digitales y constituyen un medio seguro para certificar el origen, propiedad y autenticidad de los activos digitales.

13.2. FIABILIDAD

Entendida como la capacidad de un documento para asegurar que su contenido es una representación completa, fidedigna y precisa de las operaciones, las actividades, los hechos que testimonia o se puede establecer, declarar o sostener el acto o hecho del que es relativo, determinando la competencia del autor y examinando tanto la completitud en la forma del documento como el nivel de control ejercido durante su proceso de producción.

Requisitos para la presunción de fiabilidad de los documentos electrónicos de archivo.

Los documentos de archivo electrónico deberán ser creados así:

Dando testimonio de la operación o actividad que reflejan, declarando el acto o hecho del que es concerniente.

Dando testimonio del lugar, estableciendo la competencia del autor.

Dando certeza de estar completo en la forma del documento de archivo, incluyendo información de control de su producción.



Manteniendo su identidad inequívoca, es decir los atributos de contexto y procedencia que le son propios, como evidencia electrónica de las transacciones, actividades o hechos a lo largo del tiempo.

Mediante métodos seguros y verificables.

Por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones.

13.3. INTEGRIDAD

Entendida como la cualidad de un documento electrónico de archivo para estar completo y sin alteraciones, con la cual se asegura que el contenido y atributos están protegidos a lo largo del tiempo. Es uno de los componentes que conforman la confianza del documento.

Requisitos para la presunción de integridad de los documentos electrónicos de archivo:

Los documentos deben permanecer completos, protegidos contra modificaciones y alteraciones no autorizadas.

Se deben especificar las adiciones o anotaciones pueden realizarse en un documento después de su creación, en qué circunstancias pueden autorizarse dichas adiciones o anotaciones y quién está autorizado para llevarlas a cabo. Cualquier anotación, adición o supresión autorizada que se realice en un documento debería indicarse de forma explícita y dejar traza.

Analizar los casos especiales donde se puedan llevar a cabo estas actividades, los riesgos, las implicaciones jurídicas, dichas actividades deberá estar previamente autorizadas y documentadas.

Conservar los metadatos de contexto, que den cuenta de la naturaleza procedimental, jurídica, administrativa y tecnológica (auditoria) que da origen al documento dándole la confiabilidad requerida.

Mantener de manera permanente la relación entre el documento electrónico de archivo y sus metadatos.

En caso de requerirse algún cambio por razones de obsolescencia tecnológica, preservación a largo plazo, se debe realizar por personal debidamente autorizado dejando evidencia en el documento (a través de metadatos) y en la documentación del procedimiento de los cambios realizados, conforme a reglas



establecidas, limitadas y controladas por la entidad. (Esto debe previamente ser autorizado por una instancia de nivel decisorio; adicionalmente debe quedar reglamentado en el Sistema Integrado de Conservación.)

Proporcionar y mantener pistas de auditoría u otros métodos de seguimiento que demuestren que los documentos de archivo están protegidos frente a la utilización, la modificación y la destrucción no autorizadas.

Conservar los niveles de restricción de acceso, en caso de que el contenido de los documentos sea clasificado o reservado, según la Ley 1712 de 2014.

Estas medidas de control pueden formar parte del sistema en el que se gestionan o producen los documentos o ser externas al mismo donde se pueda demostrar que la actualización, el mantenimiento habitual o cualquier fallo de funcionamiento del sistema no afectan a la integridad de los documentos.

“La integridad de la información tiene que ver con que el contenido del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario, tarea que puede cumplirse técnicamente utilizando el procedimiento conocido como “sellamiento” del mensaje, mediante el cual aquel se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de ella en función de las características del mensaje realmente recibido; de modo, pues, que si el mensaje recibido no es exacto al remitido, el sello recalculado no coincidirá con el original y, por tanto, así se detectará que existió un problema en la transmisión y que el destinatario no dispone del mensaje completo. Incluso, la tecnología actual permite al emisor establecer si el receptor abrió el buzón de correo electrónico y presumiblemente leyó el mensaje”.

Esa característica guarda una estrecha relación con la “inalterabilidad”, requisito que demanda que el documento generado por primera vez en su forma definitiva no sea modificado, condición que puede satisfacerse mediante la aplicación de sistemas de protección de la información, tales como la criptografía y las firmas digitales.

Ejemplo: Un documento con criptografía solo puede ser visto por la persona que lo envió o lo recibió, y el destinatario puede verificar si el remitente es auténtico y si el documento ha sido modificado o alterado.

Mecanismos técnicos y tecnológicos de integridad:

Adicional a lo mencionado anteriormente, se debe establecer:

Políticas y procedimientos para la administración de bases de datos, documentos electrónicos y demás registros de información.



Integridad personal, responsabilidad, confianza del personal que maneja información sensible de la organización.

Medidas de protección para evitar la pérdida o corrupción de los documentos de archivo y los medios de almacenamiento.

Segregación de funciones, es decir asignar y monitorear los permisos de acceso a los datos y documentos electrónicos para que cada función tenga los privilegios que necesita y no abusen de los mismos. Este es un concepto de probada eficacia práctica, en el que seguramente harán hincapié las auditorías internas cuando se revisen sistemas y transacciones de carácter confidencial.

Integridad en bases de datos, se establece desde la etapa de diseño de una base de datos mediante la aplicación de reglas y procedimientos estándar, y se mantiene a través del uso de rutinas de validación y verificación de errores. Esto incluye integridad de las entidades, la integridad de los dominios y la integridad referencial.

Para contribuir con la integridad en los documentos electrónicos la entidad pueden hacer uso de las siguientes técnicas:

Controlar los privilegios y derechos de acceso para prevenir cambios no autorizados de la información.

Autenticación, cuando se habla de la integridad del origen (Fuente de los datos). Ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

Parches de seguridad sobre el sistema operativo y software base para evitar mantener vulnerabilidades que puedan ser aprovechadas para afectar la integridad de los documentos electrónicos de archivo.

13.4. DISPONIBILIDAD

Entendida en un documento electrónico de archivo, como la capacidad actual y futura de que tanto el documento como sus metadatos asociados puedan ser consultados, localizados, recuperados, presentados, interpretados, legibles, y por tanto estar en condiciones de uso.

Requisitos para la presunción de disponibilidad de los documentos electrónicos de archivo.



Cada documento deberá contener la información necesaria para identificar el contexto de las actividades administrativas que lo conforman y el vínculo archivístico, existentes entre los documentos de archivo y el expediente de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).

La información debe estar disponible para consulta presente y en el futuro independientemente del sistema que la produjo, su estructura o medio de registro original.

Mantener el vínculo permanente entre el documento y sus metadatos.

Los documentos electrónicos y la información en ellos contenida, debe estar disponible en cualquier momento, mientras la entidad está obligada a conservarla, de acuerdo con lo establecido en las Tablas de Retención Documental (TRD).

13.5. MECANISMOS TECNICOS Y TECNOLOGICOS DE DISPONIBILIDAD

Para garantizar la disponibilidad de los documentos electrónicos en sus diferentes formatos y formularios utilizados en el Ministerio, debe establecer políticas y procedimientos como los siguientes:

Plan de respuesta a incidentes y plan de continuidad del negocio.

Acuerdos de Niveles de Servicio. La entidad debe velar por la óptima prestación de los servicios de TI “Tecnologías de la información”, identificando las capacidades actuales de los Servicios Tecnológicos y proyectando las capacidades futuras requeridas para que cumplan con los niveles de servicio acordados con los usuarios.

Gestionar la capacidad, la operación y el soporte de los servicios tecnológicos, con criterios de calidad, seguridad, disponibilidad, continuidad, adaptabilidad, estandarización y eficiencia.

Prevención de ataques de denegación del servicio: configuración de routers y firewalls para filtrar IPs inválidas, así como el filtrado de protocolos que no sean necesarios. Es recomendado contar con un Sistema de Detección de Intrusos (IDS) - Sistema de Prevención de Intrusos (IPS).

Sistemas de contingencia alternativos o manuales. De esa forma, si la tecnología principal falla parcial o totalmente, habrá un sistema de respaldo que pueda ser puesto en operación.



Debe implementar capacidades de alta disponibilidad que incluyan balanceo de carga y redundancia para los Servicios Tecnológicos que afecten la continuidad del servicio de la institución, las cuales deben ser puestas a prueba periódicamente.

Debe implementar controles de seguridad para gestionar los riesgos asociados al acceso, trazabilidad, modificación o pérdida de información que atenten contra la disponibilidad, integridad y confidencialidad de la información.

13.6. INTEROPERABILIDAD

La interoperabilidad se relaciona con el intercambio electrónico de datos, y apunta a que el Estado colombiano funcione como una sola institución eficiente que les brinde a sus ciudadanos información oportuna, trámites ágiles y mejores servicios.

Por lo tanto, el Ministerio debe garantizar la habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información, así como la habilidad de los sistemas (computadores, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar e intercambiar datos, documentos en varios formatos y formularios de acuerdo con un método definido, con el fin de obtener los resultados esperados.

El marco de interoperabilidad para gobierno en línea define la interoperabilidad como: “El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades”.

13.7. TRANSFERENCIA DE DOCUMENTOS ELECTRÓNICOS

Consiste en el proceso técnico, administrativo y legal mediante el cual se entregan, a los archivos centrales (transferencia primaria) o a los archivos históricos (transferencia secundaria), los documentos electrónicos de archivos que de conformidad con las tablas de retención documental han cumplido su tiempo de retención en la etapa de archivo de gestión o de archivo central respectivamente.

En cumplimiento de lo anterior el Ministerio deberá acoger los lineamientos emitidos por el Archivo General de la Nación para la generación de la transferencia de documentos electrónicos de archivo, de forma que se asegure su integridad, autenticidad, preservación y consulta a largo plazo.



Es importante destacar que el Archivo General de la Nación es el responsable de recibir las transferencias de los archivos de valor histórico en formato digital de entidades públicas del orden nacional del sector central de la Rama Ejecutiva, así como los organismos del orden nacional adscritos o vinculados a los ministerios, departamentos administrativos, agencias gubernamentales y superintendencias, para asegurar su protección, conservación y acceso a los ciudadanos.

En la siguiente tabla, se presentan los formatos para la conservación de documentos electrónicos a largo plazo.

FORMATO	CARACTERISTICAS	EXTENSION	ESTANDAR
PDF	De tipo compuesto (imagen vectorial, mapa de bits y texto), que contiene soporte para anotaciones, metadatos, etc.	.pdf	ISO 32000
PDF/A	Formato de archivo de documentos electrónicos para la Preservación a largo plazo.	.pdf	ISO 19005
PDF/A-1	PDF/A-1 Restricciones en cuanto al uso del color, fuentes, y otros elementos.	.pdf	ISO 19005-1
	PDF/A-1b (Subnivel b = Básico) Garantiza que el texto del documento se puede visualizar correctamente.		
	PDF/A-1a (Subnivel a = avanzado) Documento etiquetado lo que permite añadirle información sobre su estructura.		



PDF/A-2	PDF/A-2 Características adicionales que no están disponibles en formato PDF/A-1	.pdf	ISO 19005-2 ISO 32000-1
	PDF/A-2b (Subnivel b = Básico) Se cumplen todos los requisitos descritos como necesarios.		
	PDF/A-2a (Subnivel a = avanzado) Adicional contiene información textual o sobre la estructura lógica del documento.		
	PDF/A-2u (Subnivel u = Unicode) Requisito adicional, todo el texto en el documento tienen equivalentes en Unicode		
PDF/A-3	PDF/A-3 Ofrece soporte para archivos incrustados.	.pdf	ISO 19005-3 ISO 32000-1
	PDF/A-3b (Subnivel b = básico) Se cumplen todos los requisitos descritos como necesarios para un PDF/A-3.		
	PDF/A-3a (Subnivel a = avanzado) etiquetado de forma que se describa y conserve la estructura lógica — el orden de lectura		



XML	Es un estándar abierto, flexible y ampliamente utilizado para almacenar, publicar e intercambiar cualquier tipo de información.	.xml	W3C HTML Estándar Abierto
JPEG2000	JPEG2000 (sin pérdida) permite reducir el peso de los archivos a la mitad en comparación con las imágenes no comprimidas.	.jpg2 .jp2	ISO/IEC 15444
OpenDocument	Formato de archivo abierto y estándar de la familia ODF para el almacenamiento de gráficas	.odg	OASIS ISO/IEC 26300
TIFF	TIFF (sin compresión) Archivos más grandes que un formato comprimido	.tiff	ISO 12639
SVG	Formato para describir gráficos vectoriales bidimensionales, tanto estáticos como animados en formato XML.	.svg .svgz	W3C
BWF	Formato de archivo que toma la estructura de archivos WAVE existente y añade metadatos adicionales	.bwf	EBU - TECH 3285



JPEG2000-Motion	Formato para la Preservación sin pérdida de vídeo en formato digital y migración de las grabaciones de vídeo analógicas obsoletos en archivos digitales	.mj2 .mjp2	ISO 15444-4
GML	Geography Markup Language (GML) Formato basado en XML para el modelaje, transporte y almacenamiento de información geográfica.	.gml	ISO 19136 Estándar Abierto
GMLJP2	GML en JPEG 2000 proporcionar una codificación XML de los metadatos necesarios para la georreferenciación de imágenes JPEG2000, utilizando GML	.gml .jp2	Open Geospatial Consortium (OGC).
GZIP	Formato de compresión de datos	.gz	RFC 1952 Estándar Abierto
SIARD	Formato para el archivo de bases de datos relacionales en una forma independiente del proveedor, delimitado archivos planos (texto sin formato) con DDL	.siard	N/A
WebARChive	Utilizado para almacenar "Web crawls" como secuencias de bloques de contenido	.warc	ISO 28500



	recolectados de la World Wide Web		
EML	Diseñado para almacenar mensajes de correo electrónico en forma de un archivo de texto sin formato	.eml	RFC 822
MBOX	Formato utilizado para almacenar conjuntos de correos electrónicos.	.mbox .mbx	N/A

Los documentos que no tengan valor probatorio y que no requieran firma digital, sino que su característica principal es de consulta y no requieran conservación a largo plazo se pueden digitalizar teniendo en cuenta los siguientes requisitos mínimos:

- Formato PDF/A
- 100 dpi mínimo
- Reconocimiento OCR

Los documentos con valor probatorio susceptibles de implementación de firma digital y conservación a largo plazo deben cumplir con los siguientes requisitos:

- Los archivos digitalizados deberán estar en formato PDF/A.
- El documento digitalizado deberá permitir hacer OCR para seleccionar el documento o parte de el para poderlo copiarlo.
- Los documentos preparados se deben digitalizar con una resolución mínima de 300 DPI en blanco y negro
- El formato en PDF/A debe permitir la consulta en ambiente cliente servidor vía WEB.
- Si algún documento no cuenta con el tamaño carta u oficio, el contratista deberá pegar en una hoja blanca del tamaño a que haya lugar, para su digitalización y hará parte del expediente con su respectiva foliación. (papel que será suministrado por el contratista).
- Profundidad de bit: estar determinada por las características del documento de tal forma que la imagen obtenida no presente fallas de calidad. El valor máximo a utilizar es de 16 bits.



- Brillo y contraste: estar determinados por las características del documento y del escáner utilizado de tal forma que la imagen obtenida no presente fallas de calidad. El valor recomendado es 50/50.
- El tamaño de un archivo de una página deberá estar en el rango de 60 a 100 kb dependiendo de la cantidad de caracteres de la página.

Lo anterior garantizará que los documentos cumplan con lo establecido por la normativa actual vigente y garantizará la óptima gestión de los documentos digitales.

BIBLIOGRAFIA

COLOMBIA. ARCHIVO GENERAL DE LA NACIÓN. Acuerdo 004 Por el cual se reglamenta el procedimiento para la elaboración, aprobación, evaluación y convalidación, implementación, publicación e inscripción en el Registro único de Series Documentales – RUSD de las Tablas de Retención Documental – TRD y Tablas de Valoración Documental – TVD. Bogotá D. C.: AGN. 2019.

COLOMBIA. ARCHIVO GENERAL DE LA NACION. Guía de metadatos. Guía para la formulación de un esquema de metadatos para gestión de documentos: Disponible en:

<http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/SINAE/Productos%20SINAE%202013/Guia%20de%20metadatos.pdf>

COLOMBIA. ARCHIVO GENERAL DE LA NACION. Instrumentos archivísticos. Consultado 27 de junio 2018. Disponible en:

<http://www.archivogeneral.gov.co/politica/instrumentos-archivisticos>

COLOMBIA. ARCHIVO GENERAL DE LA NACION. Manual de implementación de un programa de gestión documental. Bogotá: AGN. 2014.

COLOMBIA. ARCHIVO GENERAL DE LA NACION. Preservando para el futuro. 2012. Consultado 26 de agosto de 2018. Disponible en: <<http://preservandoparaelfuturo.org>>

COLOMBIA. MINISTERIO DE CULTURA. Decreto 1080 de 2015. Decreto Unico Reglamentario del Sector Cultura. 2015.

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS Y LAS COMUNICACIONES. Gobierno en Línea. Guía 5 Digitalización certificada de documentos: 2014. Disponible en: <http://programa.gobiernoenlinea.gov.co/apc-aa>



files/da4567033d075590cd3050598756222c/guia-5-digitalizacin-de-documentos.pdf

INTERNATIONAL STANDARD ORGANIZATION. ISO 15489. Información y Documentación. Gestión de Documentos. Ginebra: Departamento de Derechos de Autor ISO. 2001. 37 p.

REAL ACADEMIA ESPAÑOLA DE LA LENGUA. Diccionario Real Academia Española de la Lengua. La academia. 2014. 689 p.